NACDL FOURTH AMENDMENT CENTER

Geofence Warrant Primer

Geofence warrants are a type of reverse warrant where the government seeks to know who was within a "geofence," a defined physical area during a specific period of time. These are a type of "reverse warrant," used to identify suspects when none are known without the data gathered by the warrant. The government utilizes geofence warrants to compel companies, such as Google, to produce information about devices interacting with their technology within a particular geographic region.

Geofence warrants are an unprecedented increase in the government's ability to locate individuals without substantial investigation or investment of resources. Through geofence warrants, the government can obtain what Google refers to as "Location History" data. Location History keeps records about where a user's device is at any given time through a variety of data, including: GPS information, Bluetooth beacons, cell phone location information from nearby cell towers, Internet Protocol address information, and the signal strength of nearby WiFi networks. *United States v. Chatrie*, 2022 WL 628905, *3 (E.D. Va. Mar. 3, 2022). For a more in depth discussion of Location History and the differences from CSLI, please see NACDL's Geofence webinar.[1]

Geofence warrants are general warrants — which are prohibited by the Fourth Amendment — because they are devoid of probable cause and particularity. To suppress evidence from a geofence warrant, it is necessary to demonstrate a Fourth Amendment search occurred, the search violated the constitution, and the good faith exception does not apply.

Steps in the Geofence Process

The geofence process involves up to three steps, which may be completed through a single or multiple warrants or through a combination of warrants and other forms of process.

Step One: The government first seeks anonymized numerical identifiers and time-stamped location coordinates for every device that passed through an area in a specified window of time. This information is obtained from a company, most commonly Google, using a geofence warrant. The data provided to law enforcement in Step One is not truly anonymized because people can be easily identified from their Location History data, and the government can get subscriber information for anonymous IDs with only a subpoena after Step One. *See Chatrie*, 2022 WL 628905 at *22 n.39 (noting that the collection of "anonymized location data" through a geofence warrant "can reveal astonishing glimpses into individuals' private lives").

Step Two: The government reviews the list and culls it using other investigative techniques. Sometimes the government requests more information about particular accounts from the company. That request may be made by a private letter to the company for more location history for a longer period of time with no geographic limitations.

Step Three: The government further narrows the list and requests identifying information (e.g., usernames, birth dates, and other identifying information of the phones' owners) from the company for the culled list of users through the initial warrant or an additional warrant, court order, or subpoena.

Was There a Fourth Amendment Search?

To establish there was a search, first argue there is a reasonable expectation of privacy under *Carpenter v. United States*, 138 S. Ct. 2207, 2217 (2018). Under *Carpenter's* test, users have a reasonable expectation of privacy in their Google Location History.

First, Location History has "depth, breadth, and comprehensive reach" similar to the cell site location information ("**CSLI**") at issue in *Carpenter*, and allows the government to historically reconstruct an individual's past movements in a way that would have been impossible at the time of the adoption

of the Fourth Amendment. 138 S. Ct. at 2223; *see also Leaders of a Beautiful Struggle v. Baltimore*, 2 F.4th 330, 334 (4th Cir. 2021) (holding "*Carpenter* squarely applie[d]" when images in a location tracking scheme allowed law enforcement to "travel back in time" as if they had "attached an ankle monitor" to every person in the city). In an amicus brief in one geofence warrant case, Google stated that Location History "can often reveal a user's location and movements with a much higher degree of precision than [CSLI]." *Chatrie*, 2022 WL 628905 at *2 n.5.

Second, Location History is sensitive and reveals the "privacies of life." *Carpenter*, 138 S. Ct. at 2214. Geofence warrants request information on all devices within a virtual perimeter defined by law enforcement from large technology companies like Google with the hope of identifying a suspect amongst innumerable people. Depending on the boundaries of the geofence, the data may locate cell phones or other devices within "private residences, doctor's offices, political headquarters, and other potentially revealing locales," *Carpenter*, 138 S. Ct. at 2218; *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (stating that courts should carefully consider the "power of technology to shrink the realm of guaranteed privacy"). This invasion of constitutionally protected spaces is "presumptively unreasonable in the absence of a search warrant." *Katz v. United States*, 389 U.S. 347, 361 (1967).

Finally, the third-party doctrine does not apply because Location History, like CSLI, is distinct from "the limited types of personal information addressed in Smith and Miller." *Carpenter*, 138 S. Ct. at 2219. Google account holders cannot voluntarily share their location information in a meaningful way because a regular person would not be able to understand the frequency nor the precision of Google's location track-ing. See *Chatrie*, 2022 WL 628905 at *26.

Users also have a possessory interest in their Location History data. Google treats Location History as user property that it holds in trust. *See Chatrie*, 2022 WL 628905 at *2 n.5 ("Location History is not a business record, but is a journal stored primarily for the user's benefit and is controlled by the user."). The right to total exclusion of others from one's property 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 government's acquisition of a user's Location History constitutes a search under a traditional approach to the Fourth Amendment.

Was There a Constitutional Warrant?

The Fourth Amendment requires 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) (cleaned up). If a geofence warrant fails even one these requirements it is unconstitutional, and if a warrant is invalid, the appropriate remedy is to sup-press the evidence derived from it. *United States v. Calandra*, 414 U.S. 338, 347 (1974).

Geofence warrants implicate the First Amendment because location information can expose a person's speech or "familial, political, professional, religious, and sexual associations." *See United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Courts must apply Fourth Amendment requirements to geofence war-rants with "the most scrupulous exactitude" when they implicate First Amendment concerns. *Stanford*, 379 U.S. at 485.

Was the Search Overbroad?

By design, geofence warrants do not specify the person or people whose Google accounts will be searched. Instead, the goal is to search across "numerous tens of millions" of user accounts and then identify specific accounts that law enforcement would like to search further. Decl. of Marlo McGriff ¶ 13, *Chatrie*, No. 3:10-cr-130-MHL (E.D. Va. (Mar. 11, 2020), ECF No. 96-1). The scope of geofence warrants is intentionally overbroad. However, to be constitutional, 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). But, the fact that users caught in a geofence warrant were close to the site of an alleged crime does not, without more, give rise to probable cause to search that person. *See Ybarra v. Illinois*, 444 U.S. 85, 91.

Similarly, the fact that an alleged crime occurred does not support probable cause to search many or any unidentified people. 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 nearby." *Chatrie*, 2022 WL 628905 at *24. Geofence warrants are overbroad searches without sufficient, or any, probable cause.

Was the Search Particularized?

Geofence warrants permit law enforcement and Google to exercise an impermissible amount of discretion during Fourth Amendment searches and seizures.

In Step 1 of a geofence warrant, the government does not particularly describe what will be searched or seized, instead leaving both determinations to Google's discretion. A geofence warrant generally requires Google to search "all location data." It does not particularly describe what data Google must search (e.g., Location History data versus Web & App Activity data versus Google Location Accuracy data) based on probable cause. Also, a geofence warrant does not particularly describe the things to be seized. Instead, it leaves to Google's discretion how to "count" which users fall within a geofence, without providing necessary probable cause for those users. This falls short of the particularity requirement because "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979).

In Step 2 and 3 of a geofence warrant, law enforcement seeks and Google provides additional, deanonymizing information about users without justifying their choices to a judge. In *Chatrie*, the court implied that to satisfy particularity a geofence warrant must leave "ultimate discretion as to which users' information [is disclosed] to the reviewing court, not to Google or law enforcement." *Chatrie*, 2022 WL 628905, at *23. The court emphasized that constitutional warrants must incorporate "a court's authorization" when law enforcement successively seeks information about specific users, not authorization from a third party. *Chatrie*, at *24.

Did the Government Act in Good Faith?

The good-faith exception is limited to when law enforcement acts in good faith reli-ance on a warrant that is later found to be unconstitutional. *United States v. Leon*, 468 U.S. 897, 922 (1984). Note, some jurisdictions do not have the good faith exception, while others have additional factors in the inquiry. Ultimately, good faith requires a very fact-dependent argument.

Due to the glaring deficiencies of geofence warrants as a category — the absence of probable cause for all individuals searched, the overbreadth, and the lack of particularity for what is searched and seized — law enforcement cannot have an "objectively reasonable reliance" on geofence warrants. *Leon*, at 922. Furthermore, the good faith exception to the exclusionary rule is inapplicable because so much of the evidence that is collected through geofence warrants is particularized behind closed doors and without judicial approval.

Discovery and Subpoena Material

You will need to get information from both the government and Google to successfully litigate a motion to suppress. NACDL has several resources available for reference:

- Geofence Discovery Motion from *United States v. Chatrie* [2]
- Motion to Suppress from *United States v. Chatrie* [3]
- Order Granting Defense Request for Subpoena to Google[4]

More resources can be found on NACDL's website [5]

Case List

- *Carpenter v. United States*, 138 S. Ct. 2206 (2018)
- *United States v. Di Re,* 332 U.S. 581 (1948)
- *Katz v. United States,* 389 U.S. 347 (1967)
- *Kyllo v. United States,* 533 U.S. 27 (2001)
- *Leaders of a Beautiful Struggle v. Baltimore,* 2 F.4th 330 (4th Cir. 2021)
- *Loretto v. Teleprompter Manhattan CATV Corp.,* 458 U.S. 419 (1982)
- *Smith v. Maryland,* 442 U.S. 735 (1979)
- *United States v. Chatrie*, 2022 WL 628905 (E.D. Va. Mar. 3, 2022)
- *United States v. Miller,* 425 U.S. 435 (1976)
- *Dalia v. United States,* 441 U.S. 238 (1979)
- *Illinois v. Gates,* 462 U.S. 213 (1983)
- *In re Information Stored at Premises Controlled by Google,* 481 F. Supp. 3d 730, (N.D. Ill. 2020)
- *Riley v. California,* 573 U.S. 373 (2014)
- *Steagald v. United States,* 451 U.S. 204 (1981)
- *United States v. Comprehensive Drug Testing, Inc.,* 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam)
- *United States v. Galpin,* 720 F.3d 436 (2d Cir. 2013)
- *United States v. Leon,* 468 U.S. 897 (1984)
- *Ybarra v. Illinois,* 444 U.S. 85 (1979)
- *NAACP v. Alabama*, 357 U.S. 449 (1958)
- *Stanford v. Texas*, 379 U.S. 476 (1965)
- *United States v. Jones,* 565 U.S. 400 (2012)

Additional Resources

- Thomas Brewster, "Feds Order Google to Hand Over a Load of Innocent Americans' Locations," *Forbes* (Oct. 23, 2018)
- Tyler Dukes, "To Find Suspects, Police Quietly Turn to Google," *WRAL* (Mar. 15, 2018)
- Jennifer S. Granick, *Making Warrants Great Again: Avoiding General Searches in the Execution of Warrants for Electronic Data* (Dec. 2021)
- Michael Price & Bill Wolf, *Building on Carpenter: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider* (Dec. 2018)
- Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181 (2016)
- Google, Privacy Policy, Information Google Collects: Your location information (2022)

NACDL Resources

- *United States v. Chatrie* Content Page
- Digital Location Tracking Content Page
- Reverse Search Warrant Content Page

Editor's Note: *The content pages listed above can be found at nacdl.org. In addition, NACDL's webinars on geofences, location privacy after Carpenter, and the third-party doctrine and location tracking can be found by visiting https://www.nacdl.org/Content/Fourth-Amendment-Center-Videos.*

Notes

1. https://www.nacdl.org/Content/When-Google-Searches-for-You-Challenging-Geofence
2. https://www.nacdl.org/getattachment/0d3728fa-24b0-4df5-929a-9ccaef71c0fb/189110047428.pdf
3. https://www.nacdl.org/getattachment/a16a7368-3691-4b32-b479-ad8128c53016/5f0ba578-cfe1-4fb9-9e76-5d40778f3f40.pdf
4. https://www.nacdl.org/getattachment/19831ec4-9272-4072-ae89-d5bf4827235d/order-granting-defendant-s-motion-for-issuance-of-subpoena-duces-tecum.pdf
5. https://www.nacdl.org/Landing/Resource-Center

About the National Association of Criminal Defense Lawyers (NACDL)

The National Association of Criminal Defense Lawyers (NACDL) envisions a society where all individuals receive fair, rational, and humane treatment within the criminal legal system.

NACDL's mission is to serve as a leader, alongside diverse coalitions, in identifying and reforming flaws and inequities in the criminal legal system, and redressing systemic racism, and ensuring that its members and others in the criminal defense bar are fully equipped to serve all accused persons at the highest level.

About the Fourth Amendment Center

NACDL's Fourth Amendment Center offers direct assistance to defense lawyers handling cases involving new surveillance tools, technologies and tactics that infringe on the constitutional rights of people in America.

The Center is available to help members of the defense bar in bringing new Fourth Amendment challenges. To request assistance or additional information, contact **4AC@nacdl.org**.

How to Support Our Work

You can support our mission and enhance your career by becoming a member of the NACDL. Learn more by visiting **https://www.nacdl.org/Landing/JoinNow**.

NACDL FOURTH AMENDMENT CENTER

For litigation assistance and other resources contact 4AC@nacdl.org

[redacted]

IN THE UNITED STATES DISTRICT COURT
[redacted]

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Criminal Number:** [redacted]
	)	
[redacted]	)	
Defendant.	)	

MOTION TO SUPPRESS EVIDENCE FROM A GEOFENCE WARRANT

[redacted] though undersigned counsel, moves this Court to suppress Google Location History evidence obtained by a modern-day general warrant, in violation of the Fourth Amendment. The "geofence warrant" searched and seized Google "Location History" data belonging to an unknown number of people after a robbery of [redacted]' Bank in [redacted] Mr. [redacted] had a Fourth Amendment interest in his Location History data, and the warrant was overbroad and lacking particularity under the Fourth Amendment. The FBI seized data beyond the warrant's scope. The application was based on false statements, omitted material facts, and was facially invalid. The good faith doctrine is thus inapplicable, and consequently, the warrant and its fruits should be suppressed.

FACTS

Someone robbed the [redacted]' Bank at [redacted] in [redacted], [redacted] around [redacted] 2018. Surveillance video from a nearby pizza place appeared to show a dye pack exploding in the parking lot and police recovered a dye stained $50 bill from the area. In the videos, police also identified a silver Ford Focus with the same individual and no visible passengers driving away from the bank. The next morning, at around 8:30am, a witness found a $50 bill with red dye [redacted], approximately 0.7 miles from the bank.

Police investigated several leads of suspects other than Mr. [redacted] but made no arrests. Instead, the FBI applied for, and received, a novel geofence warrant for the search and seizure of Google "location history" data from an unspecified number of unknown Google users. *See* Ex. A

[redacted]

(Search Warrant & Application) at 3. The warrant application describes generally that Google collects location data from some users, *id.* at 11; described the bank robbery in one paragraph, *id.* at 12, and asserted that criminals generally use phones to coordinate crimes and take pictures of evidence or contraband, *id.* at 12-13. The application did not refer to any other possible suspects. It provided no evidence that the bank robber in this case had a cell phone. It provided no evidence that the robber had a Google account, let alone one linked to a cell phone. It did not offer any facts to indicate that such a phone would have had Google Location History enabled. And it did not allege any that the robber had such a phone with him at the time of the robbery.

I. Location History

Location History is a Google feature that logs device location data, showing where a user has been with that device. *See* Ex. B (Google Amicus) at 5. When Google saves this data, it associates it with unique user accounts it keeps in the "Sensorvault." Ex. C (McGriff Decl.) at 3. If a user has the Google Location History enabled, then Google estimates the user's device location using GPS data, the signal strength of nearby Wi-Fi networks, Bluetooth beacons, and cell phone towers. Ex. C at 4. Location History is not an "app"; it is a setting on the Google account associated with a device, and it is currently an "opt-in" feature. Once enabled, it records that device's location as often as every two minutes, regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. *See* Ex. D (*Chatrie* Tr.) at 436–37, 513. Approximately one-third of all active Google users have Location History enabled on their accounts. Ex. C. at 4; Ex. D at 205. Google has been unable or unwilling to say exactly how many users this was in 2019, but Google acknowledges that it was at least "numerous tens of millions" of people. *Id.*

Google saves Location History data in each user's "Timeline," Ex. C. at 2, which Google describes as a "digital journal" of a user's locations and travels. Ex. B at 16. Google considers this information to be communications "content" for purposes of the Stored Communications Act, 18

U.S.C. § 2703, requiring the government to obtain a warrant to access it. *See id.* Google also uses Location History data to target advertising based on a user's location, although it obscures individual device information, preventing businesses from being able to track individuals. *See* Ex. D at 197.

Neither the Timeline feature nor the advertising relies on a high degree of accuracy. Rather, Location History is merely Google's ***estimation*** of where a device is. Ex. D at 212. It is not hard data, but is instead Google's best guess at device location based on available information. *See* Ex. B at 10–11 n.7 ("In that respect, LH differs from CSLI [Cell Site Location Information], which is not an estimate at all, but simply a historical fact: that a device connected to a given cell tower during a given time period. An LH user's Timeline, however, combines and contextualizes numerous individual location data points …"). As Google puts it, Location History is a "probabilistic estimate," and each data point has its own "margin of error." *Id.* Thus, when Google reports a set of estimated latitude/longitude coordinates in Location History, it also reports a "confidence interval," or "Map Display Radius," to indicate Google's confidence in its estimation. Ex. D at 212, 530–31.

On a map, Google shows the coordinates as a small, solid "blue dot." And it shows the Display Radius as a larger "light blue circle" around the dot. *See* Google, *Find and Improve Your Location's Accuracy*, https://support.google.com/maps/answer/2839911 ("The blue dot shows you where you are on the map. When Google Maps isn't sure about your location, you'll see a light blue circle around the blue dot. You might be anywhere within the light blue circle."). *See* Figure 1.

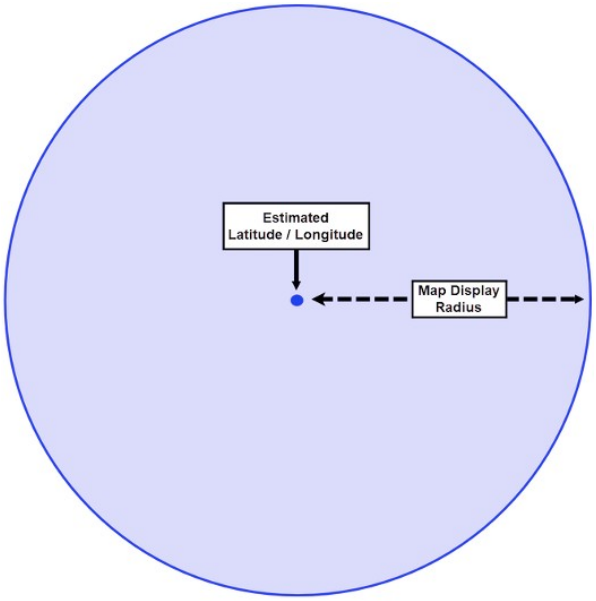

Figure 1

Importantly, Google is equally confident that a device could be anywhere within the Display Radius, *i.e.*, the shaded circle. Ex. D at 214. The estimated coordinates are simply the center point of that circle. It is equally likely that the device is at the center point as anywhere else in the shaded circle, even at the edge. Indeed, Google users may be familiar with this phenomenon, as "in the common scenario of realizing that your cell phone GPS position is off by a few feet, often resulting in your Uber driver pulling up slightly away from you or your car location appearing in a lake, rather than on the road by the lake." *In re Search Warrant Application for Geofence Location Data Stored at Google*, No. 20 M 525, 2020 WL 6343084 at *9 (N.D. Ill. Oct. 29, 2020). The Map Display Radius is not a fixed margin of error; it expands and contracts in accordance with Google's confidence in each location estimation.

Significantly, there is only an "estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot." Ex. C at 8-9. To maintain 68% confidence, Google adjusts the size of the Display Radius. As Google explains, "The smaller the circle, the more certain the app is about your location." Google, *Find and Improve your Location's Accuracy* at 1. By contrast, a large circle means that Google is less confident in a user's location, indicating that they could be anywhere within a much larger area, the product of a larger Display Radius. *See* Ex. D at 213, 530-31. There is always a 32% chance a device is outside of the Display Radius altogether. *See id.* at 213. Or in other words, the odds are almost 1-in-3 that the user's actual location lies beyond the shaded circle.

A confidence interval of 68% is the industry standard, and as Google explains it is "an

[redacted]

approximation sufficient for its intended product uses," namely Timeline and advertising. *See* Ex. D at 581; Ex. G ([redacted] Location History). Because it was not intended to solve crimes, Google warns that its use in geofence warrants risks generating "false positives." Ex. B at 20 n.12. According to Google, "the margin of error associated with LH data means that the government's effort to use this information for purposes for which the LH service was not designed creates a likelihood that the LH data will produce false positives—that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." *Id.*

Google is also clear that it does not use Location History to geotarget ads, and that it does not ever share Location History data with advertisers or other third parties. Ex. D at 198; 367-69. This is done for privacy purposes, so that advertisers do not get to see which devices were in the area. *Id.* at 197, 199. Likewise, advertisers cannot go back to Google and ask for more information about where certain devices were before or after they saw an ad or visited a store. *Id.* at 199. In fact, advertisers cannot get any identifiable information about individual Google users. *Id* . at 199.

1. The Geofence Warrant Application Requested, and the Warrant Authorized, A Three-Step Process for Searching and Seizing Users' Location History Data.

a. Step 1

In Step 1, the warrant directed Google to "query location history data" to identify devices in two locations: 1) the [redacted] Bank, and 2) a point on the [redacted] *Id.* at 3-4. The warrant then directed Google to produce "GPS, Wi-Fi or Bluetooth sourced location history data" from devices that "reported a location within" a 150-meter radius of those two points between 4:45 p.m. and 5:05 p.m. *Id.* at 3-5. It also stated that Google "shall" produce this data in "anonymized" form by specifying the "unique device ID" instead of "identifying information."[1] *Id.* at 5.

The two locations included over 20 private homes, a clubhouse, a grocery store, several

[1] As Mr. [redacted] explains below in Section V, the "unique device ID" is not actually "anonymous" data.

restaurants, a law firm, at least two other banks, a gas station, the entrance to a set of professional buildings, an acupuncture office, the parking lot of a daycare, and a mental health treatment provider that specializes in adults with intellectual disabilities. *See* Figure 2.

Location 1 **Location 2**

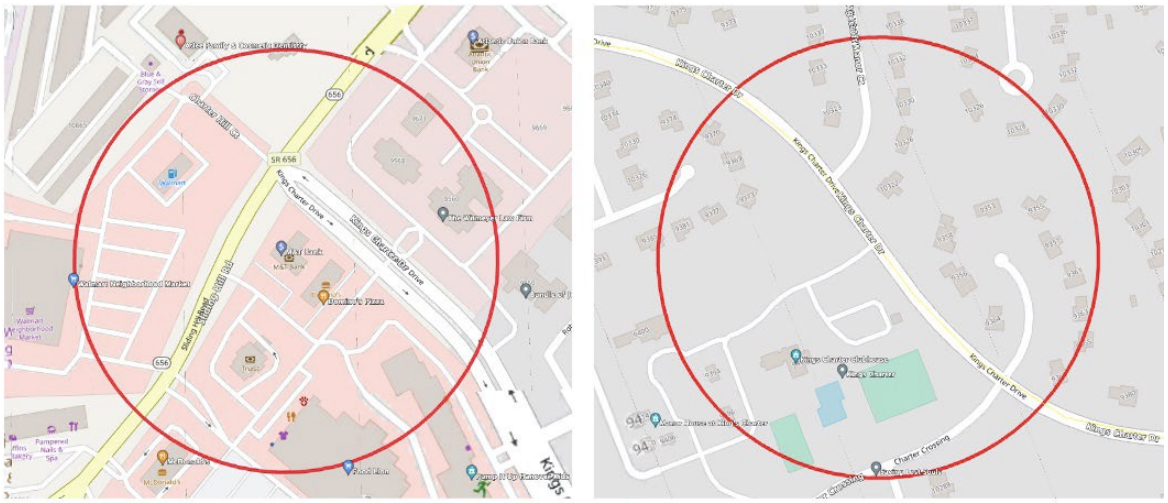

Figure 2

In order to conduct this initial "query," Google was required to search all Google users with Location History enabled, not just those in the area. Thus, Google had to search the "roughly one-third of active Google users (i.e., numerous tens of millions of Google users)" who have Location History enabled. Ex. C at 4. This figure was likely over 500 million in 2019.[2] A geofence warrant requires searching the contents of *every one of these accounts* because there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." Ex. B at 12. Thus, to conduct a geofence search, Google had to "search across all [Location History] journal entries to identify users with potentially responsive data, and then run a computation against every set of coordinates to determine which (Location History] records match the time and space parameters in the warrant." *Id.* at 12-13.

In fact, the geofence warrant required Google to conduct ***two*** searches of "numerous tens

[2] Google said it had over 1.5 billion active users on October 26, 2018, a third of which is 500 million. *See* @gmail, Twitter (Oct. 26, 2018, 9:02), https://twitter.com/gmail/status/1055806807174725633.

of millions" of accounts—one for each location. As a result, to produce the requested records in Step 1, Google had to search the approximately 500 million Google accounts—twice. Discovery reports reveal that it took Google five months to conduct these searches and send the data to the FBI. Mr. [redacted] has requested all communications between Google and the government, which might shed light on the reason for this delay, but the government has yet to produce them.

Google ultimately identified 98 unique Device IDs at Location 1 and 17 unique IDs at Location 2 during the specified timeframe. Three of those IDs appeared at both locations, meaning that there was a total of 112 unique Device IDs identified in this warrant, associated with 111 accounts. The government seized the Step 1 data for these 112 IDs, which contained 352 distinct location points with Display Radii ranging from 3m to 1793m. Figure 3 illustrates these results.

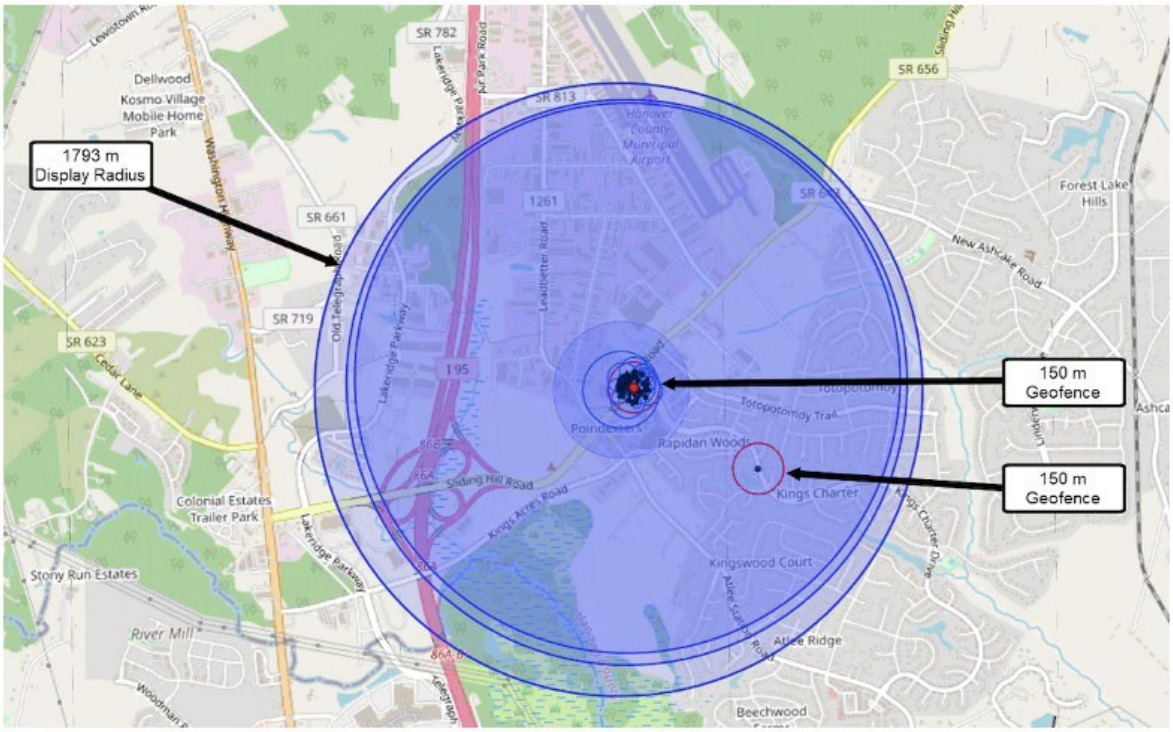

Figure 3

The light blue circles in Figure 3 represent the Display Radius data, meaning that the devices identified as being inside the red geofences were equally as likely (68%) to be anywhere inside the blue circles. They represent the effective range of the geofence data seized at Step 1, and they encompass

[redacted]

an area 71.4 times as large as the area of the two geofence locations put together. The effective range includes: churches; a preschool; pharmacies; a health clinic; a law office; a laser skin removal office; a municipal airport; dance studios; supermarkets; restaurants; construction and home improvement companies; auto repair shops; hundreds of individual homes; and, perhaps obviously, a handful of banks including the one involved here.

b. Step 2

In Step 2, the warrant authorized the government to obtain "additional location coordinates for the Time Period outside of the Target Location." Ex. A at 5. These "contextual location coordinates" sought to track devices outside the geofence described in Step 1, allowing the government to obtain additional location data on devices it deemed "relevant to the investigation." *Id.* at 5. The warrant contained no objective criteria to identify such devices. Instead, the warrant left it up to the FBI to determine whether the additional data to be seized was "relevant." *Id.* at 4.

Here, the FBI seized additional Location History data for six different Device IDs. Two of those six devices were in both locations at Step 1; the FBI did not seek additional information on the third ID. It remains unclear how or why the FBI selected the other four IDs for further scrutiny. It took Google about one month to produce the Step 2 data. The defense has requested, but has not yet received, in discovery copies of all communications between the FBI and Google regarding the warrant that will detail the back-and-forth between Google and the government in this case. Notably, the warrant kept the same "Time Period" in both Steps 1 and 2, limited to 20 minutes around the robbery (4:45 to 5:05 p.m.). But the FBI somehow seized data for all six IDs far beyond that 20-minute window, from 3:45 p.m. to 6:04 p.m.—almost two more hours.

c. Step 3

In Step 3, the government further culled the list and seized from Google the de-anonymized account information for four Device IDs, including the username and subscriber information,

associated email addresses and telephone numbers. *See* Ex. A at 5. Google provided a final file matching each Device ID with its "Gaia ID" as well as records reflecting the associated subscriber information. In this case, the four IDs turned out to be related to just three registered accounts: one for Mr. [redacted] one for another user, and two devices logged into a third Google account. Mr. [redacted] was the only ID in both locations to make it to Step 3. The FBI did not seek Step 3 data on two other IDs reported in both locations. The government has yet to disclose how it determined that those four IDs were relevant to its investigation. Again, the defense has requested, but has not yet received in discovery, copies of communications between the FBI and Google about the Stage 3 returns. Based on the data it obtained from the geofence warrant, the government obtained a warrant for Mr. [redacted] the Google account on [redacted] 2019.

ARGUMENT

The geofence warrant was an unconstitutional search that intruded upon Mr. [redacted] reasonable expectation of privacy in his Google data. For the reasons below, Mr. [redacted] maintains that the warrant was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. The good faith doctrine does not apply, and the warrant was so obviously deficient that it was *void ab initio*. As a result, this Court should suppress the results of the geofence warrant, including all of the fruits thereof.

I. Mr. [redacted] Had a Reasonable Expectation of Privacy in His Location History Data

Mr. [redacted] had a reasonable expectation of privacy in his Location History data following the Supreme Court's landmark decisions in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and *United States v. Jones*, 565 U.S. 400 (2012), because, like CSLI and GPS data, Location History reveals the "privacies of life." *Carpenter*, 138 S. Ct. at 2214. Although this case involves a shorter duration of data, the precision and always-on nature of Location History makes it even more invasive, requiring less to achieve the same effect. Indeed, just a small amount of Location History

[redacted]

can identify individuals inside of their homes and other private spaces. And as a result, a geofence warrant almost always involves intrusion into these constitutionally protected areas, infringing on fundamental privacy interests recognized by the Court in *United States v. Karo*, 468 U.S. 705, 715-18 (1984), and *United States v. Kyllo*. 533 U.S. 27, 37 (2001).

A. Location History Is At Least As Precise as CSLI, Often Has GPS-Quality Accuracy, and Is Highly Intrusive

Location History data, even small quantities, can reveal the "privacies of life" because of its greater precision and frequency of collection. It is at least as precise as CSLI, but it can also be as accurate as GPS. *See* Ex. B at 10. That is because Google uses multiple data sources to estimate a user's location, including CSLI and GPS, as well as Wi-Fi and Bluetooth, which vary in their accuracy. *Id.;* Ex. C at 4. In this case, all the estimated Location History points with known data sources derive from either Wi-Fi or GPS signals, which Google states are "capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." *Id.* Furthermore, Location History logs a device's location as often as every two minutes—regardless of whether any app is open or closed, the phone is in use, or the device is in a public or private space. *Id.* at 436–37, 513.

By contrast, the precision of CSLI "depends on the geographic area covered by the cell site." *Carpenter*, 138 S. Ct. at 2211. This may be sufficient to place a person "within a wedge-shaped sector ranging from one-eighth to four square miles," for example. *Id.* at 2218. As a result, a single CSLI data point could be used to determine which neighborhood or zip code someone was in, but it would not be accurate enough to identify the block and building. Moreover, even though cell phones 'ping' nearby cell sites several times a minute, service providers only log when the phone makes a connection, by placing a phone call or receiving a text message, for example. *Id.* at 2211.

These differences between Location History and CSLI are significant because they affect how much data is needed to infer where someone was and what they were doing. While *Carpenter* anticipated

that the precision of CSLI would improve, *id.* at 2218-19, the Court also faced technology that required stitching together some minimum amount of CSLI to reveal the "privacies of life." The Court settled on seven days, but this was not a magic number; it was simply the timespan for the shortest court order in the record. *See id.* at 2266-67 (Gorsuch, J., dissenting). In fact, that order only produced *two* days of CSLI. *Id.* at 2212. *Carpenter* explicitly declined to say "whether there is any sufficiently limited period of time for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *Id.* at 2217 n.3. But short-term searches may still be capable of revealing the "privacies of life," *id.* at 2214, which was the main concern in both *Carpenter* and *Jones*.

Although *Jones* and *Carpenter* involved so-called "long-term" searches, what motivated the Court in each case was the risk of exposing information "the indisputably private nature of which takes little imagination to conjure: the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones,* 565 U.S. at 415 (Sotomayor, J., concurring) (internal quotation omitted); *accord Carpenter*, 138 S. Ct. at 2215. Thus, "[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance . . . will require particular attention." *Jones*, 565 U.S. at 415. The same is true for the data here, given that "[a] cell phone faithfully follows its owner beyond public throughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218.

Before *Jones* and *Carpenter*, the Court was concerned with short-term location tracking, especially when it reveals information about a private interior space. In *Karo*, using an electronic beeper to track an object inside a private residence was a search. 468 U.S. at 716. In *Kyllo*, using a thermal imaging device to peer through the walls of a private residence was a search despite taking "only a few minutes" and not showing people or activity inside. 533 U.S. at 30, 37.

Location History's greater precision and frequency of collection means that less time is needed

[redacted]

to reveal the "privacies of life." It might take days of CSLI to piece together a mosaic with enough detail to be so revealing, but it takes just a little Location History to achieve the same end. In this case, the data was more than sufficient to reveal individuals in private homes connected to their WIFI, at the address of a mental health treatment provider, an unrelated bank, and an office park that included a law firm, medical billing company, and acupuncture provider. Although Google initially "anonymized" this data, the FBI could have obtained the subscriber information at any time using a subpoena. *See Matter of Search of Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 749 (N.D. Ill. 2020) ("Fuentes Opinion"). Others who have considered geofence warrants have also recognized the private nature of Location History data. *See* Fuentes Opinion, 481 F. Supp. 3d at 737 ("[T]here is much to suggest that *Carpenter*'s holding, on the question of whether the privacy interests in CSLI over at least seven days, should be extended to the use of geofences involving intrusions of much shorter duration."); *Matter of Search of Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *5 n7 (N.D. Ill. July 8, 2020) ("Weisman Opinion") ("The government's inclusion of a large apartment complex in one of its geofences raises additional concerns … that it may obtain location information as to an individual who may be in the privacy of their own residence").

The *en banc* Fourth Circuit also recently confronted a similar retrospective location tracking scheme, and held that citizens whose locations were recorded had a reasonable expectation of privacy. *Leaders of a Beautiful Struggle v. Baltimore Police Dept.* involved a police-contracted surveillance program in which planes flew over Baltimore continuously, capturing high-resolution photographs that depicted over 32 square miles for 12 hours a day. 2 F.4th 330, 334 (4th Cir. 2021). The images were kept for 45 days. *Id.* During that time, when a crime occurred, police could review photographs from the area, and then, just as with a geofence warrant, track individuals and compile reports with images. *Id.* These "tracks" were "often shorter snippets of several hours or less." *Id.* at 342.

The Fourth Circuit held that "*Carpenter* applies squarely to this case" because the data allowed

police to "travel back in time" to observe a target's movements, as if they had "attached an ankle monitor" to every person in the city. *Id.* at 341. This "'retrospective quality of the data' enables police to 'retrace a person's whereabouts,' granting access to otherwise 'unknowable' information." *Id.* at 342. Google location history is far more intrusive than the pixilated surveillance photos in *Leaders*. In fact, Location History data is even more intrusive than aerial surveillance photos, because it records movements *inside* as well as outside, including in private homes. And Location History data can stretch back months or years, for as long as the service has been enabled. Thus, under *Leaders,* as well as *Carpenter*, *Jones*, *Karo*, and *Kyllo*, Mr. [redacted] had a reasonable expectation of privacy in his data.

B. The Third-Party Doctrine Does Not Apply

The so-called "third-party doctrine" does not foreclose finding an expectation of privacy in Location History data. The Supreme Court has never sanctioned a warrantless search of an individual's cell phone location data, let alone the search of millions at once. *See* 138 S. Ct. at 2219 (noting that the Court has "shown special solicitude for location information in the third-party context"). Indeed, the *Carpenter* Court declined to extend the third-party doctrine to similar data and instructed lower courts not to "mechanically" apply old rules to new technologies. *Id.*

To begin with, Location History is not an "invited informant" as in *Hoffa v. United States*, 385 U.S. 293, 302 (1966)). Likewise, Location History is not a "business record," as in *Smith v. Maryland*, 442 U.S. 735 (1979). And Location History is not a "negotiable instrument," as in *United States v. Miller*, 425 U.S. 435, 438 (1976). All of these "third-party doctrine" cases involved situations where individuals were actively aware that they were interacting with another person or business. Here, by contrast, Location History was likely enabled without Mr. [redacted] even realizing it—meaning he would have had no awareness that it was on, silently recording, every two minutes. He would not have known Location History was enabled, let alone how much data was being collected or how to manage it. There would have been no monthly bill to remind him, unlike the digits dialed in *Smith*. *See* Ex. B at

22. And there would have been no deposit slip or receipt from the bank. Rather, Location History data is most like the CSLI at issue in *Carpenter*, in which the Supreme Court found the third-party doctrine inapplicable.

Moreover, Mr. [redacted] did not "voluntarily" convey his Location History data to Google in a meaningful way. Although Location History must be enabled by the user, the process of doing so is unlikely to have been knowing or informed, but perfunctory at best and deceptive at worst. Mr. [redacted] does not yet have information about when Location History was enabled on his account or how. Nonetheless, Mr. [redacted] is aware that in the years preceding the warrant, it was possible to enable Location History in multiple ways, including during the initial setup of a cell phone or during the first use of certain Google applications or services. If enabled in this fashion, a user would have seen one line of text about Location History in a pop-up screen.

One iteration told users that it "Creates a private map of where you go with your signed in devices." Ex. I at 4. A later version said that Location History "Saves where you go with your devices." Ex. J at 19. This was the only text a user would have been required to read, and it was not only inadequate, but outright confusing. Additional information was available on another screen with "copy text," but users would have had to actively seek it out. Even then, what little else Google said about Location History did not adequately convey how it functioned.

First, it was not clear that location data would be saved by Google, as opposed to stored locally on the device. A user might reasonably infer that this "private map" or saved data would be saved only on their device, not with Google. Ex. D at 301, 346 (descriptive text does not make a "distinction" as to whether location information is saved on-device or on Google servers). In fact, that is how certain personalized features work on Apple Maps, available on Apple iPhones. *See* Apple, *Privacy*, https://www.apple.com/privacy/features/ (describing how certain personalized features on Apple Maps "are created using data on your device" to "help[] minimize the amount of data

sent to Apple servers"). Unless a user actively clicked the small "expansion arrow" on the other side of the screen from "Location History," there would be no indication that the data is saved in the cloud on Google's servers. *See* Ex. D at 110,330.[3]

Second, nothing explained that Location History will operate independently, regardless of whether the phone is in use. This is in stark contrast to the facts in *Smith v. Maryland*, where phone users often had to interact with telephone operators using switching equipment to make calls. *See* 442 U.S. at 742. Here, Mr. [redacted] could have enabled Location History by accident well before December 2018. Even if he never again engaged with Google's "location-based services," or any other Google service, Location History would track his location at all times, even while he slept.

Finally, Google's Privacy Policy or Terms of Service have little if any bearing on an individual's Fourth Amendment expectations of privacy. *See 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 even though Facebook informed users that it collects user information). That is because Fourth Amendment rights do not rest on the terms of a contract. *See United States v. Byrd*, 138 S. Ct. 1518, 1529 (2018) (recognizing that drivers have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement). As the Court said in *Smith*, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." 442 U.S. at 745. Otherwise, by "choosing" to

[3] Additional language may also appear at the bottom of the screen, away from the Location History "descriptive text," and in lighter font. There are two potential versions of this language, *see supra* at 11-12, but both state that this "data may be saved" and that "You can see your data, delete it and change your settings at account.google.com." *Id.* Neither version mentions Location History or location data, nor gives any indication of what it is, let alone that the phone will begin to transmit its location to Google every two minutes in perpetuity, or that this information may be available to the government.

[redacted]

live in the digital age and to participate in the digital world, an individual would be forfeiting any right to privacy in their effects. Such a state of affairs cannot stand when "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 138 S. Ct. at 2214 (quoting *United States v. Di Re,* 332 U.S. 581, 595 (1948)).

As in *Carpenter*, the question is not whether there was an agreement between an individual and a service provider. The question is whether, in a "meaningful sense," users "voluntarily 'assume[] the risk' of turning over a comprehensive dossier of [their] physical movements" to the government. *Carpenter*, 138 S. Ct. at 2220. And in the case of Location History, Google's pop-ups and terms of service do not suffice to extinguish users' privacy interest in their account data.

II. Mr. [redacted] Had a Property Interest in His Location History Data

Mr. [redacted] also had a property interest in his Location History data, the digital equivalent of his private "papers and effects." U.S. Const. Amend. IV. Google was a mere bailee of Mr. [redacted] data, and the government converted his property interest in his data through its search and seizure. Supreme Court jurisprudence has long adhered to—and continues to validate—a property-based understanding of the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2213-14 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *Jones*, 565 U.S. at 406-07 ("For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."); *id.* at414 ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.") (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 40 ("well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass"). Most recently, in his dissenting opinion in *Carpenter*, Justice Gorsuch opined that under a "traditional approach" to the Fourth Amendment, the protection against unreasonable searches and seizures applied as long as "a house, paper or effect was yours under law." *Id.* Justice

[redacted]

Gorsuch drew a strong analogy between cell phone location data and mailed letters, which have had an established Fourth Amendment property interest for over a century, whether or not they are held by the post office. *Id.* at 2269. Just as Gmail messages belong to their senders and recipients (and not to Google), so too does Location History data belong to the users who generate them. *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010); *see also* Michael J. O'Connor, *Digital Bailments*, 22 U. Pa. J. Const. L. 1271, 1309 (2020) ("Founding sentiment, courts, and scholars all agree: Yes, digital documents are indeed the same papers, even if they use new and unfamiliar ink.").

Mr. [redacted] location information belongs to Mr. [redacted] Google may be responsible for collecting and maintaining it, but Google also understands that it is private user data. For example, Google's privacy policy in effect at the time that Mr. [redacted] created his account consistently refers to user data as "your information," which could be managed, exported, and even deleted from Google's servers at "your" request. *See* Ex. E (May 2018 Google privacy policy). Google even 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 his or her records after death, or in the alternative whether Google should delete the data. *See* Ex. F.

These are not "business records." Businesses do not let customers export or delete the company's records at will. Mr. [redacted] merely entrusted his information to Google. The data is heritable, alienable, and exclusive—classic attributes of property. In short, it is Mr. [redacted] (and millions of other citizens') "papers" under the Fourth Amendment, held in trust by Google. As Justice Gorsuch explained in *Carpenter*, "[e]ntrusting your stuff to others is a bailment. A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'" 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting). Here, Google is the bailee, and it owes a duty to the bailor, Mr. [redacted] to keep his data safe. While Google reserves the right to use the data for advertising or development purposes, it also promises not to disclose it to "companies,

[redacted]

organizations, or individuals outside of Google," subject to a short list of explicit exceptions.[4] In other words, Mr. [redacted] retains the right to exclude others from his location data, a quintessential feature of property ownership. *See* William Blackstone, 2 Commentaries on the Laws of England *2 (1771) (defining property as "that sole and despotic dominion … exercise[d] over the external things … in total exclusion of the right of any other."); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) (calling the right to exclude "one of the most treasured strands" of the property rights bundle); *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979). The government converted this interest and thus committed a search and seizure under the Fourth Amendment, frustrating Mr. [redacted] right to exclusivity and control over his Location History data.

III. The Warrant Was Overbroad

The geofence warrant here entailed two massive searches of all Google users who had Location History enabled on their devices. Step 1 was an epic dragnet, conducted by Google at the government's direction. The FBI commandeered Google to search through millions of private accounts to determine if any of them contained data of interest. The warrant was therefore unconstitutionally overbroad, a modern-day general warrant. And as if that was not sufficient, the FBI somehow found a way to exceed its scope, seizing an additional two hours of Location History data in Step 2, for which it had no authorization whatsoever.

A. Step 1

Overbreadth concerns probable cause, which is defined as "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates* 462 U.S.

[4] One of these exceptions is "For legal reasons," but – like attorneys' records, the contents of a bank deposit box, or other bailments, this is not a free pass to hand over user data to law enforcement. It is implied that legal process must be valid, which includes establishing probable cause and following the strictures of the Fourth Amendment, not just submitting the proper form. *See, e.g.,* Jim Harper, *The Fourth Amendment and Data: Put Privacy Policies in the Trial Record*, The Champion, Jul. 2019, at 21.

213, 238 (1983). And it is axiomatic that a warrant may not authorize a search or seizure broader than the facts supporting its issuance. *See Veeder v. United States*, 252 F. 414, 418 (7th Cir. 1918). Here, however, the government did not have probable cause to search millions of Google accounts. It did not have probable cause to search 112 accounts, six accounts, or even one account. Indeed, it is difficult to imagine that any amount of probable cause could justify a search of "numerous tens of millions" twice over. But in this case, the government had none.

That is because probable cause requires a logical connection, or evidentiary "nexus" between the crime for which probable cause exists and the evidence to be seized, which the government did not demonstrate. *See United States v. Lyles*, 910 F.3d 787, 795 (4th Cir. 2018); *see also* LaFave, 2 Search and Seizure (6th Ed.), § 3.7(d). And according to the Fourth Circuit, this means a nexus between the alleged crime and any phone that is the subject of a warrant. In *Lyles*, for example, the government obtained a warrant to search a house for items including cell phones. 910 F.3d at 790-91. But the Fourth Circuit (Judge Wilkinson, writing for the Court), held the warrant invalid because:

> the warrant application lacked any nexus between cell phones and marijuana possession. There is insufficient reason to believe that any cell phone in the home, no matter who owns it, will reveal evidence pertinent to marijuana possession simply because three marijuana stems were found in a nearby trash bag. At some point an inference becomes, in Fourth Amendment terms, an improbable leap.

Id. at 795. As in *Lyles*, the warrant application here provided no case-specific facts that the robber had a cell phone, was a Google user, or had Location History enabled at the times in question. The affidavit did not allege, even inferentially, that the robber used or possessed a cell phone or acted in concert with anyone else. Ex. A at 12, ¶16. Instead, the application offers only generalizations that when people commit crimes "in concert," they use cell phones to coordinate; and that criminals often take pictures of contraband. Ex. A at 12-13, ¶18. Yet the robbery as alleged was not committed "in concert" with anyone else; the government has only ever alleged that one person was involved in the

robbery. Moreover, the government provides no reason to think that ***photos*** saved on a phone would have anything to do with Location History data stored in a Google account.

Broad conjecture does not amount to probable cause. Probable cause must be based on individualized facts, not group probabilities. *See Ybarra v. Illinois* 444 U.S. 85, 91 (1979). For this reason, the D.C. Circuit struck down a warrant authorizing the search of all cell phones in a house, finding that the affidavit "conveyed no reason to think that [the suspect], in particular, owned a cell phone" and no "reason to believe that a phone may contain evidence of a crime." *United States v. Griffith* 867 F.3d 1265, 1272-74 (D.C. Cir. 2017). And in Illinois, Judge Fuentes denied a geofence application on similar grounds. *See In re Information Stored at Premises Controlled by Google* (N.D. Ill. 2020) 481 F. Supp. 3d 730, 754. As here, Judge Fuentes found that 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. Id.*

Boilerplate assertion that criminals use phones to commit crimes "'cannot substitute for the lack of evidentiary nexus'" between the particular crime for which probable cause exists and the evidence sought. *United States v. Ramirez*, 180 F. Supp. 3d 491, 495 (W.D. Ky. 2016) (quoting *United States v. Schultz*, 14 F.3d 1093, 1097 (6th Cir.1994)). An officer's training and experience is, of course, relevant to whether an affidavit establishes probable cause. But profile evidence must describe both the characteristics of the type of person that commits the asserted crime, and facts that fit the subject of the search into that profile. For example, this Court held that an officer's affidavit describing in detail the typical practices of drug dealers and alleging relevant facts (three phones in car where common cutting agent found) sufficed to establish a nexus between the phones and the crime. *United States v. Peterson*, 2019 WL 1793138, *12 (E.D. Va. 2019). By contrast, the affidavit here does not discuss the typical practices of bank robbers, or even robbers, or even robbery-related crimes. Instead, it generalizes to, quite literally, all crimes.

From the outset, the government enlisted Google to search untold *millions* of unknown accounts in the largest type of fishing expedition in Fourth Amendment history. The number of individuals affected by this case dwarfs the number of people searched in any other reported criminal opinion. The fact that Google produced records for 112 Device IDs in Step 1 does not diminish the scope of the initial search conducted at the government's behest. On the contrary, it illustrates just how broad the search really was.[5] Unlike scenarios where a company must search defined records to identify responsive data, the search here did not identify any specific users or accounts to be searched. Instead, the warrant forced Google to act as an adjunct detective, scouring the accounts of "numerous tens of millions" of users to generate a lead for the government. In short, Step 1 compelled a search of the intimate, private data belonging to millions, in a digital dragnet that snared 112 Device IDs, the data for which the FBI then seized—all without probable cause to search or seize data from a single account. Step 1 was a massive fishing expedition, fatally overbroad from the beginning.

B. Steps 2 & 3

Steps 2 and 3 fare no better. Following Step 1, the government still lacked probable cause to search or seize the Location from a single account (let alone two times "numerous tens of millions"). In Step 2, the government also overstepped the bounds of the warrant itself by seizing nearly 2 hours of additional Location History data for six Device IDs without authorization.

Step 2 allowed the government to seize Location History data beyond the geographic limits of the two 150-meter geofences. However, it only permitted the FBI to do so "for the Time Period" identified in Step 1, *i.e.*, the 20 minutes from 4:45pm to 5:05pm. Ex. A at 4 (". . . provide additional location coordinates for the Time Period that fall outside of the Target Location."). That is not what

[5] Assuming that Google had at least 1.5 billion active users in 2019, a third of which had Location History enabled (500 million) and whom the government searched twice (1 billion), then 112 responsive Device IDs represents a miniscule hit rate of 0.0000112%. In fact, it is even less considering that two Device IDs belonged to one account, meaning 111 accounts were responsive.

happened. Instead, the government seized the data for six Device IDs for a span of 2 hours and 19 minutes, from 3:45 p.m. until after 6:04 p.m., almost 2 hours more data than the warrant authorized. Figure 4 shows the first and last entries in the Step 2 data seized:

	A	B	C	D	E	F	G	H
1	Device ID	Date	Time (America/New_York -05:00)	Latitude	Longitude	Source	Maps Display Radius (m)	
2	[redacted]	[redacted]/2018	15:45:07 (-05:00)	[redacted]	[redacted]	GPS	3	
568	[redacted]	[redacted]/2018	18:01:27 (-05:00)	[redacted]	[redacted]	WIFI	30	

Figure 4

The Step 2 seizure was literally unwarranted and should be treated as such. The seizure of evidence not named in a warrant must be treated as a warrantless seizure. *See Horton v. California*, 496 U.S. 128 (1990) (analyzing warrant for robbery proceeds, seizure of firearms and other evidence of robbery as warrantless seizure under plain view exception). Mr. [redacted] had a Fourth Amendment interest in his Location History data, and no warrant exception applies. On the contrary, the government exhibited a "flagrant disregard" for the terms of the warrant. *United States v. Ruhe*, 191 F.3d 376, 383 (4th Cir. 1999). The timeframe was clear, and the government clearly disregarded it. Suppression of the entire warrant return and its fruits is therefore justified. *Ruhe*, 191 F.3d at 383-84.

Step 3 allowed the government to seize additional identifying information about four Device IDs that the FBI selected from the data it obtained in Steps 1 and 2. Once again, the warrant application did not demonstrate probable cause to search or seize this data. And the government cannot bootstrap its way to probable cause by relying on information it obtained unlawfully in Steps 1 and 2. In fact, Step 3 was a farce. The government could have obtained the subscriber information for any Device ID identified in Steps 1 and 2 simply by issuing a subpoena to Google. *See* Fuentes Opinion, 481 F. Supp. 3d at 749 (finding "no practical difference between a warrant that harnesses the technology of the geofence, easily and cheaply, to generate a list of device IDs that the government may easily use to learn the subscriber identities, and a warrant granting the government unbridled discretion to compel Google to disclose some or all of those identities."). Indeed, the government has

previously argued that such warrants allow them to seize Step 2 and Step 3 data for *all* devices from Step 1. *See United States v. Chatrie*, 3:19cr130, ECF No. 207-2 at 38-39 (E.D. Va.). As a result, the entire 3-step process is superfluous, including the purported anonymization. All that remains is a search that was fundamentally and thoroughly overbroad, lacking in probable cause for the data it authorized the FBI to seize, and executed without regard for the minimal limitations it proffered.

IV. The Warrant Lacked Particularity

The Fourth Amendment's requirement that warrants "particularly describe[e] . . . the things to be seized," U.S. Const. Amend. IV, means that the description of "what is to be taken" can leave "nothing . . . to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Stanford v. Texas*, 379 U.S. 476 (1965). The description must be provided or confirmed by a "detached" magistrate, "instead of being judged by the officer engaged in the often-competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 13-14 (1948). A magistrate issuing a warrant cannot "assign[] judicial functions to the executive branch." *In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 176 (4th Cir. 2019). The warrant here violates the particularity requirement by delegating discretion at each step to Google and the FBI, not a judge, to answer basic critical questions.

A. Step 1

Step 1 fails the particularity requirement because it does not specify the accounts to be searched and the data to be seized. Instead, it concocted a three-step process to mask that is actually searching "numerous tens of millions" of accounts (twice). It also left it to Google and the government to determine whether devices were "within" the geofences.

i. The Warrant Did Not Adequately Identify the Accounts to Be Searched

Geofence warrants differ from other types of police requests. Typical requests compel Google to disclose information for a specific user, while "[g]eofence requests represent a new

[redacted]

and increasingly common form of legal process that is not tied to any known person, user, or account." Ex. B at 11. Here, the warrant did not identify Mr. [redacted] Nor did it identify any of the individuals whose personal information was searched and turned over to the FBI. Instead, the warrant operated in reverse: it required Google to search all accounts with Location History enabled—*i.e.*, "numerous tens of millions"—a portion of which was then seized.

To be sure, there are circumstances where the government need not identify the name of the individual whose information is to be searched and seized. But this is not one of them. So-called "John Doe" warrants—warrants that do not expressly identify the person to be searched or arrested—require something more. To comply with the Fourth Amendment, they must provide "a particularized description of the person to be arrested . . . on the face of the 'John Doe' warrant." *United States v. Jarvis*, 560 F.2d 494, 497 (2d Cir. 1977) (citing *West v. Cabell*, 153 U.S. 78, 86 (1894)).

"All persons" warrants, which aim to search and/or seize all individuals who happen to be at a location during a search—require much more: "probable cause to believe that ***all*** persons on the premises at the time of the search are involved in the criminal activity." *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276 (4th Cir. 2004). Here, the government has not alleged any good reason to suspect or believe that all persons present within the 150-meter radius was guilty of committing the robbery. As in *Owens*, such "all persons" language is insufficient if it is "based on nothing more than their proximity to a place where criminal activity *may or may not* have occurred." *See id.* at 276-77.

Finally, anticipatory warrants, which rely on a triggering condition not yet met at the warrant's issuance, require at least more than being in the wrong place at the wrong time. *See United States v. Grubbs*, 547 U.S. 90, 96-97 (holding anticipatory warrants must satisfy two prerequisites—1) "*if* the triggering condition occurs 'there is a fair probability that contraband or evidence of a crime will be found in a particular place'"; and 2) "there is probable cause to believe the triggering condition *will occur*"—to meet the Fourth Amendment's probable cause requirement); *see*

[redacted]

also United States v. McLamb, 880 F.3d 685, 688 (4th Cir. 2018) (noting that in order to access a child pornography website running FBI malware, a user had to download special software and enter a 16-character URL consisting of random letters and numbers, as well as a username and password).

The warrant here contained no names, and it contained no particularized description of the accounts to be searched and seized. There was no basis to conclude that all 98 of the devices identified in Step 1 were involved in the bank robbery. There was no triggering condition to cabin officer discretion. The warrant simply failed to adequately identify any accounts and thus lacked the particularity required by the Fourth Amendment.

ii. The Warrant Did Not Adequately Identify the Data to Be Seized

Step 1 failed to provide clear instructions on what could be seized. The warrant left it up to Google and the government to decide which users would have their account information handed over to the FBI—the hallmark of an unparticularized warrant. *See Steagald v. United States*, 451 U.S. 204, 220 (1981); *Stanford v. Texas*, 379 U.S. 476, 482-83 (1965) (describing the "battle for individual liberty and privacy" as finally won when British courts stopped the "roving commissions" given authority "to search where they pleased"). Furthermore, in doing so, the warrant ensnared people who had nothing to do with the robbery.

Step 1 returned devices with Map Display Radii that far extended beyond the geofence, making it at least equally as likely that those devices were outside the geofence. *See* Figure 3. Moreover, because Google only aims to be 68% confident in the Map Display Radius, there was a 32% chance that those devices were even farther afield. This situation, as Google explains, "creates a likelihood [of] false positives—that is, that it will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there." Ex. B at 20 n.12.

Not only did the government not inform this Court of that likelihood, *see infra* Section V, it also exploited it to increase the amount of data seized. The warrant says Google shall produce

[redacted]

data for "each location point recorded within the Initial Search Parameters." Ex. A at 5. But it does not specify how to determine whether a device is "within" those parameters. Because Location History is only an estimation of where a device was, determining the devices "within" a geofence is much more complicated and open to interpretation than the warrant makes it appear. Determining who is "within" a geofence involves a choice, made without judicial oversight and approval, about whose data gets seized. The government was aware of this fact and stayed silent, leaving it up to Google and investigators to work out among themselves, without input from a judge.

As is apparent from Figure 3, there are very real and measurable consequences to the choice of how to count devices within the geofences here. Although the government may claim that the geofence boundaries limit their discretion, the reality is that Google and the government decided to read the warrant in way that produced data on devices that were as likely to be within 150 meters of the bank as they were to be a mile away. One device had a Display Radius of 1,793 meters (1.1 miles); another had 1,660 meters (1.03 miles); and a third had 1,616 meters (1 mile). *See* Ex. H (Step 1, Location 1 Data). Consequently, the effective range of the warrant was not 150 meters, but 1,793 meters, meaning that at least one device was 68% likely to have been anywhere within 1,793 meters, an area is 71.4 times larger than the two geofences combined.

B. Steps 2 & 3

Steps two and three of the warrant *explicitly* gave the FBI discretion to determine which Google users will be subject to further scrutiny. Step two said: "If additional information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the Time Period that fall outside of the Target Location." Ex. A at 5. This means that the FBI was responsible for identifying what was "relevant" and what else to seize. Here, the FBI identified Mr. [redacted] data as "relevant," and without returning to the court for additional authorization.

[redacted]

And what's more, the FBI somehow obtained an additional two hours of his Location History data in the process, including similar data for five other devices.

In Step 3, the FBI had the opportunity to identify "relevant" accounts, for which Google was required to provide subscriber information, including the account holder's name, email address, and phone number. The warrant stated: "For those device IDs identified as relevant . . . law enforcement may request that Google Provide identifying information . . . for the Google Account associated with each identified device ID." *Id.* at 5. Once again, the warrant left it up to the FBI, not a judge, to determine whose data to seize. This is precisely the kind of officer discretion that the particularity requirement was designed to prevent. *See In re Information Stored at Premises Controlled by Google,* 481 F. Supp. 3d at 754 (finding a geofence warrant lacked particularity because it "puts no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information"); *In re Information Stored at Premises Controlled by Google*, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020) ("[T]his multi-step process simply fails to curtail or define the agents' discretion in any meaningful way.").

The Fourth Amendment does not "countenance open-ended warrants, to be completed while a search is being conducted and items seized[.]" *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979). The Warrant Clause requires the determinations of probable cause and particularity be made *ex ante* by a "neutral and detached judicial officer," and not through "the hurried judgment of a law enforcement officer engaged in the often competitive enterprise of ferreting out crime." *Id.* at 326. In Steps 2 and 3, the warrant explicitly empowered officers to determine whose and what data was subject to seizure. But the Fourth Amendment cannot sustain such a warrant because it lacks particularity.

V. The Good Faith Exception Does Not Apply

The Fourth Amendment's most fundamental restraint is the warrant requirement. In *United States v. Leon*, 468 U.S. 897, 919 (1984), the Supreme Court qualified that restraint where a warrant is

based on "objectively reasonable law enforcement activity." But, *Leon* "good faith" offers no qualifications in four circumstances: (1) where a warrant is based on knowing or recklessly false statements, *id.* 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 288); (3) where a warrant affidavit lacks a substantial basis to determine probable cause, *id.* at 915 (citing *Gates*); and (4) where no officer could reasonably presume the warrant was valid, *id.* at 923.

The Supreme Court tethered the exclusionary rule to the primary tenets of the Fourth Amendment: particularity, probable cause, and a neutral magistrate who is "not [an] adjunct[] to the law enforcement team." *Id.* at 917, 923. The *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. As set forth above, this geofence warrant is void from its inception and is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh v. Ramirez*, 540 U.S. 551, 558 (2004) ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law."). But, even if the Court determines that *Leon* applies here, three of the firm boundaries to the good faith rule that *Leon* recognized clearly apply.

First, the good faith exception should not apply because the geofence warrant was "so lacking in indicia of probable cause" to search for Mr. [redacted] data that it was entirely unreasonable for any objective officer—*i.e.*, one with even a rudimentary understanding of the Fourth Amendment's requirements—to rely on. *See Leon*, 468 U.S. at 923. Police must demonstrate a fair probability that the evidence the police seek will be where they are searching. *See United States v. Doyle*, 650 F.3d 460, 472 (2011) (rejecting good-faith exception where warrant application contained "remarkably scant evidence . . . to support a belief that [the defendant] *in fact* possessed child pornography"); *see also United States v. Church*, 2016 WL 6123235, at *6-7 (E.D. Va. Oct. 18, 2016) (observing that good-faith exception inappropriate where no evidence to connect suspect's house to the crime under

investigation); *United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013). That did not happen here. Rather, the police obtained a warrant based on conjecture that Google had location data for a robbery suspect—a suspect the police had no evidence had a cell phone, let alone one with a Google account that had Location History enabled. Obtaining warrants based on conjecture is certainly not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

Second, the good faith exception should not apply because the geofence warrant was "facially deficient" and no objective officer could reasonably presume it was valid. *See Leon*, 468 U.S. at 923. As set forth above, "it is obvious that a general warrant authorizing the seizure of 'evidence' without [complying with the particularity requirement] is void under the Fourth Amendment" and "is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise." *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992); *see also United States v. Leary*, 846 F.2d 592, 607-09 (10th Cir. 1988) ("reasonably well-trained officer should know that a warrant must provide guidelines for determining what evidence may be seized," and collecting like cases).

Third, the warrant application is riddled with false and misleading statements and is severely compromised by material omissions that would have informed the reviewing judge about the effects of authorizing such a warrant. In *Franks*, the Supreme Court observed: "When the Fourth Amendment demands a factual showing sufficient to comprise 'probable cause,' the obvious assumption is that there will be a truthful showing." (original citation omitted). 438 U.S. at 164-65. Where a substantial preliminary showing demonstrates that an affiant made material, false statement with reckless disregard for the truth, the Court must determine whether to strike those portions of the application and if so, whether the remaining content establishes probable cause. *Id.* At 155-56. In considering the veracity of the affidavit in support of the search warrant, the Court must also consider omissions that the affiant made with reckless disregard for the truth. *See United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990); *United States v. Tate*, 524 F.3d 449, 455 (4th Cir. 2008).

[redacted]

Here, the application says nothing about the numerous tens of millions of accounts to be searched, that the effective radius of the geofence would extend well beyond the authorized 150 meters, that the geofence would capture devices outside of the geofence, or that the approximate device locations were only an estimated 68% accurate. The warrant also falsely claimed that the information returned would be anonymous. Ex. A at 4. While the identifying Device ID is a number rather than a name, it takes little effort to identify an individual person through just a few location points. *See* Ex. D at 62-70; Ex. K (finding in study of 1.5 million people that four location points were enough to identify 95% of individuals in the study). The Device ID also remains the same from warrant to warrant, meaning that the police know who that person is from warrant to warrant. Ex. D at 451-54. This level of omission and misinformation only underscores that the geofence warrant in this case was not "objectively reasonable law enforcement activity." *See Leon*, 468 U.S. at 919.

The government cannot argue it did not understand how this warrant would work because the basic contours of a geofence warrant came from repeated discussions between Google and the Computer Crimes and Intellectual Property Section ("CCIPS") of the Department of Justice in 2018. Ex. D at 456-57 ("CCIPS is an agency that . . . our counsel engages with to discuss sort of certain procedures that may be relevant for the way that . . . Google will need to handle these types of requests"); *id.* at 476 (noting repeated "engagement" between CCIPS and Google "help[ed] to socialize the concept of these types of warrants"); *id* at 552-53. The Justice Department even provided "go-by" language to local law enforcement agencies for use in plug-and-play geofence warrant applications. *Id.* at 552-553. For any of these reasons, the Court cannot find that the good-faith exception applies to evidence obtained from the geofence warrant and the fruits flowing therefrom.

CONCLUSION

Thus, Mr. [redacted] moves this Court to suppress the warrant returns as well as their fruits.

[redacted]

Respectfully Submitted,

[redacted]

By: /s/

Laura Koenig
Va. Bar No. 86840
Office of the Federal Public Defender
701 E. Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
Laura_koenig@fd.org

/s/

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

SUPREME COURT, STATE OF COLORADO Colorado State Judicial Building 2 East 14th Ave., Denver, CO 80203	
Denver District Court, Div. 5A Honorable Judge Egelhoff Case Number 21CR20001	DATE FILED: January 11, 2023 11:10 AM FILING ID: 89D918329A1B7 CASE NUMBER: 2023SA12
PEOPLE OF THE STATE OF COLORADO, Plaintiff, v. GAVIN SEYMOUR, Juvenile Defendant.	☐ COURT USE ONLY ☐
JENIFER STINSON (#35993) Alternate Defense Counsel Stinson Law Office 1245 E. Colfax Avenue, Suite 300 Denver, Colorado 80218 Phone: (303) 483-3161 E-mail: JStinsonLaw@gmail.com MICHAEL JUBA (#39542) Alternate Defense Counsel The Juba Law Office, PLLC 675 N. Grant Street Denver, CO 80203 Phone: (303) 974-1080 E-mail: Juba@JubaLawOffice.com MICHAEL W. PRICE (#22PHV6967) National Association of Criminal Defense Lawyers 1660 L Street NW, 12th Floor Washington, DC 20036 Phone: (202) 465-7615 E-mail: MPrice@NACDL.org	Case Number:
IN RE: PEOPLE OF THE STATE OF COLORADO V. GAVIN SEYMOUR	

CERTIFICATE OF COMPLIANCE

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

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

☒It contains 24,630 words (principal brief does not exceed 9,500 words; reply brief does not exceed 5,700 words).

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

Michael S. Juba, Atty Reg. #39542

Identity of the Parties:

1. This Court has original jurisdiction pursuant to C.A.R. 21(a). Gavin Seymour is the Petitioner-Juvenile Defendant. The proposed Respondent is the District Court of Denver County.

2. Mr. Seymour was charged when he was sixteen years old pursuant to the direct-file statute, C.R.S. § 19-2.5-801(1)(a). The most significant charges are five (5) counts of First Degree Murder – After Deliberation.[1]

3. This case is being heard in Denver County before the Honorable Martin Egelhoff in case 21CR020001. The case is the People of the State of Colorado v. Gavin Seymour. A status conference is set for January 20, 2023.

[1] Mr. Seymour is also charged with five (5) counts of First Degree Murder – Extreme Indifference, five (5) counts of Felony Murder, three (3) counts of Attempted First Degree Murder – After Deliberation, two (2) counts of Attempted First Degree Murder – Extreme Indifference, four (4) counts of First Degree Assault, two (2) counts of Second Degree Assault, one (1) count of First Degree Burglary, one (1) count of Second Degree Burglary, three (3) counts of First Degree Arson, eight (8) counts of Fourth Degree Arson, two (2) counts of Conspiracy to Commit First Degree Murder, one (1) count of Conspiracy to Commit First Degree Burglary, one (1) count of Conspiracy to Commit Second Degree Burglary, one (1) count of Conspiracy to Commit First Degree Arson, one (1) count of Conspiracy to Commit Fourth Degree Arson, and fourteen (14) Crime of Violence sentencing enhancers.

4. Mr. Seymour requests relief against the People of the State of Colorado and the District Court.

Ruling Complained Of and Relief Being Sought:

5. On June 30, 2022, Mr. Seymour filed several Motions to Suppress in this case. At issue here is the Motion to Suppress Evidence From a Keyword Warrant & Request For a Veracity Hearing ("Motion to Suppress"). *See Exhibit 1*.

6. On July 1, 2022, the Electronic Frontier Foundation filed an *amicus* brief in support of the Motion to Suppress. *See Exhibit 2 (Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant's Motion to Suppress)* ("EFF Amicus").

7. On August 12, 2022, the District Attorney filed a Response to Motion to Suppress Evidence From a Keyword Warrant & Request For a Veracity Hearing. *See Exhibit 3*.

8. During the Motions Hearing on August 19, 2022, the District Court received testimony from Nikki Adeli, a Legal Information Specialist at Google, and from Detective Ernest Sandoval of the Denver Police Department. *See Exhibit 4*

(8/19/22 Tr.). At the conclusion of the hearing, the District Court authorized both parties to file additional briefings on the issues litigated during the hearing, including the keyword warrant issue.

9. On September 16, 2022, Mr. Seymour filed Defendant's Reply to People's Responses to Motion to Suppress Evidence From a Keyword Warrant and Motions to Suppress Evidence Unlawfully Obtained [Def-25], [Def-26], [Def-27], [Def-29], [Def-30], and [Def-37]. *See Exhibit 5*.

10. On September 30, 2022, the District Attorney filed People's Reply to Defendant's Motion to Suppress. *See Exhibit 6*.

11. Lastly, on September 30, 2022, Mr. Seymour filed Defendant's Response to People's Written arguments on Defendant's Motion to Suppress. *See Exhibit 7*.

12. On November 16, 2022, during a hearing, the District Court denied Mr. Seymour's Motion to Suppress. The District Court did not enter any written orders regarding the Motion to Suppress. *See Exhibit 8 (11/16/22 Tr.)*.

This Court Has Jurisdiction Under Colorado Appellate Rule 21:

13. Review is appropriate under Colorado Appellate Rule 21 ("C.A.R. 21") because this case raises an issue of first impression of significant public importance:

whether the United States and Colorado constitutions prohibit police from using a novel "reverse keyword warrant" to search *everyone's* Google search histories to identify a criminal suspect. Additionally, the normal appellate process is inadequate because it would leave the public's constitutional rights in limbo while requiring a child to stand trial as an adult and face five life sentences.

14. "An original proceeding under C.A.R. 21 is an extraordinary remedy that is limited both in its purpose and availability." *People v. Tafoya*, 434 P.3d 1193, 1195 (Colo. 2019) (citing *Wesp v. Everson*, 33 P.3d 191, 194 (Colo. 2001)). Despite this general rule, orders that would not normally be subject to interlocutory review can still warrant relief under C.A.R. 21. *See Cardenas v. Jerath*, 180 P.3d 415, 420 (Colo. 2008) ("Because discovery orders are interlocutory in character, they generally are not reviewable in a C.A.R. 21 original proceeding…However, a discovery order is 'not exempted from extraordinary relief under appropriate circumstances.'").

15. Original jurisdiction under C.A.R. 21 is appropriate in two circumstances. First, "[t]his court will generally elect to hear C.A.R. 21 cases that raise issues of first impression and that are of significant public importance." *People v. Steen*, 318 P.3d 487, 490 (Colo. 2014). Second, it is appropriate when appeal would not

provide a plain, speedy, and adequate remedy." *People v. Dist. Court*, 953 P.2d 184, 187 (Colo. 1998). Both grounds are present here.

I. This Issue Is a Matter of First Impression and Public Importance

16. As this Court has often stated, "We generally elect to hear cases under C.A.R. 21 that raise issues of significant public importance that we have not yet considered." *Wesp*, 33 P.3d at 194 (citing *City & County of Denver v. Dist. Court*, 939 P.2d 1353, 1361 (Colo. 1997)); *see also Higgs v. Dist. Court*, 713 P.2d 840, 849 (Colo. 1985); *Williams v. Dist. Ct.*, 700 P.2d 549, 553 (Colo. 1985) (holding relief appropriate where an "order raises a substantial issue relating to the administration of criminal justice… or places an accused at an unwarranted disadvantage in a pending criminal trial…"); *Accetta v. Brooks Towers Residences Condominium Assn., Inc.*, 434 P.3d 600, 602 (Colo. 2019); *Smith v. Jeppsen*, 277 P.3d 224, 226 (Colo. 2012); *People v. Higgins*, 383 P.3d 1167 (Colo. 2016); *Steen*, 318 P.3d at 490. This is one of those cases.

17. A keyword warrant is a digital dragnet of immense proportions. It requires Google to search the accounts belonging to billions of Google users and produce information about anyone who looked for certain terms or keywords during a given time. It is profoundly different from traditional search warrants

seeking data belonging to a suspect. Instead, the process operates in reverse—search everyone first, and identify suspects later.

18. For this reason, keyword warrants are also known as "reverse warrants," and are similar to so-called "geofence warrants" that have recently been found unconstitutional. *See, e.g.*, *United States v. Chatrie*, 590 F. Supp. 3d 901, 905 (E.D. Va. 2022); *In re Search of Information that is Stored at the Premises Controlled by Google*, 542 F. Supp. 3d 1153, 1158-59 (D. Kan. 2021); *In re Information Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 756-57 (N.D. Ill. 2020); *In re Information Stored at Premises Controlled by Google*, No. 20 M 297, 2020 WL 5491763, *8 (N.D. Ill. July 8, 2020).

19. Unlike geofence warrants, however, there are no state or federal decisions addressing keyword warrants, apart from this case. It is an issue of first impression in Colorado, and nationally as well.

20. The first reported use of a keyword warrant was in Minnesota in 2017. *See* Thomas Brewster, "Exclusive: Government Secretly Orders Google To Identify Anyone Who Searched A Sexual Assault Victim's Name, Address Or Telephone Number," *Forbes* (Oct. 4, 2021).[2] But until now, examples were

[2] *Available at*: https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/.

rare, and their legality was never litigated. *Id.* As a result, keyword warrants are facing judicial scrutiny for the first time here.

21. The government's use of reverse warrants, however, is becoming more frequent. According to Google, the use of geofence warrants in Colorado has increased dramatically year-over-year: 27 in 2018; 174 in 2019; and 243 in 2020, the most recent year for which data is available.[3] Google has not published the equivalent statistics for keyword warrants, but it is likely that they follow a similar trajectory. *See* EFF Amicus at 9; 11/16/22 Tr. at 26 ("the police's use of these kinds of warrant requests or other kinds of electronic data is becoming more and more common").

22. The constitutionality of keyword warrants is a matter of great public importance because they implicate the privacy rights of everyone who runs a Google search. Because Google does not know ahead of time which accounts might have relevant data, they must indiscriminately search the records belonging to billions of Google users, in Colorado and everywhere else. Such dragnets will inevitably sweep up people with no connection to the crime, especially if the terms are broad. *See Exhibit 2 (EFF Amicus)* at 8-11.

[3] Google, Supplemental Information on Geofence Warrants in the United States, https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (click on "Download supplemental data as a CSV" for state-by-state statistics).

23. Furthermore, keyword warrants harm expressive freedoms guaranteed by the First Amendment and Article II, Section 10 of the Colorado Constitution. As the Electronic Frontier Foundation explained in its *amicus* brief, search engines like Google are indispensable for browsing the internet. *Id.* at 15. Thus, "querying a search engine implicates not just the First Amendment's well-known protection for the freedom of speech, but also the rights to distribute and receive information, and to freely and privately associate with others." *Id.*; *see also Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044 (Colo. 2002). Keyword warrants threaten to chill the public's right to seek out information and deter participation in a robust exchange of ideas by transforming every Google search into a risk.

24. Members of the public, however, will rarely if ever be able to detect and challenge the use of keyword warrants that infringe on their privacy. Law enforcement does not often disclose its use of keyword warrants, let alone notify people whose data they searched, effectively foreclosing civil litigation as a means of redress. As a result, the only opportunity for courts to assess the constitutionality of keyword warrants could be in criminal cases like this one. While this Court might eventually reach this issue on direct appeal, it would likely be many years before that occurs. Thus, for the public, this petition may

be the only way to affirm their privacy and expressive rights in a timely manner.

25. Indeed, the keyword warrant issue has already generated significant public interest in this case. *See, e.g.,* Jon Schuppe, "Police Sweep Google Searches to Find Suspects. The Tactic Is Facing Its First Legal Challenge," NBC News (June 30, 2022)[4]; Thomas Brewster, "Warrants Can Force Google To Look Through Your Search History—A Tragic Arson Case May Decide If That's Constitutional," Forbes (June 30, 2022)[5]; Elise Schmelzer, "'Digital Dragnet' or Necessary Tool? Denver Police's Use of Controversial Google Search Technique in Deadly Arson Draws Legal Fight," Denver Post (July 8, 2022).[6]

26. Public concerns included the effects on protesters, the press, religious and LGBTQ communities, as well as people seeking access to reproductive care, including abortions. *See, e.g.,* Albert Fox Cahn & Julian Melendi, "The New Way Police Could Use Your Google Searches Against You," Slate (Aug. 1,

[4] *Available at*: https://www.nbcnews.com/news/us-news/police-google-reverse-keyword-searches-rcna35749.
[5] *Available at*: https://www.forbes.com/sites/thomasbrewster/2022/06/30/warrants-can-force-google-to-look-through-your-search-historya-tragic-arson-case-may-decide-if-thats-constitutional/.
[6] *Available at*: https://www.denverpost.com/2022/07/08/denver-police-reverse-keyword-search-arson-murder/.

2022);[7] Scott Norvell, "Police Use of 'Keyword Warrants' to Monitor Americans' Online Search Queries Comes Under Increasing Scrutiny," New York Sun (July 12, 2022);[8] Corin Faife, "Powerful Keyword Warrants Face New Challenge in Deadly Arson Case," The Verge (July 1, 2022).[9] In short, this case has tremendous public importance, with consequences for almost every member of the public, affecting not only their privacy, but their expressive and associational rights as well.

27. Despite the significance of this issue, as well as extensive briefing, testimony, and argument before the District Court, Judge Egelhoff did not issue a written opinion on the Motion to Suppress. Instead, on November 16, 2022, the judge issued an oral opinion denying the motion, citing just one single case. *Exhibit 8 (11/16/22 Tr.)* at 7. The court focused instead on process—on the fact that police obtained a warrant—and did not address Mr. Seymour's argument that such general warrants are constitutionally impermissible.

[7] *Available at*: https://slate.com/technology/2022/08/keyword-search-warrants-colorado-roe.html.
[8] *Available at*: https://www.nysun.com/article/police-use-of-keyword-warrants-to-monitor-americans-online-search-queries-comes-under-increasing-scrutiny.
[9] *Available at*: https://www.theverge.com/2022/7/1/23191406/denver-arson-google-keyword-warrant-challenge-constitutional-fourth-amendment-privacy.

28. Judge Egelhoff referred to the keyword warrant as "novel" no less than six times, yet the District Court's reasoning elided the very facts that make this search so new and troublesome. *Id.* at 11, 12, 14, & 28. Specifically, the court was "not persuaded" that a search occurred of the data belonging to billions of Google users, *id.* at 19, finding instead that it was a mere "database query" of information "in the internet." *Id.* at 19-20. Similarly, the court characterized the data returned by Google as just an "anonymized list of IP addresses," ignoring the fact that IP addresses are not only tied to individual users, but are also a common way for law enforcement to identify people online. *Id.* at 20. The District Court intended its rendition of the facts to "simplif[y] and clarif[y] the analysis," *id.* at 19, but in doing so, it decided a different question. The reason this case has such public significance is because keyword warrants affect everyone who uses Google to search the internet, including Mr. Seymour. Ignoring the facts to "simplif[y]" the legal analysis does a disservice to the public and pleads for guidance from the Supreme Court. *Id.*

29. Declining to grant this petition would simply delay resolution of this significant issue, potentially for years. In the meantime, neither police, nor the public, nor the trial courts, nor Mr. Seymour would know whether the federal or state constitutions permit general warrants that inspect *everyone's* Google search history for evidence of criminal activity, without probable cause to suspect

anyone. It would mean that Mr. Seymour, who was barely 16 at the time of the crime, would face a quintuple homicide trial as an adult. It would mean that law enforcement, during ongoing investigations, would not know if similar warrants will make or tank their cases. And it would mean the public will be left to wonder if their private data is private, and if the police can make Google search for them.

30. Accordingly, because of the multiple constitutional rights at play, the likelihood that this issue will recur, and the implications of this case beyond its confines, this Court should provide guidance now, in a case of first impression with statewide and national importance. *See People v. Kilgore*, 455 P.3d 746, 749 (Colo. 2020) ("[G]iven the constitutional rights potentially at play, the number of jury trials held every month throughout our state, and the prevalence of standard case-management orders, we view this as an issue of significant public importance that is likely to recur. Hence, we feel compelled to provide guidance."). *See also People v. Rowell*, 453 P.3d 1156, 1159 (Colo. 2019); *People v. Lucy*, 467 P.3d 332, 336 (Colo. 2020).

II. No Appellate Remedy Is Adequate

31. While this is an important case of first impression, jurisdiction is also appropriate because no appellate remedy is adequate. *See Tafoya*¸434 P.3d at 1195 (exercising jurisdiction under C.A.R. 21 because "an appellate remedy would be inadequate") (citing *Fognani v. Young*, 115 P.3d 1268, 1271 (Colo. 2005)). *See also People v. Casias*, 59 P.3d 853, 856 (Colo. 2002) (internal citations omitted) (holding that exercise of jurisdiction under C.A.R. 21 "is appropriate where the ruling in question 'may have a significant impact on a party's ability to litigate the merits of a controversy' or where 'an appellate remedy would not be adequate'"). "The granting of this remedy is entirely within the discretionary authority of this court." *People v. Dist. Court*, 869 P.2d 1281, 1285 (Colo. 1994).

32. The District Court's denial of the Motion to Suppress has a significant impact on Mr. Seymour's ability to litigate his case. All of the evidence in the People's case flows directly from the results of the keyword search warrant. *See Exhibit 8 (11/16/22 Tr.)* at 18 ("I think the real starting point with respect to all this relates to the keyword search that was conducted pursuant to the search warrant because, by and large—at least this is my understanding of how this all played out—based upon the results of that keyword search, the other searches, the other information, the other avenues of investigation flowed from that particular

search and search warrant and was revealed from it."). In other words, the issue is dispositive.

33. And for a juvenile like Mr. Seymour, in a case involving charges of such severity, a post-trial, post-conviction, post-sentencing appeal is not an adequate remedy to resolve such a dispositive legal issue. The U.S. Supreme Court has repeatedly held that juveniles should be treated differently than adults under the law, and Mr. Seymour's youth should likewise be a factor in determining whether an appellate remedy is adequate.

34. Similarly, for this Court to eventually resolve this critical issue, Mr. Seymour would have to forego a favorable plea offer, face a quintuple murder trial as a teenager, and risk being sentenced to life in prison. This is because criminal defendants in Colorado may no longer enter a "conditional plea." *See Neuhaus v. People*, 289 P.3d 19 (Colo. 2012) ("*Neuhaus II*"). As a result, C.A.R. 21 is the only way in which Mr. Seymour can obtain interlocutory appeal without incurring the draconian penalties of going to trial.

A. Juveniles Are Different from Adults.

35. Just as the U.S. Supreme Court has determined that juveniles must be treated differently when it comes to sentencing and other phases of the criminal justice process, so too should this Court find that C.A.R. 21 is the only adequate

remedy for a juvenile like Mr. Seymour. Mr. Seymour has been in pre-trial detention for two years already, and any direct appeals process would likely add years more. This Court should take Mr. Seymour's youth into account when assessing whether such a process is an "adequate" remedy to resolve a dispositive and pressing question of constitutional law.

36. It is critical to recognize that Mr. Seymour was a juvenile at the time of this offense and was charged under Colorado's direct-file statute. The direct-file statute states:

> "A juvenile may be charged by the direct filing of an information in the district court or by indictment only if the juvenile is sixteen years of age or older at the time of the commission of the alleged offense" and, as is the case here, "[i]s alleged to have committed a class 1 or class 2 felony."
>
> C.R.S. § 19-2.5-801(1)(a).

37. Mr. Seymour was 16 years and 4 days old on the date of offense. However, because he has been charged as an adult, he is facing five life sentences in the Department of the Corrections.

38. If this incident had occurred five days earlier, the circumstances in this case would have been extraordinarily different. For the People to try someone between the ages of 14 and 15 as an adult, they must file a petition in juvenile court alleging that the juvenile is "[f]ourteen years of age or older at the time of

the alleged offense and is a juvenile delinquent by virtue of having committed a delinquent act that constitutes a felony." C.R.S. § 19-2.5-802(1)(a)(I)(B). The juvenile court must then hold a "transfer hearing," where the court shall consider 19 total factors. C.R.S. § 19-2.5-802(3)(a)-(b), (4)(a)-(b)(XIV). At the conclusion of the transfer hearing, if the juvenile court finds that it would "be contrary to the best interests of the juvenile or of the public to retain jurisdiction," C.R.S. § 19-2.5-802(1)(a)(II), the juvenile court can enter an order waiving jurisdiction over the juvenile and the People can then file an information in district court, where the juvenile will be tried as an adult.

39. This was not the case for Mr. Seymour. Because Mr. Seymour was *barely* 16 at the time of the alleged offense, the People were able to charge him by direct filing of information. After the People charged him as an adult, Mr. Seymour filed a motion in district court to transfer the case to juvenile court pursuant to C.R.S. § 19-2.5-801(4)(a). The "reverse-transfer hearing" is similar to the aforementioned transfer hearing in that the court considers 11 factors enumerated in the statute and decides whether it should maintain jurisdiction over the case. C.R.S. § 19-2.5-801(4)(b)(I)-(XI).

40. The District Court held Mr. Seymour's combined preliminary hearing and reverse-transfer hearing from January 10 to January 12, 2022. On January 25,

2022, Judge Egelhoff entered an oral ruling denying Mr. Seymour's motion to transfer the case to juvenile court.

41. Mr. Seymour was a 16-year-old child when this incident took place. The United States Supreme Court has emphasized that the distinctive attributes of youth diminish the penological justifications for imposing the harshest sentences on juvenile offenders, even when they commit terrible crimes.

42. The U.S. Supreme Court has handed down a series of cases with a strong direction of change for the prosecution of juveniles. These cases recognize the mitigating qualities of youth and credit the consistent weight of authority regarding how juveniles think and respond in criminal cases. Starting with *Roper v. Simmons*, 543 U.S. 551, 570 (2005), the Supreme Court tacitly endorsed the wisdom of reduced juvenile culpability when it recognized that a juvenile's criminal conduct is "not as morally reprehensible as that of an adult."

43. Then in *Graham v. Florida,* 560 U.S. 48 (2010), and *Miller v. Alabama,* 567 U.S. 460 (2012), the Court explicitly recognized reduced juvenile culpability and reaffirmed those holdings again in *Montgomery v. Louisiana,* 577 U.S. 190 (2016). As the Court stated in *Roper*, 543 U.S. at 570, "[j]uveniles' immaturity, vulnerability, and changeability—while they in no way excuse juveniles' crimes—substantially lessen their culpability and undermine any justification

for definitively ending their free lives." As a result, "children are constitutionally different than adults" due to their lack of maturity, underdeveloped sense of responsibility, vulnerability to peer pressure, and the less fixed nature of the juvenile's character. *Miller*, 567 U.S. at 470; *see also Graham*, 560 U.S. at 67; *Roper*, 543 U.S. at 469-70.

44. Changes in legislation in Colorado reflect the nationwide trend to recognize the inherent mitigating qualities of youth. In 2012 and 2016, the Colorado legislature passed watershed reforms of the sentencing options available when sentencing children. The legislature raised the age for direct-file eligibility, removed several crimes from direct-file eligibility, and allowed the defense to petition for a reverse-transfer hearing, as discussed above. C.R.S. § 19-2-517(1)(a); HB 12-1271 § 1. In these amendments, the legislature made the decision to no longer allow children under the age of 16 from being direct-filed into adult court. The sentencing statutes were also modified to create a sentencing structure where children receive less severe sentences than under the prior law. *See* C.R.S. § 19-2-517(6)(a)(I).

45. The Supreme Court cases, recent legislative enactments, and the Colorado governor's recent commutations confirm what social science has been stating for decades: children are different and deserve to be treated differently in the

eyes of the law, and no child should forever be defined by his worst act, particularly when research has firmly established that the teenage brain is not yet fully developed.

46. Accordingly, the question of what counts as an "adequate" appellate remedy should be viewed through this lens as well. Mr. Seymour was a child when this incident occurred, and without relief under C.A.R. 21, he will be placed is the very adult position of having to decide between a favorable plea offer or risking trial and receiving five life sentences. That is a decision that any adult would struggle to make. But for a juvenile, it is confounded by the same factors counseling mitigation: "immaturity, vulnerability, and changeability." *Roper*, 543 U.S. at 570.

47. Moreover, Mr. Seymour recognizes that if he is found guilty at trial, a direct appeal will take years to litigate. Mr. Seymour has already spent nearly two years in custody awaiting trial, and the prospect of spending a substantial amount of additional time in prison to resolve such a dispositive, novel issue places Mr. Seymour in an impossible position for a juvenile whose brain and decision-making skills are still developing.

B. C.A.R. 21 Is the Only Remaining Mechanism for Interlocutory Review for Mr. Seymour.

48. Mr. Seymour faces this dilemma because a third option, a "conditional plea," is no longer available to criminal defendants in Colorado. Although the People may seek interlocutory review for any number of reasons, Mr. Seymour cannot do the same. Consequently, C.A.R. 21 is the only adequate remedy for Mr. Seymour to obtain relief without risking life in prison.

49. Defendants were not always this disadvantaged. In Colorado, a defendant was previously able to able to enter a "conditional plea," where they could enter a guilty plea contingent on being able to appeal a specific issue. *See People v. Neuhaus*, 240 P.3d 391, 393 (Colo. App. 2009) ("*Neuhaus I*") (citing *Conditional Guilty Pleas*, 93 Harv. L. Rev. 564, 566 (1980)) ("One form of conditional guilty plea 'allows the defendant to plead guilty, thus avoiding a trial which would serve no purpose, while expressly preserving the right to appeal the denial of his motion to suppress evidence on constitutional grounds.'").

50. In its decision, the *Neuhaus I* court discussed the procedural history of conditional pleas in Colorado. In that case, the defendant pled guilty to one count of possession of a weapon by a previous offender, and the People dismissed the rest of his charges. *Id.* A condition of the plea was that the

defendant was "permitted to appeal the trial court's ruling on his suppression motion." *Id*. The parties stated:

> "The results of the appeal would be 'dispositive' of the charges, meaning that, if defendant were successful, the subsequent suppression of the evidence would deprive the prosecution of sufficient evidence to go forward with the case. If this court were to reverse the trial court's order denying the suppression motion, the prosecution would allow defendant to withdraw his guilty plea and would dismiss the charges."
>
> *Id.*

51. Pursuant to the agreement, the defendant appealed the suppression issue. *Id*. The appellate court asked two questions: "(1) whether the plea agreement was a conditional plea; and (2) if so, whether we have authority to review the suppression issue." *Id*.

52. The court noted that the purpose of plea agreements is to:

> "lead[ ] to prompt and largely final disposition of most criminal cases;…avoid[ ] much of the corrosive impact of enforced idleness during pre-trial confinement for those who are denied release pending trial;'…and, by shortening the time between charge and disposition, [they] enhance[ ] whatever may be the *rehabilitative prospects of the guilty* when they are ultimately imprisoned.'"
>
> *Id.* (emphasis added) (citing *Santobello v. New York*, 404 U.S. 257, 261 (1971).

53. The court noted that "[t]he general rule is that a valid guilty plea waives all nonjurisdictional objections, including allegations that constitutional rights have

been violated," and as such, the defendant "has no right to raise a constitutional claim after pleading guilty unless such a claim relates directly to the guilty plea's adequacy." *Id.* (citing *People v. Isham*, 923 P.2d 190, 195 (Colo. App. 1995). However, the court noted, an exception to this rule, the conditional guilty plea, has been adopted by other jurisdictions. *Id.*

54. In Colorado, for a long time, the courts were split on the issue of conditional pleas. In *People v. Pharr*, 696 P.2d 235 (Colo. 1984), the defendant entered a conditional guilty plea "that purported to preserve the right to appeal the constitutionality of the statute establishing the crime with which he was not charged." *Neuhaus I*, 240 P.3d at 393. The *Pharr* court "'specifically disapprove[d]' of this procedure because it was not 'recognized by either rule or statute.'" *Id*. (citing *Pharr*, 696 P.2d at 236). Then, in *Waits v. People*, 724 P.2d 1329 (Colo. 1986), the Supreme Court "stated that a guilty plea precludes a defendant from attacking the plea on the ground that the seizure of evidence was the product of an illegal search 'unless a right to challenge the plea is preserved by statute.'" *Neuhaus I*, 240 P.3d at 393-94 (citing *Waits*, 724 P.2d at 1337).

55. *People v. Bachofer*, 85 P.3d 615 (Colo. App. 2003), came next. The *Bachofer* court disagreed with *Pharr* and *Waits*, stating:

> "We perceive no probation of the [conditional guilty plea] agreement used here and conclude that in the interest of judicial economy, there is no justification for barring a stipulation whereby a defendant pleads guilty to a charge on the condition that he or she may nevertheless seek review of an adverse pretrial ruling that directly affects the charge."
>
> *Id.* at 617.

56. After *Bachofer*, the Supreme Court decided *People v. McMurtry*, 122 P.3d 237 (Colo. 2005). "The [*McMurtry*] court cited *Pharr*, and then noted that it had 'never publicly endorsed' the use of such pleas." *Neuhaus I*, 240 P.3d at 394 (citing *McMurtry*, 122 P.3d at 243). However, the "plea at issue in *McMurtry* was not a conditional plea," so the court "stated that it would 'leave to another day the issue of whether the conditional plea is an acceptable practice in Colorado.'" *Id*. (citing *McMurtry*, 122 P.3d at 243).

57. The *Neuhaus I* court was therefore presented with the issue, despite the *Bachofer* decision. After discussing the history of conditional pleas in Colorado, the court turned to the history of conditional pleas in other jurisdictions. *Id*. at 394. The "[d]ebate over the propriety of conditional guilty pleas" began in the early 1970s, and the federal circuits "eventually fractured over whether such pleas were authorized by law." *Id*. "The Second and Third Circuits approved of them," and "[t]he Eighth and District of Columbia Circuits praised the concept, although the Eighth Circuit thought its adoption would best

be accomplished by a statute, a court rule, or a decision of the Supreme Court." *Id*. On the other hand, "[t]he Fourth, Fifth, Sixth, Seventh, Ninth, and Tenth Circuits found conditional guilty pleas to be improper," and "[t]he First Circuit reserved judgment." *Id*.

58. In order to resolve this split, Fed. R. Crim. P. 11(a)(2) was created in 1983. *Id*. The statute states:

> "With the consent of the court and the government, a defendant may enter a conditional plea of guilty or nolo contendere, reserving in writing the right to have an appellate court review an adverse determination of a specified pretrial motion. A defendant who prevails on appeal may then withdraw the plea."
>
> *Id.*

59. Of note, the statute "has been interpreted to require that the issue preserved for appeal be dispositive of the case." *Neuhaus I*, 240 P.3d at 395 (citing *United States v. Wong Ching Hing*, 867 F.2d 754, 758 (2d Cir. 1989)).

60. The *Neuhaus I* court noted that "[a]lthough the Committee Note to [F.R.C.P. 11(a)(2)] indicate [sic] that a few jurisdictions, such as California, New York, and Wisconsin, had statutes or court rules authorizing conditional pleas" before F.R.C.P. 11(a)(2) was passed, the court's research "reveals that, as of now, at least thirty-two jurisdictions, including federal courts and the United States

military, have approved of conditional guilty pleas." *Neuhaus I*, 240 P.3d at 394.

61. At the time of the *Neuhaus I* decision, conditional pleas were authorized in three ways: "Ten jurisdictions have statutes…Sixteen jurisdictions authorized conditional guilty pleas for the first time by court rules," and "[s]ix jurisdictions adopted conditional pleas by judicial decision," four of which "also subsequently promulgated court rules." *Id*. at 394-95. Of these thirty-two jurisdictions, "only two rely exclusively on judicial decisions for that authority." *Id.* at 395. The *Neuhaus I* court turned to Colorado statutes and court rules, noting that none of the statutes and rules regarding pleas mentioned conditional pleas. *Id.*

62. Then, the court detailed the numerous ways in which the prosecution can lodge interlocutory appeals, and discussed the inability of defendants to do the same.

63. This is where the inequity lies. Crucially, under C.R.S. § 16-12-102(2) (2009) and C.A.R. 4.1(a), "the prosecution is authorized to take interlocutory appeals to the supreme court if a trial court suppresses evidence for reasons enumerated" in § 16-12-102(2), Crim. P. 41(e) and (g), and Crim. P. 41.1(i). *Id.* "These reasons include suppression orders based on determinations that evidence was seized in an illegal search." *Id.* (citations omitted). *See also* Crim.

P. 5(a)(4)(V) ("If the prosecutor believes the court erred in its finding of no probable cause, the prosecutor may appeal the ruling to the district court…pursuant to the procedures for interlocutory appeals in Rule 37.1…").

64. On the other hand, "[t]he statute and the court rule *do not* provide defendants with a right to an interlocutory appeal, and the supreme court has repeatedly ruled that defendants *are not entitled to interlocutory relief under the statute and rule*." *Neuhaus I*, 240 P.3d at 395 (emphasis added). "Therefore, if a district court resolves a suppression issue against a defendant, the supreme court does not have jurisdiction to address that ruling in an interlocutory appeal." *Id*.

65. The *Neuhaus I* court therefore concluded that "conditional guilty pleas are not authorized in Colorado by statute or court rule," and moved onto "whether United States Supreme Court and Colorado case law governing guilty pleas in general provides a basis for authorizing conditional guilty pleas." *Id.* at 395-96.

66. Despite the court's thorough analysis of other jurisdictions' acceptance of conditional pleas, and the recognition that the People are able to file interlocutory appeals under many more circumstances than defendants, the court ended its opinion by emphasizing the "'fundamental and basic inconsistency between knowingly and intelligently entering a plea of guilty, and

then appealing from the judgment entered on the basis of that plea.'" *Id*. at 396-97 (citing *United States v. Cox*, 464 F.2d 937 (6th Cir. 1972)). The court therefore held that "without a statute or court rule," Colorado "does not authorize conditional guilty pleas." *Id*. at 398.

67. The Court then released three concurrent decisions: *People v. Hoffman*, 289 P.3d 24 (Colo. 2012) ("*Hoffman II*"), *Neuhaus II*, 289 P.3d 19, and *Escobedo v. People*, 289 P.3d 25 (Colo. 2012). *Neuhaus II* stated that the issue was "one of first impression" and required the court "to determine whether a defendant may reserve the right to appeal an unsuccessful motion to suppress evidence despite having entered a guilty plea." *Neuhaus II*, 289 P.3d at 20. The court held that conditional pleas are not permitted and "declin[ed] to create by judicial decision an exception allowing conditional guilty pleas…because a reservation of that right is better created by statute or court rule, if at all." *Id.* at 20-21. *Hoffman II*, 289 P.3d 24, and *Escobedo*, 289 P.3d 25, held the same. The right that defendants had to enter into conditional plea deals was therefore unambiguously taken away.

68. The People are able to lodge interlocutory appeals in a plethora of situations. Defendants, including Mr. Seymour, are not given the same courtesy. As a result of the holdings in *Neuhaus II*, *Hoffman II*, and *Escobedo*, defendants lost

the right to enter conditional guilty pleas, and C.A.R. 21 is the only way in which a defendant can set an interlocutory appeal in motion under these circumstances.

69. The aforementioned federal statute authorizing conditional guilty pleas exists for a reason, as do the statutes and court rules in other states. The previously discussed split between the divisions of the Colorado Court of Appeals also existed to the same end. These decisions and rules highlight why allowing defendants to enter conditional pleas is the fair thing to do, as the existence of conditional pleas closed the gap between the ability of prosecutors to appeal a trial court's decision before trial and the lack of defendants' ability to do the same. Colorado does not have a similar rule, despite the fact that the prosecution is given so many opportunities to appeal unfavorable decisions by the trial court, including the ability to file C.A.R. 21 petitions.

70. The only way Mr. Seymour can get *adequate* relief is through this petition. Before 2012, there would have been a speedy, adequate appellate remedy other than the one permitted by C.A.R. 21: a conditional guilty plea.

71. Conditional pleas are not an option anymore. As a result, Mr. Seymour, who was a child when this incident occurred, faces an impossible decision at such a young age. He may plead guilty and forfeit his right to appeal a dispositive

suppression issue in a matter of national importance. Or he can proceed to trial, where he would likely be found guilty, and be sentenced to a mandatory term of five life sentences in prison, just to gain the opportunity to risk the chance that an appeal would be successful in the Court of Appeals. Under the specific and unusual circumstances of this case, this would not afford Mr. Seymour an "adequate" remedy under the law.

72. This is an issue of first impression and of great public importance, and an appeal would not provide an adequate remedy. Extraordinary relief is warranted for an extraordinary case. Jurisdiction under C.A.R. 21 is therefore appropriate here.

Issue Presented:

73. Whether a "reverse keyword warrant" violates 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*.

Factual Background:

74. On August 5, 2020, at 5312 North Truckee Street in Denver, Colorado, five people were killed in a house fire believed to be arson. Video surveillance footage showed three individuals standing in the side yard of the home shortly before the fire. The individuals were wearing masks and hooded sweatshirts

with the hoods up. The footage also showed these individuals running through the backyard of the home shortly after the fire.

75. During its investigation into who was responsible for setting the fire, the Denver Police Department partnered with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). Fifty-seven warrants were issued throughout the investigation. The first 23 warrants failed to produce any leads in the investigation. *See Exhibit 9 (11/12/21 Tr*.) at 47.

76. So, with no suspects, investigators sought a novel reverse keyword warrant. Investigators determined that 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. *Id.* This warrant would require Google to determine which, if any, users had searched for nine variations of the address of the arson (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*. In practice, investigators obtained three keyword warrants. Google rejected the first two and complied with the third.

I. Reverse Keyword Warrants Generally

77. Google provided a declaration in this case, describing, for the first time, how a reverse keyword search works. *See Exhibit 4 (Declaration of Nikki Adeli)*. Google also provided live testimony at the hearing on August 19, 2022. *See Exhibit 10 (8/19/22 Tr.)* at 24-66.

78. First, Google states that it requires law enforcement to obtain a warrant. *Id*. at ¶ 3. This is because Google treats search query data as private content belonging to individual Google users. *See Exhibit 11 (Google Privacy Policy)* at 22. Google records every search query that users make. If a Google user is signed-in to their account, then their queries are logged and saved to their account, which is personally identifiable by a "GAIA ID" ("Google Accounts and ID Administration") number. *Exhibit 4 (Declaration of Nikki Adeli)* at ¶ 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*. at ¶ 7. Both the GAIA ID and the Browser Cookie ID are personally identifiable with information available to law enforcement with a subpoena. In both cases, Google also logs the user's IP address, which law enforcement can use to subpoena subscriber information, including names and addresses. *See id.*

79. Google asserts that it "generally" uses a "staged process" for executing keyword warrants. *Id*. at ¶ 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.* at ¶ 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.* at ¶ 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.* Similarly, there is no way to geographically restrict the scope of the query by state or region, *see Exhibit 10 (*8*/19/22 Tr.)* at 49.

80. 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 Exhibit 4 (Declaration of Nikki Adeli)* at ¶¶ 7-8. Google decides, for example, 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.* at ¶ 6 (e.g., "1600 Amphitheater Parkway" vs. "1600 Amphitheater Parkway Google Headquarters"). *See also Exhibit 10 (8/19/22 Tr.)* at 45. It will do so even where the search results strongly imply that a keyword search is irrelevant. *See id.* at ¶ 8 (stating that Google will disclose search results for similar addresses in other cities or states).

81. Before turning over the query results to law enforcement, Google may "de-identif[y]" the results. *Id.* at ¶ 8. The "production version" of the query results "typically includes the following categories of information: (1) the date and time of the [keyword] search, 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.* at ¶ 7. The "Query" is the search query a user enters into Google Search or Google Maps. *Id.* at ¶ 4. The "Result" refers to the "result generated by Google from a user's queried search." *Id.* at ¶ 7. The "Host" is "the Google domain name that the user contacted (e.g., google.com and

google.fr).” *Id.* The GAIA ID is a unique number associated with each Google account. Lastly, a “Browser Cookie ID” is a unique number associated with the web browser that conducted the search. *Id. See also Exhibit 10 (8/19/22 Tr.)* at 47-50; *Exhibit 11 (Google Privacy Policy)* at 23.

82. While Google asserts that it de-identifies these results before disclosing them to law enforcement, *see Exhibit 4 (Declaration of Nikki Adeli)* at ¶ 3, the information it provides 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.* at ¶ 9. Separate from this, law enforcement can use a subpoena to obtain the name and address of the account holder. *See id.* (stating that law enforcement can use subpoenas under 18 U.S.C. § 2703(c)(2) to obtain various categories of identifying information 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 so-called de-identified query results.

83. Importantly, Google does not follow this process in all cases. Rather, Google qualifies that it "generally" uses the staged process described, *id.* at ¶ 3, but in some cases, such as this one, Google deviates significantly. As detailed below, the operative 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 ID. Law enforcement used the IP addresses provided in order to identify Google users, including Mr. Seymour.

84. Law enforcement obtained three keyword search warrants in this case. Each warrant focused on the same address over the same fifteen days, but they differed significantly in the types of data to be produced and the process for obtaining it from Google. Google did not comply with the first two, but it produced data in response to the third.

II. The First Keyword Warrant

85. On October 1, 2020, law enforcement submitted the first keyword warrant to Google. This warrant requested information on "any Google accounts that conducted a search while using Google Services…using one or more of the following search terms." *See Exhibit 12 (10/1/20 Keyword Search Warrant)*. The search terms were nine variations of "5312 Truckee Street," the address of

the arson, over the course of fifteen days ("July 22, 2020 at 00:01 M.S.T. through and to include August 5, 2020 at 02:45 M.S.T.").[10] *Id.* at 3138-39. The warrant had only 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. *See Exhibit 13 (Supplementary Report)* 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 Exhibit 4 (Declaration of Nikki Adeli)* at ¶ 11.

III. The Second Keyword Warrant

86. On October 20, 2020, the government submitted a second keyword warrant to Google. *See Exhibit 14 (10/20/20 Keyword Search Warrant)*. Like the first

[10] 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 North Truckee"; and "5312 North Truckee Street".

warrant, the October 20 warrant used the same nine variations of the "5312 Truckee Street" address and involved the same fifteen-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 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.

87. Despite the revised process, 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 warrant 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." *Id.* at 3068. 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." *Exhibit 13 (Supplementary Report)* at 3759.

88. 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." *Id.* at 3760. The Denver District Attorney was invited to join, *see Exhibit 15 (Email with Google)* at 6110-13, and DA Katherine Hansen participated. *Exhibit 10 (8/19/22 Tr.)* at 74. Counsel for Google told investigators that they were "skipping a step" by trying to obtain identifying information during the first stage of the warrant. *Id.* at 75. On November 19, 2020, the government submitted a third and final keyword warrant to Google. *See Exhibit 16 (11/19/20 Keyword Search Warrant)* at 2656-58.

IV. The Third Keyword Warrant

89. The third keyword warrant again sought returns for the same nine variations of the address where the fire occurred and the same fifteen-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. However, significantly, it also demanded "the IP addresses used by all accounts that are found to have conducted" one of the keyword searches. *Id.*

90. Including IP addresses is significant because they are *not* anonymous identifiers. Police routinely use them 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 Exhibit 9 (11/12/21 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.").

91. Google also recognized the significance of including the full IP address, which is why their keyword warrant procedure did not allow for the disclosure of that information. *See Exhibit 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.

92. Consequently, Google searched billions of users – worldwide – and produced two spreadsheets containing a total of sixty-one queries that it deemed responsive. *See Exhibit 17 (Keyword Warrant Return Data).* The government has testified that the search was limited to the entire state of Colorado, *see Exhibit 9 (11/12/21 Tr.)* at 82 ("I believe we limited it to Colorado"), but this is incorrect.[11] The spreadsheets returned by Google include a list of states ("Subdivisions") associated with each IP address. Of the sixty-one queries, thirty-eight were associated with Colorado, two were associated with Illinois, and twenty-one were blank. *See Exhibit 18 (12/4/20 Google Warrant)* at 2612. Google also affirmed that the search was *not* geographically limited to Colorado. *See Exhibit 10 (8/19/22 Tr.)* at 55.

93. Moreover, most of the queries Google returned did not match any of the nine variations of "5312 Truckee St." specified in the warrant. Only five did. Instead, there were forty-five that contained additional search terms, such as

[11] 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.

state, zip code, or the word "interior." There were another eleven entries that did not specify the search query used at all, leaving that field entirely blank.

94. Still, Google provided either a truncated GAIA or Cookie ID for each of the sixty-one queries, depending on whether the user was signed-in to their account at the time. *See Exhibit 17 (Keyword Warrant Return Data)*. There were five distinct GAIA IDs and four distinct Cookie IDs, suggesting that the data seized belonged to up to nine people.[12] *Id. See also Exhibit 9 (11/12/21 Tr.)* at 132, 135 (stating that the return included IP addresses). There were twelve distinct IP addresses responsible for those sixty queries, indicating that at least two of the nine people had searched Google from more than one IP address. *See id.*

95. Based on Google's return from the third keyword warrant, investigators focused on the five Google accounts with IP addresses in Colorado. *See Exhibit 18 (12/4/20 Google Warrant)* at 2612; *see Exhibit 9 (11/12/21 Tr.)* at 131. They

[12] The government has testified that Google provided five "accounts" in response to the keyword search warrant. *Exhibit 9* 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 into a Google account. *See Exhibit 19* (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 Exhibit 9 (11/12/21 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 the 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.").

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." *Exhibit 9 (11/12/21 Tr.)* at 48. Consequently, on December 4, 2020, investigators obtained five additional warrants seeking subscriber information associated with that activity. *See id.* at 135; *Exhibit 19 (Report of Investigation No. 7)* at 5843.

96. One warrant required Google to produce subscriber information in addition to all account contents, for all five accounts. *See Exhibit 18 (12/4/20 Google Warrant)* at 2604-05. Google refused to produce the account contents. *See Exhibit 4 (Declaration of Nikki Adeli)* at ¶ 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 Exhibit 19 (Report of Investigation No. 7)* at 5843.

97. The Google keyword search warrant results showed that Kevin Bui, one of Mr. Seymour's co-defendants, completed a query for 5312 Truckee St on July 23, 2020, thirteen times, on July 28, 2020, and July 29, 2020. The results also showed that on July 28, 2020, D.S., Mr. Seymour's other co-defendant,

completed a query for 5312 Truckee St. four times. Lastly, the results showed that on July 28, 2020, Mr. Seymour completed a query for 5312 Truckee St. fourteen times.

98. Law enforcement also served an additional warrant on Google for the account information belonging to E.M. There was no connection between Mr. Seymour, Mr. Bui, D.S., and E.M., except that E.M. searched for the address of the fire within the specified time frame. As a result, law enforcement obtained E.M.'s entire Google history, including all of her location history and search history, but did not find any connection to the fire.

99. The other four warrants required various internet service providers, including Comcast, AT&T, Verizon, and T-Mobile, to produce subscriber information associated with the full IP addresses in the keyword search return. Comcast complied, stating that two of the accounts were registered to "Stephanie Johnson" at an address in Lakewood, Colorado. *See Exhibit 20 (Comcast Warrant Return)* at 2775. Ms. Johnson is Mr. Seymour's mother, and they lived together at the same address in Lakewood.[13]

[13] Comcast stated that the third IP address was registered to Tanya Bui, the older sister of co-defendant Kevin Bui. *See id.* 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 Google ID.

100. 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. The government also obtained Mr. Seymour's text messages and historical cell phone location information. After reviewing this information and conducting further investigation, law enforcement arrested Mr. Seymour on January 27, 2021.

101. On February 2, 2021, the District Attorney filed an Affidavit for Arrest Warrant, Information, and a Motion to File by Direct Information Pursuant to Crim. P. Rule 7.

Argument

102. The reverse keyword warrant in this case compelled Google to search the private data of billions of users based on a mere "hunch" that someone responsible for the fire had searched for 5312 Truckee Street. *Exhibit 10 (8/19/22 Tr.)* at 83. But for this warrant, investigators would have never identified Mr. Seymour as a suspect in this case, let alone obtained his account contents and arrested him. *See id.* at 50-51.

103. The third and final 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.

104. This search also implicates the First Amendment, and as such, 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.*, 44 P.3d at 1047 (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.

105. 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.

106. 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. 2206, 2220 (2018). 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.* Keyword search data is even more revealing than cell phone location data, so 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.

107. 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).

108. 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*).

109. 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.

110. 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.

111. As the Electronic Frontier Foundation explained in its *amicus* brief, "[e]ven a simple query for an address can be revealing. For example, knowing that a person searched for '7155 E 38th Ave, Denver,' could lead to an inference that the person was seeking an abortion. (This is the address of Planned Parenthood.)." *Exhibit 2 (EFF Amicus)* at 5. Likewise, a search for "6260 E

Colfax Ave" (an HIV/AIDS screening center) or "2525 W Alameda Ave" (SEIU Local 105 headquarters) could be equally telling. Indeed, as the Supreme Court recognized in *Jones* and *Carpenter*, it takes little imagination to conjure up a parade of indisputably private examples, including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue, or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *accord. Carpenter*, 138 S. Ct. at 2217.

112. The Court should therefore follow the test established by *Tattered Cover*, 44 P.3d at 1059, for searches involving the contents of "expressive activities." The "expressive activities" at issue in *Tattered Cover* concerned the "reading history of customers," i.e., the information people read or intend to read. *Id.* at 1053. Today, people use Google search to find and read information of all kinds; but as in *Tattered Cover*, they "may have done so for any number of reasons, many of which are in no way linked to [the] commission of any crime." *Id.* at 1063. Consequently, warrants tied to the content of Google searches, as is the case here, are precisely the type of warrants likely to have unwanted chilling effects on people's willingness to search for and obtain information on Google or other search engines.

113. Basic Fourth Amendment protections, however, do not turn on whether a search raises special First Amendment concerns. It is enough that the government searched the contents of Mr. Seymour's Google account. Just as the Fourth Amendment draws "a firm line at the entrance to a house," *Payton v. New York*, 445 U.S. 573, 590 (1980), it will not bear even a cursory inspection of one's private "papers" and "effects" without a warrant. *See Entick v. Carrington* (1765) 19 How. St. Tr. 1029 (K.B.) 1029. In *United States v. Warshak*, for example, the Sixth Circuit did not need to inquire about the contents of Mr. Warshak's emails to find that they were constitutionally protected. 631 F.3d 266, 285-86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."). Furthermore, in *Carpenter*, the Supreme Court found that Mr. Carpenter's cell phone location (at a string of cell phone store robberies) was protected by the Fourth Amendment. *See* 138 S. Ct. at 2212-13. Indeed, the evidence the government seeks may have no First Amendment value whatsoever, but a valid warrant is still required.

114. 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.

115. 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 Keyword Search Information.

116. 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.

117. 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. *United States v. Miller*, 425 U.S. 435, 440 (1976) (bank records); *Smith v. Maryland*, 442 U.S. 735, 742 (1979) (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.

118. 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.*

119. 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.

120. 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*).

121. 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).

122. 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).

123. 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.

124. 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 Exhibit 11 (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.").

125. 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).

126. 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.

127. Judge Egelhoff was therefore correct in rejecting the state's argument that the keyword warrant did not implicate a reasonable expectation privacy. *See Exhibit 8 (11/16/22 Tr.)* at 21-22 ("I reject that. I'm not prepared to say that simply by availing oneself of the internet, that the users surrender all expectation of privacy with respect to that use.") As the court explained, "I think that certainly implicates Fourth Amendment concerns and the expectation of privacy. So I certainly reject the assertion that there is no expectation of privacy with respect to this type of information." *Id.* This Court should reach the same conclusion and hold that the third-party doctrine does not apply to Google search data.

C. People Have a Possessory Interest in Their Keyword Search Information.

128. Government conduct is a Fourth Amendment search if it involves an incursion

into areas where someone has a property interest. *See Jones*, 565 U.S. at 404-05. 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. As Google testified, it is a part of a user's "account contents," *Exhibit 10 (8/19/22 Tr.)* at 27 & 31, just like emails, photos, or documents that a user stores with Google. It is one's digital property. And because the government trespassed upon this property interest, it was a search under the Fourth Amendment. *See Jones*, 565 U.S. at 404-05 (placing a GPS tracker on a car is a trespass and thus a search); *Kyllo v. Unitd States*, 533 U.S. 27, 37 (2001) (using a thermal imager on a home is a search); *Silverman v. United States*, 365 U.S. 505, 512 (1961) (using a "spike mike" on a party wall intrudes into a constitutionally protected area and is a search); *see also Carpenter*, 138 S. Ct. at 2257 (Gorsuch, J., dissenting) (urging the Court to apply a property law analysis to the search of historical cell phone location information).

129. This more "traditional approach" asks "if a house, paper or effect was *yours* under law." *Carpenter* 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 40 ("well into the 20th

century, our Fourth Amendment jurisprudence was tied to common-law trespass"); *Soldal v. Cook County*, 506 U.S. 56, 62 (1992) ("our cases unmistakably hold that the Amendment protects property as well as privacy"); *Weeks v. United States*, 232 U.S. 383, 391 (1914) (recognizing that the essence of a Fourth Amendment violation is "the invasion of his indefeasible right of personal security, personal liberty, and private property."); *Ex parte Jackson*, 96 U.S. 727, 732-33 (1878) (holding that postal mail is just as protected under the Fourth Amendment as those papers and effects kept in the safety of one's home).

130. From a property law perspective, any intrusion into Mr. Seymour's Google account data, even one that does not implicate strong privacy interests, is a trespass under the Fourth Amendment. For example, in *Soldal*, the Supreme Court unanimously held that removal of a tenant's mobile home was a Fourth Amendment seizure even though the owner's "privacy" was not invaded. 506 U.S. at 62 ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Likewise, in *Kyllo*, Justice Scalia found that the use of a thermal imager on a home was a search, even though it only produced a "crude visual image" and "[n]o intimate details of the home were observed." 533 U.S. at 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained.").

And finally, in *Jones*, the Court's opinion rested on trespass grounds. 565 U.S. at 404-05. The *Jones* Court found that placement of a GPS tracker on a car was a "physical intrusion" that "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted," regardless of how long the surveillance lasted. *Id.*

131. Thus, it is highly relevant 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 Exhibit 21 (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).

132. 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. *Exhibit 21 (Google Terms of Service)*. 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.

133. 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).

134. Account holders can also delete their search history. *See Exhibit 10 (8/19/22 Tr.)* at 27-28. ("[I]t's up to the user if they've kept the searches saved."). *See also Exhibit 11 (Google Privacy Policy)* (consistently referring to user data as "your information," which can be managed, exported, and even deleted from Google's servers at "your" request). Businesses do not let customers delete the company's records at will. Rather, search history is part of a user's account contents—i.e., their property. *See Exhibit 10 (8/19/22 Tr.)* at 27, 31. Mr.

Seymour merely entrusted his information to Google, as so many people do.[14] *Id.* at 31. His account contents are not Google's "business records."

135. 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*, 590 F. Supp. 3d at 929 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

[14] As Justice Gorsuch explained in *Carpenter v. United States*, "[e]ntrusting your stuff to others is a bailment. A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose.'" 138 S. Ct. 2206, 2268–69 (2018) (Gorsuch, J., dissenting). Here, Google is the bailee, and it owes a duty to the bailor, Mr. Seymour, to keep his data safe.

possibility.

136. On the contrary, Google represents that information like search history is private user data that cannot be publicly disclosed. As Ms. Adeli testified on behalf of Google during the preliminary hearing, it is not Google's data; it is the users' data, which Google holds in trust. *See Exhibit 10 (8/19/22 Tr.)* at 27, 31. 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) (calling 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….").

137. The Supreme Court has also 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.").

138. 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.

139. 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.

140. In his oral ruling, however, Judge Egelhoff did not acknowledge this possessory interest. Rather, the court stated that the warrant "was not a search of any individual user account. It wasn't a search of any particular person or user. As I understand it, it wasn't even a search for any specific content of any—of the information in the internet." *Exhibit 8 (11/16/22 Tr.)* at 19. In the court's view, it appears, the warrant was simply "a database query submitted to the custodian of the database, which was Google." *Id.* at 20. But this data does not belong to Google. Rather, a more apt analogy would be a digital bank vault containing billions of safe deposit boxes, the online homes for the digital papers and effects of Google users. It is a repository of their personal papers and effects – their search history and other account contents – which belong to them. *See Exhibit 10 (8/19/22 Tr.)* at 27. A warrant to search all of Google search history records would be like making that bank search the contents of every safe deposit box, worldwide, for evidence of a crime.

141. Mr. Seymour had both a reasonable expectation of privacy and a possessory interest in his 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.

142. The government commanded Google to search Mr. Seymour's data, as well as the data belonging to every other user of Google during the relevant timeframe, and provide it to the Denver Police Department. That the search concerned a street address does not lessen the Fourth Amendment's guarantees. On the contrary, the keyword warrant directly infringed on Mr. Seymour's Fourth Amendment interests in order to identify and obtain evidence against him.

II. The Keyword Warrant Is Unconstitutional.

143. 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. *U.S. Const. amend. IV*; *Colo. Const. art. II, § 7*; *Dalia v. United States*, 441 U.S. 238, 255 (1979). *See also People v. Cox*, 439 P.3d 75, 70 (Colo. 2018); *People v. Pacheco*, 175 P.3d 91 (Colo. 2006).

144. 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.

145. 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.

146. 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). *See also People v. Coke*, 461 P.3d 508, 516 (Colo. 2020) (holding that "[g]eneral warrants," which permit "a general, exploratory rummaging in a person's belongings," are prohibited).

147. 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*, 365 U.S. at 511 ("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.").

148. 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).

149. 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.

150. 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*, 460 U.S. at 283-84, 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." That time is now.

151. 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*, 590 F. Supp. 3d at 927 (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 Was Overbroad.

152. 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.[15] If the government had probable cause to search 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.

153. 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.*

---

[15] 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 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.

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. *See also United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) (stating that "[t]he connection between the [location to be searched] and the evidence of criminal activity must be specific and concrete, not 'vague' or 'generalized,'" and that "the affidavit must suggest 'that there is a reasonable cause to believe that the specific 'things' to be searched for and seized are located [in the location to be searched] and not merely 'that the owner of the property is suspected of a crime.'").

154. 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 Exhibit 16 (11/19/20 Keyword Search Warrant)* at 3053–59 *with Exhibit 12 (10/1/20 Keyword Search Warrant)* at 2596–601 and *Exhibit 14 (10/20/20 Keyword Search 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. *Exhibit 16 (11/19/20 Keyword Search Warrant)* at 3055–56. However, 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*.

155. This was pure, unsupported conjecture. At the time, investigators simply "didn't know" who they were looking for. *Exhibit 9 (11/12/21 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 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.

156. If, on November 19, 2020, the Denver Police Department had sought a warrant for only Mr. Seymour's Google data, they would not have had probable cause to support it. By Detective Sandoval's own admission, he did not know who Mr. Seymour was prior to the third keyword warrant. *See Exhibit 10 (8/19/22 Tr.)* at 83. Mr. Seymour was not a suspect in the case at that point, and Detective Sandoval admitted he did not have probable cause to search him. *Id.* Specifically, Detective Sandoval testified that he did not believe he had probable cause to search Mr. Seymour's Google account prior to the keyword warrant. *Id.* ("Q. Would you say you had cause, by which I mean probable cause, to search [Mr. Seymour's] Google account prior to the keyword search warrant? A. I don't believe so, and we did not do that.").

157. Detective Sandoval's admission is highly probative. If the police did not have probable cause to search Mr. Seymour's account, then they also did not have probable cause to search Mr. Seymour's account plus billions more.

158. The truth of the matter, according to Detective Sandoval, was that the police

had nothing more than a "hunch" that the address "could have possibly been searched." *Exhibit 10 (8/19/22 Tr.)* at 83. A "hunch," however, is not probable cause. A "hunch" is not even enough to create reasonable suspicion, and it is "obviously less than is necessary for probable cause." *Kansas v. Glover*, 140 S. Ct. 1183, 1187 (2020) (quoting *Navarette v. California*, 572 U.S. 393, 397 (2014)).

159. The government maintains that because they describe the evidence that they want with specific detail, they do not need probable cause to search any particular account. The Fourth Amendment, however, requires probable cause for both the things to be seized and the places to be searched. *Cox*, 429 P.3d at 79. Thus, for example, when seeking a warrant to search an apartment or apartments in a multi-unit dwelling, it is insufficient to merely identify the larger structure and not the particular subunits to be searched. *See People v. Avery*, 478 P.2d 310, 312 (Colo. 1970) ("The basic philosophy that a man's home is his castle applies no less to an apartment dweller's apartment or to a roomer's room; and it is not to be invaded by any general authority to search and seize his goods and effects."). This is equally true when officers "knew or should have known" that the house was not a one-family residence. *See People v. Alarid*, 483 P.2d 1331, 1332 (Colo. 1971); *see also* 2 Wayne R. LaFave, *Search and Seizure: A Treatise On The Fourth Amendment* § 4.5(b) (6th ed.

2021) ("[T]he probable cause requirement would be substantially diluted if a search of several living units could be authorized upon a showing that one of the units within the description, not further identifiable, probably contained the items sought.").

160. 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).

161. 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." 590 F. Supp. 3d at 933. That inverted probable cause argument is the same one being made regarding keyword warrants in this case and similarly must be rejected.

162. In this case, the warrant identifies Google's headquarters as the place to be searched. However, Google's search history database is like an apartment building with billions of units.[16] The data inside belongs to individual users and is a part of each user's account contents, which in turn are private and inaccessible to other users. *See Exhibit 10 (8/19/22 Tr.)* at 27. Moreover, police knew that they would be searching the data from more than one account in the database, even if they did not know exactly how many. Detective Sandoval testified that he believed the search would cover at least the accounts in

[16] It is appropriate for this Court to consider the nature of Google's search history database, just as it was appropriate for this Court to consider the nature of the residences in *Avery* and *Alarid*. *See Avery*, 478 P.2d at 312; *Alarid*, 483 P.2d at 1332. The *Cox* decision only considered extrinsic evidence in the context of a probable cause determination. *See* 429 P.3d at 81. It did not discuss the use of extrinsic evidence in a particularity challenge, which necessarily requires the use of such evidence. For example, in *Alarid*, the warrant appeared to be sufficiently particularized on the four corners because it named a specific address. However, based on extrinsic evidence introduced at the hearing, the Court found that it was insufficiently particular. *See* 483 P.2d at 1332. Moreover, the *Cox* Court recognized that evidence outside the "four corners" of the affidavit will often be necessary to assess the affiant's good faith and veracity. *See* 429 P.3d at 79.

Colorado. *See id.* at 79.

163. It was therefore insufficient for the warrant to merely identify "1600 Amphitheater Parkway" as the place to be searched, as the affidavit did not establish probable cause for each account subject to the reverse keyword query. Instead, as it has been standard practice for decades, the warrant should have identified specific accounts and established specific probable cause to search them. It is not enough to believe that evidence exists in some to-be-determined Google account. *See Commonwealth. v. Douglas*, 503 N.E.2d 28, 30 (Mass. 1987). There must be a nexus between the crime and each account to be searched. *See Ybarra*, 444 U.S. at 91 ("Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person. This requirement 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.").

164. Similarly, the warrant failed to establish probable cause of the search history that police seized, just as it did not establish probable cause to search it. Probable cause to seize data must also be particularized. *See Chatrie*, 590 F. Supp. 3d at 929. Here, however, the warrant did not include any facts to justify

collecting private search history data from each individual whose data was produced to the police. *See id.* at 21. In fact, it remains unclear exactly how many users had their data seized. *See Exhibit 10 (8/19/22 Tr.)* at 60-62. At the preliminary hearing, the government testified that Google produced data regarding five "accounts," *Exhibit 9 (11/12/21 Tr.)* at 192, but the warrant return contains search data associated with four additional "Cookie IDs," suggesting that the data belonged to as many as nine different people.

165. Furthermore, the affidavit assumed that a search for the Truckee St. address was indicative of criminal activity, but it did not account for the fact that someone may have conducted an address search for any number of reasons unrelated to the commission of a crime. *See Tattered Cover*, 44 P.3d at 1063. This is evident from the fact that the government seized user data for about 61 searches for Truckee St., many of which involved searches outside of Colorado or unrelated to the crime. In fact, as the EFF observes, "there are streets named 'Truckee' in several cities and towns in Colorado, as well as in Arizona, California, Idaho, and Nevada." *Exhibit 2 (EFF amicus)* at 11. Moreover, 45 of the 61 searches returned contained additional terms that went beyond the nine variations of "5312 Truckee St." specified in the warrant, rendering its execution overbroad as well.

166. In sum, the keyword warrant here is void for overbreadth on its face as well as in its execution. 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.

167. The Fourth Amendment requires that warrants "particularly describ[e]" the things to be searched and seized. *U.S. Const. amend. IV*; *Colo. Const. art. II, § 7.* Its purpose is "to prevent the use of general warrants authorizing wide-rummaging searches in violation of the Constitution's prohibition against unreasonable searches and seizures." *People v. Eirish*, 165 P.3d 848, 852 (Colo. App. 2007) (citation omitted). *See also Voss v. Bergsgaard*, 744 F.2d 402, 404 (10th Cir. 1985) ("[T]he 'particularity' requirement ensures that a search is confined in scope to particularly describe evidence relating to a specific crime for which there is a demonstrated probable cause.").

168. 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). The keyword warrant here violates the particularity requirement because it granted the government and Google broad discretion to search private data, neglecting the reality that almost all the information to be searched would be unrelated to the investigation.

169. 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.

590 F. Supp. 3d at 929-30. 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.

170. 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. According to Google, there are more than 1 billion average monthly users of Google Search. *Exhibit 10 (8/19/22 Tr.)* at 40. There are also more than 1 billion average monthly users of Google Maps. *Id.* Google testified that when it executes a keyword search warrant, it queries data belonging to authenticated (i.e., signed-in) users of both services. *Id.* at 26, 37. Google also testified that it searches the data belonging to unauthenticated (i.e., not signed-in) users, *id.* at 37, although it remains unclear how many additional users that represents. In any event, since 2016, Google has publicized the fact that it has a billion monthly users for both Google Search and Google Maps. *Exhibit 4 (Declaration of Nikki Adeli)* at ¶ 4. Law enforcement should have known that searching fifteen days of search history at "1600 Amphitheater Parkway" would

potentially intrude on the property and privacy interests of over a billion Google users.

171. Despite this, the keyword warrant gave law enforcement the discretion to rummage through everyone's keyword data. By contrast, in *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 at 516. 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. As a result, it was insufficiently particular to describe the place to be searched as Google headquarters instead of identifying specific user accounts to search. *See Alarid*, 483 P.2d at 1332; *Avery*, 478 P.2d at 312; *see also Chatrie*, 590 F. Supp. 3d at 929. The government should be required to target specific Google accounts to search through "objective guardrails" and benchmarks, *Chatrie*, 590 F. Supp. 3d at 934, instead of what happened here, where the warrant made no attempt to limit the number of accounts subject to search. The failure to identify Mr. Seymour's account, or any other account, left the discretion to Google and the government to determine which accounts to search and what data to seize. This 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.

172. The warrant also failed to cabin the data that the government could seize. The government attempts to justify the warrant by claiming that the search parameters describe the data to be seized with sufficient detail, but the warrant did not specify how to determine which search history data was responsive. Google testified that there are two ways to count responsive data: 1) "exact matches" to the search terms in the warrant, or 2) searches that "contain other words." *Exhibit 10 (8/19/22 Tr.)* at 43-44. Google "more commonly" follows the second method, even where the search results strongly imply that a search is irrelevant, *Exhibit 4 (Declaration of Nikki Adeli)* at ¶ 6-8, but testified that it relies on what the warrant specifies. *Exhibit 10 (8/19/22 Tr.)* at 45.

173. Where, as here, the warrant does not specify one way or another, Google escalates the matter to outside legal counsel. *Id*. In this case, Google did communicate with Detective Sandoval on multiple occasions prior to complying with the third keyword warrant. *Id.* at 74-75. Nonetheless, Detective Sandoval testified that he does not "know what Google does when they conduct these searches," *id.* at 78, and it is not clear how the decision was made here. What is clear, however, is that only 5 of the 61 searches that were produced to

police matched the terms in the warrant (45 contained "other words" and 11 had no clear search terms at all). Most importantly, it is clear that Judge Zobel had no role in deciding whether police could seize this additional account data, either when approving the warrant or afterwards. *See Exhibit 10 (8/19/22 Tr.)* at 77. Placing such discretion in the hands of Google and the government is the hallmark of an unparticularized warrant, leading here to the over-seizure of 56 search history records.

174. 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.

175. 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.

176. 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." C.R.S. § 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).

177. There is no good faith in relying on a general warrant. *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"). To hold otherwise would incentivize the kind of "systematic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring v. United States*, 555 U.S. 135, 144 (2009); *see also United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring) (finding that when a warrant is void, "potential questions of 'harmlessness'" do not matter); *United States v. Winn*¸ 79 F. Supp. 904, 926 (S.D. Ill. 2015) ("Because the warrant is a general warrant, it has no valid portions.").

178. 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.

179. 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. The warrant here is nothing short of a general warrant, antithetical to the Fourth Amendment. As such, the good-faith doctrine does not apply.

A. Knowing or Recklessly False Statements

180. Investigators were anxious to solve this case. They obtained search warrants for specific individuals' cell phone and Google data. *Exhibit 9 (11/12/21 Tr.)* at 72-76. But when these efforts proved unfruitful, their tactics shifted. *Id.* at 47. They cast digital dragnets, each bigger than the last, issuing "very general" search warrants, *id.* at 61–62, that swept up hundreds and thousands of people. *See id.* at 70–71, 127–28. And the keyword warrant was the biggest dragnet of them all.

181. When Detective Sandoval submitted the keyword warrant affidavit, he was aware, or should have been aware, that it would entail the search of billions of people. At a minimum, Detective Sandoval believed that the warrant would apply to anyone in Colorado. *See Exhibit 10 (8/19/22 Tr.)* at 79. Yet Detective

Sandoval recklessly omitted critical information about the unprecedented scope of the search to the issuing judge, and he did not inform the court about the likelihood of seizing sizable amounts of unrelated data. He failed to convey that the warrant 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.

182. In other words, the affidavit relied on false statements in the form of material omissions. *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"); *People v. Kerst*, 181 P.3d 1167, 1171 (Colo. 2008); *Leon*, 468 U.S. at 914 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)) (stating that the good-faith exception does not apply where a warrant is based on knowing or recklessly false statements). And this lack of candor was highly consequential. The Court should suppress the fruits of the keyword warrant for this reason alone, but it also speaks to the absence of good faith.

183. Had Detective 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 that the affidavit lacked a substantial basis to find of probable cause to cast such an indiscriminately broad net. It would have become apparent that there was no probable cause to search even a single account, including Mr. Seymour's. It would have become apparent that the keyword warrant was a general warrant.

184. That, however, is not what happened here. Detective 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); *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.").

185. The government obscured the warrant's deficiencies by cloaking them in the "complexities of novel technology." *Chatrie*, 590 F. Supp. 3d at 929. Even

Detective Sandoval testified that he did not understand "what Google does when they conduct these searches;" that he does not know "how they input it;" and that he does not know "how they look for it," even though he expected that the warrant would sweep at least statewide. *Exhibit 10 (8/19/22 Tr.)* at 78-79. Nonetheless, he asked Judge Zobel to rely on his "training and experience" in support of the keyword warrant affidavit. *Exhibit 16 (11/19/20 Keyword Search Warrant)* at 3053*; see also Exhibit 10 (8/19/22 Tr.)* at 144.

186. It is possible that Detective Sandoval did not know exactly how many people would be searched by the keyword warrant, but that 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").

187. It is apparent, however, that investigators had at least some idea of the scope of the search. Det. Baker stated that he believed the search covered the entire state of Colorado. *See Exhibit 9 (11/12/21 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.

188. In truth, Detective Sandoval had received no training on keyword warrants. He had no training from the Denver Police Department because there were no police policies, procedures, or memos concerning keyword warrants. *See Exhibit 10 (8/19/22 Tr.)* at 68-69. The technique had not been vetted by the Denver Police Department or by the District Attorney's office. *Id.* Two years later, Detective Sandoval remains unclear whether the Department has approved it. Similarly, Detective Sandoval received no training on keyword warrants from the ATF, where he served as a deputy agent during this case. *Id.* at 69. Detective Sandoval testified that he was not aware of any ATF policies or procedures for obtaining a keyword warrant, and that he had received no official training from ATF regarding them. *Id.*

189. Simply put, Detective Sandoval misled Judge Zobel about his training and

experience and omitted material facts about how the keyword warrant would operate. He did not explain that the warrant would require Google to search the data belonging to billions of people, despite the fact that he later testified that he expected that the warrant would sweep at least statewide. *Exhibit 10 (8/19/22 Tr.)* at 77, 79.

190. Similarly, Detective Sandoval implied that the search was more limited or different than it really was by invoking the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2703, as authorization for the search in the warrant affidavit. *See Exhibit 16 (11/19/20 Keyword Search Warrant)* at 3052. The SCA permits the government to search data belonging to "a subscriber" of a third-party service. 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.[17]

191. 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*, 590 F. Supp. 3d at 927 (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 (1987) (declining to apply good-faith exception "when police

[17] 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 Subp. 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").

officers act outside the scope of a statute, albeit in good faith"). Had Detective Sandoval truthfully described the nature of the keyword warrant to Judge Zobel, it would have been clear that the SCA, a law enacted in 1986, does not authorize such reverse searches. *See Exhibit 10 (8/19/22 Tr.)* at 84-85. A reverse keyword warrant is plainly not the kind of search authorized by the SCA, and citing it here was reckless and misleading.

192. Likewise, the promise of providing "deidentified" data is empty and misleading. Although the process outlined in the warrant required Google to produce only an "Anonymized List" of results, it also required Google to provide identifying information in the form of IP addresses. *TR 8/19/22, pp 86*. 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. 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 Exhibit 18 (12/4/20 Google 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.").

193. Detective Sandoval was aware that he could use an IP address to identify the physical location associated with the search history data. *See Exhibit 10 (8/19/22 Tr.)* at 86-88. In fact, Detective Sandoval did so with the data provided in this case, showing one IP address linked to Mr. Seymour's address. *Id.* Although Detective Sandoval obtained an additional warrant for this information, that warrant relied on the fruits of the keyword warrant – the IP addresses. However, Detective 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.

194. Finally, the application omitted that Google had refused to comply with two previous keyword warrants that were signed by a different judge. *See Exhibit 10 (8/19/22 Tr.)* at 76. 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*) at ¶ 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. In the process, Detective Sandoval had multiple conversations with Google's legal counsel at Perkins Coie, LLP, about those perceived deficiencies and how to correct them. *See Exhibit 10 (8/19/22 Tr.)* at 73-76.

195. However, Detective Sandoval failed to provide any of this information to Judge Zobel in the November 19, 2020, warrant application, which required Google to produce full IP addresses, despite Detective Sandoval knowing that the IP addresses were personally identifiable. 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.

196. In sum, the government failed to apprise the judge of critical facts that prevented the judge 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. Omitting such material facts demonstrates Detective Sandoval's knowing or reckless disregard for the true nature of the dragnet search that occurred in this case. At a minimum, Detective Sandoval should have been aware of the unprecedented nature of this search based on his repeated discussions with Google's counsel. To the extent Detective Sandoval remained unaware of how a keyword warrant works, he assumed the risk of suppression by recklessly omitting critical information and making false representations in his affidavit.

B. Lacking in Indicia of Probable Cause

197. 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.

198. As discussed *supra*, the warrant 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. The same logic could be invoked in any case, even if, as here, there are no facts to justify it.

199. Similarly, the warrant was so obviously lacking in particularity that no reasonable officer could presume it was valid. It failed to identify a single account, instead describing the place to be searched as simply "1600 Amphitheater Parkway," the street address for the equivalent of a billion-story apartment building. It failed to limit or adequately describe what the government could seize, resulting in a warrant return where the overwhelming majority of the data produced was inconsistent with its terms.

200. 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." *Exhibit 9 (11/12/21 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. During the Motions Hearing, Detective Sandoval even admitted that he did not think he had probable cause to search Mr. Seymour's Google account and that the keyword warrant was based on a mere "hunch." *Exhibit 10 (8/19/22 Tr.)* at 83. In short, the warrant application lacked a substantial basis to determine probable cause for searching anyone's Google data, let alone billions.

201. 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*, ¶¶ 153-54.

202. The government used the same basic statement of probable cause to justify the litany of warrants before the third keyword warrant, tempered only with descriptions of the searches they sought to conduct. There was nothing in those

facts to establish probable cause to search anyone, let alone everyone. And as every officer knows, obtaining warrants based on a mere "hunch," *Exhibit 10 (8/19/22 Tr.)* at 83, is impermissible. It 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

203. 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.

204. 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.[18] 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 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

[18] 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).

also establish a cornerstone criminal justice of America. *Id* at 1320.

205. The unique nature of this warrant—a reverse warrant—was apparent to Detective Sandoval. In 15 years as a police officer, he had never before used a keyword warrant. *See Exhibit 10 (8/19/22 Tr.)* at 68. Moreover, 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. *See id.* at 68-69. 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").

206. There is a lot that is new about this case, but it is not new that warrants must be supported by probable cause and must be particularized. 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.

Supporting Documents:

207. Attached are the following exhibits:

1. Motion to Suppress Evidence from a Keyword Warrant and Request for a Veracity Hearing (Exhibit 1);
2. Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant's Motion To Suppress (Exhibit 2);
3. Response to Motion to Suppress Evidence from a Keyword Warrant and Request for a Veracity Hearing (Exhibit 3);
4. Nikki Adeli's Declaration of Legal Investigations Support Analyst (Exhibit 4);

5. Defendant's Reply to People's Responses to Motion to Suppress Evidence From a Keyword Warrant and Motions to Suppress Evidence Unlawfully Obtained (Exhibit 5);
6. People's Reply to Defendant's Motion to Suppress (Exhibit 6);
7. Defendant's Response to People's Written Arguments on Defendant's Motions to Suppress (Exhibit 7);
8. Reporter's Transcript 11/16/2022 (Exhibit 8);
9. Reporter's Transcript 11/12/2021 (Exhibit 9);
10. Reporter's Transcript 8/19/2022 (Exhibit 10);
11. Google's Privacy Policy (Exhibit 11);
12. Keyword Search Warrant 10/1/2020 (Exhibit 12);
13. Supplementary Report (Exhibit 13);
14. Keyword Search Warrant 10/20/2020 (Exhibit 14);
15. Email with Google and Hayley Berlin (Exhibit 15);
16. Keyword Search Warrant 11/19/2020 (Exhibit 16);
17. Keyword Warrant Return Data (Exhibit 17);
18. Google Warrant 12/4/2020 (Exhibit 18);
19. Report of Investigation Number 7 (Exhibit 19);
20. Comcast Warrant Return (Exhibit 20);
21. Google Terms of Service (Exhibit 21).

Dated this day: January 11, 2023

/s/ Jenifer Stinson

_____

Attorney: Jenifer Stinson, #35993

_____

Attorney: Michael S. Juba, #39542

_____

Attorney: Michael W. Price, #22PHV6967

CERTIFICATE OF SERVICE

Parties: IN RE: PEOPLE OF THE STATE OF COLORADO V. GAVIN SEYMOUR

I hereby certify that on January 11, 2023, a true and correct copy of this Petition (with exhibits) was served upon the following by emailing a copy to each person listed:

Joseph Morales Courtney Johnston Honorable Judge Martin Egelhoff

Denver District Attorney
201 W. Colfax Ave.
Denver, CO 80202
jxm@denverda.org

Denver District Attorney
201 W. Colfax Ave.
Denver, CO 80202
clj@denverda.org

Denver District Court
520 W. Colfax Ave.
Denver, CO 80204
martin.egelhoff@judicial.state.co.us

Attorney: Michael S. Juba, #39542