DISTRICT COURT, DENVER COUNTY, COLORADO 520 W. Colfax Denver, Colorado 80204	DATE FILED: September 16, 2022 4:12 PM FILING ID: EA234FC1E8E7F CASE NUMBER: 2021CR20001
PEOPLE OF THE STATE OF COLORADO, Plaintiff, v. GAVIN SEYMOUR, Juvenile Defendant.	σ COURT USE ONLY σ
JENIFER STINSON (#35993) Stinson Law Office 1245 E. Colfax Avenue, Suite 300 Denver, Colorado 80218 Phone: (303) 483-3161 E-mail: JStinsonLaw@gmail.com MICHAEL S. JUBA (#39542) Juba Law Office, PLLC 675 N. Grant Street Denver, CO 80203 Phone: (303) 974-1080 E-mail: Juba@JubaLawOffice.com MICHAEL W. PRICE (#22PHV6967) National Association of Criminal Defense Lawyers 1660 L Street NW, 12th Floor Washington, DC 20036 Phone: (202) 465-7615 E-mail: MPrice@NACDL.org	Case Number: 21CR20001 Division: 5A

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]

Gavin Seymour, through counsel, submits the following Reply to the People's Responses:

Factual Background:

1. On June 17, 2022, counsel filed the following Motions relevant to this Reply:

(a) Motion to Suppress Evidence Unlawfully Obtained (Accounts) [DEF-25]
(b) Motion to Suppress Evidence Unlawfully Obtained (Cellphone Records) [DEF-26]
(c) Motion to Suppress Evidence Unlawfully Obtained (Cellphone Data) [DEF-27]
(d) Motion to Suppress Evidence Unlawfully Obtained (Home) [Def-29]
(e) Motion to Suppress Evidence Unlawfully Obtained (Social Media) [DEF-30]
(f) Motion to Suppress Statements and Observations Obtained in Violation of Gavin Seymour's Constitutional Rights to Remain Silent and To Counsel [Def-37]

2. On June 30, 2022, counsel also filed a Motion to Suppress Evidence from a Keyword Warrant and Request for a Veracity Hearing.

3. On July 15, 2022, the People filed a Motion For Court to Set Deadline for People's Responses to Defendant's Motions. On July 18, 2022, this Court issued an order requesting guidance from the People regarding how much time the People would need to prepare adequate responses and what would constitute a reasonable deadline for such responses. On July 21, 2022, the People responded stating that they would need until August 12, 2022, and this Court granted the motion on July 26, 2022.

4. August 12, 2022, the People filed the following Responses relevant to this Reply:

   (a) Response to Motion to Suppress Evidence Unlawfully Obtained (Accounts) [DEF-25]
   (b) Response to Motion to Suppress Evidence Unlawfully Obtained (Cellphone Records) [DEF-26]
   (c) Response to Motion to Suppress Evidence Unlawfully Obtained (Cellphone Data) [DEF-27]
   (d) Response to Motion to Suppress Evidence Unlawfully Obtained (Home) [Def-29]
   (e) Response to Motion to Suppress Evidence Unlawfully Obtained (Social Media) [DEF-30]
   (f) Response to Motion to Suppress Statements and Observations Obtained in Violation of Gavin Seymour's Constitutional Rights to Remain Silent and To Counsel [Def-37]
   (g) Response to Motion to Suppress Evidence from a Keyword Warrant and Request for a Veracity Hearing.

5. On August 19, 2022, this Court held a Motions Hearing. During the hearing, the Court received testimony from two witnesses: Nikki Adeli from Google and Det. Ernest Sandoval from the Denver Police Department. *TR 8/19/22, pp. 24-91 (Attachment 1).*

6. At the conclusion of the hearing, this Court permitted counsel and the People to file supplemental briefings due September 16, 2022.

7. Mr. Seymour requests the Court suppress the evidence unlawfully obtained from the warrants referenced above based upon violations of the Fourth Amendment to the United

States Constitution, and article II, Section 7 of the Colorado Constitution. Mr. Seymour requests the Court suppress Mr. Seymour's statements to police during his in-custody interview under *Miranda v. Arizona*, 384 U.S. 436 (1966).

I. Keyword Warrant

8. The 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 arson had searched for 5312 Truckee Street. *TR 8/19/22, pp. 83:2 (Attachment 1)*. In applying for this general warrant, Det. Sandoval failed to disclose that he had no experience or training on how the search would be executed, that it would necessitate a search across billions of private accounts, that it would not be limited to the terms contained in the warrant, that it had no geographic limits, or that the "deidentified" data was actually identifiable. The government now urges the court to ignore evidence withheld from the issuing judge and ask this court to find, in part, that the government acted in "good faith."

9. Mr. Seymour maintains that the keyword warrant used to search his Google account, as well as billions of other accounts, violated 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.

10. Mr. Seymour had a privacy interest in his Google search history because, as Google testified, the data belongs to him. It is definitively not a business record. Search history is also such intensely private data that Mr. Seymour had a reasonable expectation of privacy in it.

11. Mr. Seymour has standing to challenge the warrant because his data was searched. Furthermore, the search was overbroad because, as Det. Sandoval testified, there was no probable cause to search Mr. Seymour's data, nor the data of billions of other Google users. *TR 8/19/22, pp. 83:16-22 (Attachment 1*. The warrant failed to identify Mr. Seymour's account as a target of the search, and indeed failed to identify any account at all, rendering it wholly unparticularized.

12. Finally, Mr. Seymour urges this court to find that the good faith doctrine does not apply. The keyword warrant was the digital equivalent of an unconstitutional general warrant, upon which there can be no reliance in good faith. Additionally, it was based on knowing or recklessly false statements, lacked a substantial basis to determine probable cause, and was so unparticularized that no officer could have reasonably presumed it was valid. *See United States v. Leon*, 468 U.S. 897, 914-15; 926 (1984).

A. Mr. Seymour Had Fourth Amendment Property and Privacy Interests in His Search History Data.

13. Mr. Seymour's search history data is his property. Google does not own it; Mr. Seymour does. As Ms. Adeli testified on behalf of Google, search history is a part of a user's "account contents." *TR 8/19/22, pp. 27:2-7; 31:2-4 (Attachment 1)*. Just like emails,

photos, or documents that a user stores with Google, their search history is data that belongs to them.

14. That is why Mr. Seymour retains the right to exclude other people from accessing his account contents. *See id.* at 31; *see also 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) (calling the right to exclude "one of the most essential sticks" in the property rights bundle).

15. It is also why Mr. Seymour can delete his search history. *See TR 8/19/22, pp. 27:24-25; 28:1-2; 28:3-6 (Attachment 1)* ("[I]t's up to the user if they've kept the searches saved."); *see also* Google, Privacy Policy (Oct. 26, 2019), https://policies.google.com/privacy#infodelete (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. *TR 8/19/22, pp. 27:2-7; 31:2-4 (Attachment 1)*. Mr. Seymour merely entrusted his information to Google, as so many people do.[1] *TR 8/19/22, pp. 31 (Attachment 1)*. His account contents, however, are not Google's "business records."

16. Consequently, 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 v. Cook County*, 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. 56, 62 (1992) ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Likewise, in *Kyllo v. United States*, 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. 27, 37 (2001) ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Indeed, the *Kyllo* Court noted that "well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." *Id*. at 40. And finally, in *United States v. Jones*, the Court's opinion rested on trespass grounds. 565 U.S. 400, 404-05 (2012). 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."

17. Mr. Seymour's account contents are his digital property. They are his "papers" and "effects," explicitly protected by the state and federal constitutions, and on par with one's person and home. *See* U.S. Const. amend. IV; Colo. Const. art. II, § 7. Any trespass to

[1] 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.

one's digital papers and effects is a Fourth Amendment search or seizure, requiring a valid warrant.

18. At the August 19 hearing, the Court asked about the difference between searching the FBI's fingerprint or DNA databases and searching Google users' search history data. The Court remarked that "it strikes me to be a difference between fingerprints and blood and digital stuff is who owns the database." Tr. at 103. Indeed, the question of who owns search history data is critical to the Fourth Amendment question at bar. But it is now clear that Mr. Seymour—not Google or the government—owns his account contents, including search his search history. *See* Tr. at 103-04.

19. With respect to ownership, therefore, Google account contents are fundamentally different from fingerprints or blood, which are physical items abandoned at a crime scene. And consequently, the database housing Google users' search histories is not like the FBI's Integrated Automated Fingerprint Identification System ("IAFIS") (fingerprint database) or its Combined DNA Index System ("CODIS"). *See* Tr. at 103-04, 108, 112. For both IAFIS and CODIS, the government collected and analyzed the fingerprints and DNA samples in those databases. The FBI owns the data and can search it without a warrant. By contrast, a user's Google account contents belongs to the user—not to Google, not to the government, and not to anyone else. The database where Google stores users' search data is not some meaningless collection of "ones and zeroes," as the government argues. *People's Response to Motion to Suppress Evidence From a Keyword Warrant and Request for a Veracity Hearing, pp. 3*. 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 TR at 36 (Attachment 1)*. A warrant to search of all Google search history records would be like making that bank search the contents of every safe deposit box, worldwide, for evidence of a crime.

20. In addition to a property interest, Mr. Seymour also had a reasonable expectation of privacy in his Google search history. In fact, the government appears to concede this point, stating that "[t]he People are not suggesting that this was not a search at all." *People's Response, pp. 3* Instead, the government seeks to diminish its intrusion by emphasizing that its search was for a street address. *Id.* ("[I]t was not the type of search that would expose . . . 'deeply private facts about a person.'").

21. But as the Electronic Frontier Foundation ("EFF") observes 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.)." *EFF amicus, pp. 5.* Likewise, a search for "6260 E Colfax Ave" (an HIV/AIDS screening center) or "2525 W Alameda Ave" (SEIU Local 105 headqufarters) 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.

22. The Court should therefore follow the test established by *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1059 (Colo. 2002), 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 of a 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 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.

23. 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."). And 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.

24. Here, Mr. Seymour had both a property interest and a privacy interest in his Google search history data. And the government admittedly commanded Google to search that data—along with the data belonging to every other user of Google during the relevant timeframe—and provide it to the Denver Police Department. *See People's Response, pp.* 3. 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.

B. Overbreadth

25. If, on November 19, 2020, the Denver police had sought a warrant for only Mr. Seymour's Google data, they would not have had probable cause to support it. By Det. Sandoval's own admission, he did not know who Mr. Seymour was prior to the third keyword warrant. *TR 8/19/22, pp. 83:4-22 (Attachment 1)*. Mr. Seymour was not a suspect in the case before that point, and Det. Sandoval admitted he did not have probable cause to search him. *Id.* And specifically, Det. Sandoval testified that he did not believe he had probable cause to search Mr. Seymour's Google account prior to the

keyword warrant. *TR 8/19/22, pp. 83:19-22 (Attachment 1)* ("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.").

26. Det. 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. The government complains that Mr. Seymour does not have standing to assert the Fourth Amendment rights of these other Google users, *People's Response, pp. 3*, but Mr. Seymour does no such thing. Rather, Mr. Seymour agrees with Det. Sandoval that the police had no probable cause to search his data and submits that nothing more is needed to find the keyword warrant overbroad.

27. In reality, it is the government that relies on the broad and programmatic nature of the keyword warrant, given that it does not specify any accounts to search. The warrant's entire purpose was to cast a digital dragnet, so it is not surprising that the affidavit offered only broad generalizations about the popularity of Google and speculation that the suspects used Google to search for the Truckee St. address. *People's Response, pp. 8*; *TR 8/19/22, pp. 11 (Attachment 1)*.

28. The truth of the matter, according to Det. Sandoval, was that police had nothing more than a "hunch" that the address "could have possibly been searched." *TR 8/19/22, pp.83:2-3 (Attachment 1)*. A "hunch," however, is plainly 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)).

29. The government maintains that because they describe the evidence they want with sufficient detail, they do not need probable cause to search any particular account. *Response, pp. 8*. The Fourth Amendment, however, requires probable cause for both the things to be seized and the place to be searched. *See People v. Cox*, 429 P.3d 75, 79 (Colo. 2018).

30. 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 & 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 some one of the units within the description, not further identifiable, probably contained the items sought.").

31. In this case, the warrant identifies Google's headquarters as the place to be searched. But Google's search history database is like an apartment building with billions of units.[2] 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 TR 8/19/22, pp. 27, 31 (Attachment 1)*. 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. Det. Sandoval testified that he believed the search would cover at least the accounts in Colorado. *See TR 8/19/22, pp. 79 (Attachment 1)*.

32. 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 has been standard practice for decades, the warrant should have identified specific accounts and established probable cause to search them. It is not enough to believe that evidence exists in some to-be-determined Google account. *See Com. 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 v. Illinois*, 444 U.S. 85, 91 (1979) ("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.").

33. Similarly, the warrant failed to establish probable cause for 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 United States v. Chatrie*, No. 3:19CR130, 2022 WL 628905, at *19 (E.D. Va. Mar. 3, 2022). 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 Motion to Suppress, pp. 9-10*; *see also TR 8/19/22, pp. 60-62 (Attachment 1)*. At the preliminary hearing, the government testified that Google produced data regarding five "accounts," *TR 11/12/21, pp. 192*, but the warrant return contains search data associated with four additional "Cookie IDs" as well as 12 distinct IP addresses, suggesting that the data belonged to five, nine, or 12 different people. *See Motion to Suppress, pp. 9-10*.

---

[2] It is appropriate for this Court to consider the nature of Google's search history database, just as it was appropriate for the Colorado Supreme 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.

34. 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 someone may have conducted an address search for any of 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 about 61 searches for Truckee St., many of which involved searches conducted outside 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." *EFF amicus, pp. 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. *See Motion to Suppress, pp. 9-10*. In sum, the seizure of search history data was overbroad on its face as well as in its execution.

C. Particularity

35. The keyword warrant lacks particularity for many of the same reasons it lacks probable cause. That is because, like the multi-family dwelling cases, the constitutional concerns here "fall at the confluence of the Fourth Amendment's probable cause and particularity requirements." *United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011). Here, the description of the place to be searched—"1600 Amphitheater Parkway"—is so broad and all-encompassing that it outruns any measure of probable cause in the affidavit and thus fails to limit police discretion. *See id.*

36. According to Google, there are more than 1 billion average monthly users of Google Search. *TR 8/19/22, pp. 40 (Attachment 1)*. And there are also more than 1 billion average monthly users of Google Maps. *Id.* When executing a keyword warrant, Google testified that it queries data belonging to authenticated (*i.e*., signed-in) users of both services. *Id.* at 26, 37. Google also testified that they search 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. *See Adeli Decl. at para. 4.* Thus, police should have known that searching 15 days of search history data at "1600 Amphitheater Parkway" would potentially intrude on the property and privacy interests of over a billion Google users.

37. 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*, 2022 WL 628905, at *21. The failure to identify Mr. Seymour's account, or any other account, left it up to Google and the government to determine which accounts to search and what data to seize. And in so doing, it led to an unprecedented dragnet of private account data that was inevitably unrelated to the investigation. *See Chatrie*, 2022 WL 628905, at *19.

38. The government misconstrues *Dixon v. United States*, 211 F.2d 547 (5th Cir. 1954), in support of its argument that "[i]t was not necessary to specify/identify the users of the particular accounts at the outset in order for the warrant to be valid." *People's Response, pp. 8*. *Dixon* concerned a warrant *caption* that did not identify Mr. Dixon by name, but

where the affidavit stated that an officer "saw the defendant and several other men at the defendant's home handling jugs of moonshine whiskey, and that he knew the defendant had this whiskey for sale." 211 F.2d at 548. And unlike the affidavit in this case, it "contain[ed] definite statements of fact, as distinguished from mere suspicions or conclusions, [and] . . . describe[d] the offense, the premises to be searched and the property to be seized." *Id.* at 549.

39. The government also cites *Warden v. Hayden*, 387 U.S. 294 (1967), which likewise offers no support for its position. *Hayden* abolished the "mere evidence" rule prohibiting the seizure of evidence for evidential value only. *Id.* at 300-01. The Court repeatedly emphasized, however, that the probable cause and particularity requirements must be met with respect to all evidence sought. *Id.* at 302, 307, 309. In *Hayden*, the Court determined that exigent circumstances justified the warrantless entry of a home while in pursuit of a suspect seen entering a residence less than five minutes prior. *Id.* at 298. And unlike this case, that information gave police probable cause to search a particular house, 2111 Cocoa Lane. *Id.* They would not have been justified, however, in searching every home in the neighborhood, or every home in Maryland. Far from supporting the government's position, *Hayden* and *Dixon* highlight what was missing in this case: probable cause to search a single Google account, let alone Mr. Seymour's.

40. Finally, the warrant 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. *People's Response, pp. 5*. 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." *TR 8/19/22, pp. 43-44 (Attachment 1)*. Google "more commonly" follows the second method, even where the search results strongly imply that a search is irrelevant, *Adeli Decl. at ¶¶ 6-8*, but testified that it relies on what the warrant specifies. *TR 8/19/22, pp. 45 (Attachment 1)*.

41. Where, as here, the warrant does not specify one way or the other, Google escalates the matter to legal counsel. *Id.* And in this case, Google's counsel did communicate with Det. Sandoval on multiple occasions prior to complying with the third keyword warrant. Tr. at 74-75. Nonetheless, Det. Sandoval testified that he does not "know what Google does when they conduct these searches," Tr. at 78, and it is not clear how the decision was made here. What is clear, however, is that only five of the 61 searches produced to police matched the terms in the warrant (45 contained "other words" and 11 had no search terms at all). *See Motion to Suppress, pp. 9-10*. And 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 TR 8/19/22, pp. 77 (Attachment 1)*. 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.

D. Good Faith / Veracity

42. 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 "systemic 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*, F. Supp. 3d 904, 926 (S.D. Ill. 2015) ("Because the warrant is a general warrant, it has no valid portions."). The warrant here is nothing short of a general warrant, antithetical to the Fourth Amendment. As such, the good faith doctrine does not apply.

43. Even under the *Leon* good-faith test, this keyword warrant falls far short on at least three fronts: (1) it was based on knowing or recklessly false statements; (2) it lacked a substantial basis to determine probable cause; and (3) no officer could reasonably presume it was valid. *See* 468 U.S. at 914-15, 926.

44. First and foremost, Det. Sandoval recklessly omitted critical information about the unprecedented scope of the search and did not inform the court about the likelihood of seizing sizable amounts of unrelated data. 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); *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). The court should suppress the fruits of the keyword warrant for this reason alone, but it also speaks to the absence of good faith.

45. Had Det. Sandoval apprised Judge Zobel of the true scope of the search and seizure requested, it would have become immediately apparent that the application lacked a substantial basis to find probable cause to search the private account contents of more than a billion Google users. 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. And undoubtably, Judge Zobel would not have signed it. But that is not what happened.

46. Instead, the government obscured the warrant's deficiencies by cloaking them in the "complexities of novel technology." *Chatrie*, 2022 WL 628905, at *20. Even Det. 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." Tr. at 78. Nonetheless, he asked Judge Zobel to rely on his "training and experience" in support of his keyword warrant application. *Keyword Warrant 3 Affidavit, pp. 2-3; see also TR 8/19/22, pp. 144 (Attachment 1)*.

47. In truth, Det. 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 TR 8/19/22, pp. 68-69 (Attachment 1)*. The technique had not been vetted by the Department or the District Attorney's office. *Id.* at 69. And Det. Sandoval remains unclear whether, two years later, the Department has approved it. *Id.*

48. Similarly, Det. Sandoval received no training on keyword warrants from the federal Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), where he served as a deputy agent during this case. *Id.* at 69. Det. 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.*

49. The fact remains, however, that a keyword warrant demands the search of private data belonging to billions of Google users. Det. Sandoval was or should have been aware of this fact, given Google's highly public pronouncements about their active monthly users. *See Adeli Decl. at para. 4.* At a minimum, Det. Sandoval believed the warrant would apply to anyone in Colorado. *See TR 8/19/22, pp. 79 (Attachment 1)*. Nonetheless, he failed to inform Judge Zobel that execution of the warrant would entail searching the data belonging to millions or billions of Google users, based within and without Colorado.

50. It does not lessen the intrusion to call the place where their data is stored a "database," as the government contends. *See People's Response, pp. 5* (arguing that the search "was simply a computer inquiry of a database"). The type of database matters. And the database here is the digital equivalent of a billion-story apartment building, housing the modern-day papers and effects of every person who has used Google Search or Google Maps. Providing the street address for Google headquarters as the place to be searched is meaningless if not highly misleading. It is like serving a warrant on the apartment building manager to have them peek inside every resident's diary in every unit.

51. Simply put, Det. 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. *TR 8/19/22, pp. 77 (Attachment 1)*. Indeed, he later testified that he did not know "what it took for Google to conduct the search." *id.*, even though he expected that the warrant would sweep at least statewide. *Id.* at 79.

52. Similarly, Det. 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. The SCA permits the government to search data belonging to "a subscriber" of a third-party service. It does not, however, permit bulk searches, and Det. Sandoval did not inform Judge Zobel that the keyword warrant was unlike anything contemplated by the SCA, a law enacted in 1986 *See TR 8/19/22, pp. 84-85 (Attachment 1)*.

53. 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 (Attachment 1)*. Det. Sandoval was aware

that he could use an IP address to identify the physical location associated with the search history data. *See TR 8/19/22, pp. 86-88 (Attachment 1)*. In fact, Det. Sandoval did so with the data provided in this case, showing one IP address linked to Mr. Seymour's address. *Id.* And while Det. Sandoval obtained an additional warrant for this information, that warrant relied on the fruits of the keyword warrant—the IP addresses.

54. Furthermore, Det. Sandoval did not inform Judge Zobel that Google had refused to comply with two previous keyword warrants issued by a different judge. Tr. at 76. Google had rejected them both because they sought identifying information and were not truly "anonymized." *TR 8/19/22, pp. 73-76 (Attachment 1)*. And in the process, Det. Sandoval had multiple conversations with Google's legal counsel at Perkins Coie, LLP, about those perceived deficiencies and how to correct them. *See id.* Nonetheless, the keyword warrant here required Google to produce full IP addresses, which Det. Sandoval knew to be personally identifiable. He did not apprise Judge Zobel of these facts, however, and consistently characterized the data sought as "anonymized information" and the "Anonymized List." *Keyword Warrant 3 Affidavit, pp. 2*.[3]

55. Omitting such material facts demonstrates Det. Sandoval's knowing or reckless disregard for the true nature of the dragnet search that occurred in this case. At a minimum, Det. Sandoval should have been aware of the unprecedented nature of this search based on his repeated discussions with Google's counsel. But to the extent Det. 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.

56. In addition to Det. Sandoval's lack of veracity, the good-faith doctrine should not apply because the affidavit lacked a substantial basis to find probable cause, and no officer could reasonably presume such a warrant was valid.

57. The affidavit was completely devoid of any particularized probable cause, as discussed *supra*. *See also Motion to Suppress, pp. 26-27*. Det. 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." *TR 8/19/22, pp. 83 (Attachment 1)*. No reasonable officer could rely on such a warrant.

58. Similarly, the warrant was so obviously lacking in particularity that no reasonable officer could presume it was valid. *See Motion to Suppress, pp. 27-28*. It failed to identify a single account, instead describing the place to be searched as simply "1600 Amphitheater Parkway," the street address for the digital equivalent of a billion-story apartment building. It failed to limit or adequately describe what the government could seize,

[3] Google, for its part, states that it no longer provides full IP addresses in response to keyword warrants, although it is not clear how recently this change occurred. *See Adeli Decl., pp. 3, para 7* ("Google's policies and practices regarding the scope of information included in this initial production may have differed in the past, including during the time period in this matter.").

resulting in a warrant return where the overwhelming majority of the data produced was inconsistent with its terms.

59. There is a lot that that is new about this case, but it is not new that warrants must be supported by probable cause. And it is not new that warrants must be particularized. Rather, it was or should have been clear to Det. Sandoval that the warrant here was so profoundly overbroad and lacking particularity that it was nothing short of a general warrant. And there is no such thing as relying on a general warrant in good faith. 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). 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).

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

II. Accounts, Cellphone Records, Cellphone Data, Home, and Social Media Search Warrants

61. "The Fourth amendment to the United States Constitution and article II, section 7 of the Colorado Constitution prohibit the issuance of a search warrant without probable cause supported by oath or affirmation particularly describing the place to be searched or the things to be seized." *People v. Hebert*, 46 P.3d 473, 482 (Colo. 2002). "This constitutional bulwark 'safeguard[s] the privacy and security of individuals against arbitrary invasions by government officials.'" *People v. Coke*, 461 P.3d 508, 516 (Colo. 2020).

62. Although a search conducted pursuant to a warrant is typically reasonable, "so-called 'general warrants,' which permit 'a general, exploratory rummaging in a person's belongings,' are prohibited," thereby necessitating the probable cause and particularity requirements. *Id*., citing *Andreson v. Maryland*, 427 U.S. 463, 480 (1976).

63. "Probable cause exists when an affidavit for a search warrant alleges sufficient facts to warrant a person of reasonable caution to believe that contraband or evidence of criminal activity is located at the place to be searched." *Id*., citing *People v. Quintana*, 785 P.2d 934, 937 (Colo. 1990).

64. "The affidavit must supply a 'sufficient nexus between criminal activity, the things to be seized, and the place to be searched.'" *Id*., citing *People v. Kazmierski*, 25 P.3d 1207, 1211 (Colo. 2001). "An affidavit containing only vague allegations that the defendant engaged in illegal activity without establishing a nexus between the alleged criminal activity and place to be searched cannot establish probable cause." *Kazmierski*, 25 P.3d at 1211, citing *People v. Randolph*, 4 P.3d 477, 482 (Colo. 2000).

65. When searching a home, for example, "[t]he connection between the residence and the evidence of criminal activity must be specific and concrete, not 'vague' or 'generalized.'" *United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016). "The critical element in a reasonable search is not that the owner of property is suspected of crime, but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *United States v. Frazier*, 423 F.3d 526, 532 (6th Cir. 2005) (citation omitted).

66. "While an officer's 'training and experience' may be considered in determining probable cause, such training and experience cannot substitute for an evidentiary nexus, prior to the search, between the place to be searched and any criminal activity." *People v. Eirish*, 165 P.3d 848, 852 (Colo. App. 2007).

67. The particularity requirement is violated where the areas to be searched are unreasonably broad. "The purpose of this particularity requirement is to prevent the use of general warrants authorizing wide-ranging rummaging searches in violation of the Constitution's prohibition against unreasonable searches and seizures." *Id*. (citation omitted).

A. Accounts [DEF-25]

68. Counsel addressed several warrants in the Motion to Suppress Evidence Unlawfully Obtained (Accounts) [DEF-25]: the warrants requesting information regarding Mr. Seymour's Google and Apple accounts; the warrant requesting information regarding the Comcast IP address belonging to Mr. Seymour's mother; and the warrant requesting information regarding T-Mobile IMSIs. The Motion also addressed the warrants for information pertaining to anonymized Google accounts. One of those warrants requested information pertaining to 3 devices, which law enforcement obtained as a result of the first geofence warrant. The second warrant requested information pertaining to 14 devices, which law enforcement obtained as a result of the second geofence warrant (after narrowing the number of devices down from 2,103). Lastly, the Motion addressed the warrant directed at Google for information pertaining to five anonymized targets, which law enforcement obtained as a result of the keyword search warrant.

69. The People argue that the motion to suppress the evidence obtained from the warrants referenced above should be denied for two reasons. First, the People argue that Mr. Seymour lacks standing to challenge the constitutionality of the search warrants for data contained in accounts belonging to others. *People's Response to Motion to Suppress Evidence Unlawfully Obtained (Accounts) [Def-25], pp. 3*. Second, the People argue that the warrants for records related to Mr. Seymour's Google and Apple accounts were constitutionally sufficient because (1) there was particularity in the location to be searched; (2) there was particularity in the data to be searched and seized; and (3) there was probable cause to believe that evidence related to the incident would be located in the data requested. *Id., pp. 4*.

(a) Standing

70. First, Mr. Seymour is not challenging the constitutionality of the search warrants for Google and Apple data belonging to his co-defendants, Mr. Bui and D.S. He is challenging the constitutionality of the search warrants as they pertain to him. The same goes for the Comcast account belonging to his mother, because the IP address is used by the entire household.

71. Furthermore, Mr. Seymour was swept up in the anonymized account information that law enforcement issued a warrant for after receiving the results from the keyword search warrant. One of those five accounts belonged to Mr. Seymour, and law enforcement obtained all of the information from Mr. Seymour's account that was requested in that warrant, which encompassed the entire account.

(b) Probable Cause

72. The People argue that the warrants meet the probable cause requirement. The People first argue that there was probable cause to believe "that the three defendants in this case were the three masked persons who were in the backyard of the victims' residence minutes before it went up in flames." *Id., pp. 8*.

73. In support of this assertion, the People argue that the "records obtained from Google," i.e., the keyword search warrant, narrowed down the number of devices that searched for the address of the arson. *Id.* The People state that this led to the identification of Mr. Seymour, Mr. Bui, and D.S., who were "linked together by where they live, what schools they attended, their known associates and their social media postings." *Id., pp. 9*.

74. The People also argued that there were "reasonable grounds" to believe that the accounts listed would contain evidence relevant to the arson. *Id.* The People argue that "because the video footage showed that three individuals were involved in the homicide, there was a substantial likelihood that communications between any of these individuals would include details relevant to this offense." *Id*.

75. The People further argue that location data would "also be highly relevant," because it could establish presence at locations relevant to the offense. *Id*. The People state that "[o]ther substantive content was relevant as well, such as photos and videos," because they could establish connection between the involved parties, and because a video of the arson could be found in Mr. Seymour's accounts. *Id*. The People also reference the importance of metadata being recovered. *Id*.

76. Lastly, the People argue that usage of social media or cloud accounts are important to establish "establish attribution for the substantive content deemed relevant to the offense," to essentially prove ownership of the account, which necessitates "looking at longer periods of data than the time just before and after an offense." *Id., pp. 10*.

77. Despite the People's contentions, these warrants lack a sufficient nexus between the alleged criminal activity, the things to be seized, and the places to be searched.

78. All of these warrants stemmed from the earlier keyword search warrant directed at Google. When law enforcement drafted the subsequent warrants, they only had information that at some point, the address of the arson was entered into a Google search bar, and they had identifying information for which Google accounts were connected to those searches.

79. Despite this, there is a lack of nexus tying that search to Mr. Seymour's data in all of these different accounts, particularly his iCloud account through Apple. After law enforcement identified Mr. Seymour as a suspect, they thought of every account he could feasibly have, and listed every single piece of information they could possibly find in those accounts, without articulating why evidence of the arson would be present in, for example, "iWorks (including Pages, Numbers, and Keynote), or "iCloud Keychain."

80. The warrants also authorized law enforcement to search the content of <u>*all*</u> of Mr. Seymour's emails, along with the data attached to those emails, regardless of who Mr. Seymour was contacting. Similarly, there is no nexus between the alleged offense and the content of Mr. Seymour's emails, regardless of who they were to or what they contained.

(c) Particularity

81. The People argue that there was particularity in the location to be searched, because the warrants "identify the entities in control of the records being requested." *Id., pp. 4*. The People also argue that there was particularity in the data to be searched and seized. *Id*.

82. Regarding particularity in the data to be searched, the People cite *United States v. Pinto-Thomaz*, 352 F.Supp. 3d 287 (S.D.N.Y. 2018), for the proposition that a warrant does not lack particularity simply because it is broad. *People's Response, pp. 5*. The People failed to include, however, that the defendant in *Pinto-Thomaz* was accused of insider trading. *Pinto-Thomaz*, 352 F.Supp. 3d 287. The court in that case specifically noted that "[t]he level of specificity required depends on the nature of the crime," and cited *United States v. Levy*, 803 F.3d 120 (2nd Cir. 2015), which held that a broad warrant was justified by the complexity of the alleged fraud. *Id*. at 305. The court also cited *United States v. Dupree*, 781 F.2d 115, 149 (E.D.N.Y. 2011), which stated that "[t]he nature of the crime…may require a broad search" including where "complex financial crimes are alleged." *Id*.

83. The People also cite *People v. Roccaforte*, 919 P.3d 799 (Colo. 1996) for the similar proposition that the quantity of items listed in a warrant does not necessarily have a bearing on the validity of the search itself. *People's Response, pp. 5.* The defendant in *Roccaforte* was accused of financial crimes in 1996, before cellphones were widely available and used. *Roccaforte*, 919 P.3d 799. In *Roccaforte*, law enforcement obtained one warrant for the search of the defendant's home, and one warrant for the search of a storage space rented by the defendant's company. *Id*. at 801. The issued warrants authorized searches for books, records, and any other business-related documents in the name of the defendant's business and in the name of the defendant, the co-defendant, and the defendant's wife, who was a co-owner, for a thirty-day period. *Id*.

84. The *Roccaforte* court agreed with the lower court and the defendant's assertion that the warrants at issue were "essentially 'all records' warrants." *Id*. at 803. However, the court stated that the fact that the warrants were "all records" warrants was "not dispositive of the question of whether they were sufficiently particularized to be valid." *Id*. The court stated that "[a]n 'all records' warrant is appropriate where there is probable cause to believe that the crime alleged encompasses the entire business operation and that evidence will be found in most or all business accounts…In this case, the alleged crime is tax fraud," which the court found encompassed the entire business. *Id*. (citation omitted) (emphasis added).

85. The People then cite *United States v. Gatto*, 313 F.Supp. 3d 551 (S.D.N.Y. 2018) for the proposition that a warrant to search for a wide range of potentially relevant material does not necessarily violate the particularity requirement. *People Response, pp. 5*. *Gatto*, like *Pinto-Thomaz* and *Roccaforte*, is a case involving wire fraud and money laundering, specifically an allegation that the defendant was bribing high school basketball players to sign with certain universities. *Gatto*, 313 F.Supp. 3d at 554. The warrant at issue in *Gatto* was to search the defendant's cellphone using a Cellebrite download. *Id*. Importantly, the warrant authorized law enforcement to search for "evidence of schemes" to "pay NCAA coaches in exchange for those coaches using their influence with NCAA players to convince those players and/or their families to retain certain agents, financial advisors, or others," and "pay high school and NCAA players and conceal those payments from universities." *Id*. at 555-56. The warrant also authorized law enforcement to search for "evidence of 'schemes to make payments from the universities attended or intended to be attended by the players." *Id*. at 556. Crucially, the warrant "specified the categories of evidence responsive to the warrant," and "tracked the language in the applications with respect to the procedures from finding such evidence," and detailed "various targeted search techniques." *Id*.

86. The cases cited by the People are outdated, unrelated to the type of offense at issue here, and unrelated to the type of digital media at issue here.

87. Overall, regarding particularity, the People contend that the "warrant described the data to be seized with sufficient detail to allow the executing officer/personnel to know what data is encompassed within the warrant's authorization (i.e., which data they are authorized to release to the requestor)." *People's Response, pp. 6*. The People argue that the warrants here are described in "substantial detail," because it provided a list of the "***types*** of data being requested" and provided a time frame. *Id*. The People argue that "while the categories listed do encompass a large portion of the data available in the accounts or records, this alone does not violate the particularity requirement." *Id*.

88. Lastly, the People argue that the warrants were sufficiently particularized because they specify that the requested data would be searched for information that related to the incident, without detailing how this would be done. *Id*.

89. These warrants do not merely encompass a "large portion" of the data available in the accounts or records. The warrants encompass everything contained within the accounts. Separating types of data into different categories does nothing if the sum of the requested data is the entirety of the account. At that point, the warrant may as well not list any categories at all.

90. During the Motions Hearing, in response to this motion, and to all of the other motions discussed below, the People stated:

> "Counsel then says, Well, they're too broad or they encompass too much. Each one of these search warrants said, Yes, we're going to ask for this data, abut we're going to tell you, whoever provides it to us and we're telling the Court that we're going to bring it back to Denver police headquarters, and we're only going to look for any evidence that's related to the arson homicide investigation of August 5th."
>
> *TR 8/19/22, pp 144:24-25, 145:1-6 (Attachment 1)*.

91. This is a gross mischaracterization of what law enforcement is permitted to do. The People admit that this amount of data is massive, and the way they obtained it all was through a general rummaging of Mr. Seymour's entire digital world. Although courts have held that searches of a wide breadth are permissible, the techniques employed to decide what to *seize* must be specific and targeted. *See Gatto*, 313 F.Supp. 3d at 556.

92. Law enforcement is not permitted to go through all of a person's belongings and then decide what is relevant to their case after the fact. The warrants need to be sufficiently particular at their inception, to prevent casting the kind of wide net that law enforcement did here.

B. Cellphone Records [DEF-26]

93. In the Motion to Suppress Evidence Unlawfully Obtained (Cellphone Records) [DEF-26], counsel addressed the January 6, 2021, search warrant directed at AT&T, which requested records pertaining to Mr. Seymour's cellphone number, for a sixty-nine-day period.

(a) Probable Cause

94. The People recite the same argument here as they did in their response to the motion regarding Mr. Seymour's accounts. The People argue that there was probable cause to search Mr. Seymour's phone records and cite the same inapplicable authority. *People's Response to Motion to Suppress Evidence Unlawfully Obtained (Cellphone Records) [Def-26], pp. 8*.

95. The People, again, argue that there was probable cause to believe that the "three defendants in this case" were the three people seen on surveillance video on the date of the arson. *Id*.

96. The People argue that Mr. Seymour's phone records would establish his location on the date of the arson, and they would establish who he communicated with in order to determine who "may have assisted him or who may have knowledge of his actions and/or his state of mind at the time the offense was committed," and would also be able to "establish his familiarity" with the location of the arson, "as well as the nature of his relationships between others involved in this case." *Id*.

97. The People also argue that "[p]atterns of usage of a cellphone account," can be "used to establish attribution of a person to the account itself." *Id*.

98. Lastly, the People argue that the time period "had the reasonable potential" to contain relevant evidence "as well as important attribution data." *Id., pp. 9*.

99. The People fail to articulate what nexus exists between the alleged offense and Mr. Seymour's cellphone records. Law enforcement had information from a keyword warrant that a particular address was searched. There is no information about how this information ties into Mr. Seymour's cellphone, particularly because there is no evidence that a cellphone was used during the offense, or at any stage or step of the offense.

100. The fact that people carry cellphones, and that data on a cellphone can show who uses that cellphone, is not sufficient probable cause to believe that evidence of the alleged offense would be present in Mr. Seymour's cellphone records from AT&T.

(b) Particularity

101. As with the Response to the motion regarding Mr. Seymour's accounts, the People again argue that the warrant describes the types of data being sought within a specified time period, and that this made the warrant sufficiently particularized, in spite of the fact that the data requested encompassed the entire account. *Id., pp. 5*.

102. In support of this proposition, the People cite several cases, some of which are inapplicable entirely, and others which are more relevant to cellphone data as opposed to cellphone records and are discussed below.

C. Cellphone Data [DEF-27]

103. In this Motion to Suppress, counsel addressed the February 2, 2021, warrant authorizing a forensic "cellphone dump" of Mr. Seymour's cellphone. The warrant authorized the search of Mr. Seymour's <u>all</u> of cellphone data and did not contain a specified time frame.

(a) Probable Cause

104. The People's argue that the "historical facts" establish probable cause that Mr. Seymour was involved in the offense, and the affidavit "set forth numerous direct facts as well as reasonable inferences upon which the court was entitled to rely…" *People's Response to Motion to Suppress Evidence Unlawfully Obtained (Cellphone Data) [Def-27], pp. 12*. The People contend that one piece of "direct evidence" are "text messages" between Mr. Seymour and Mr. Bui, even though this warrant would be the one to garner texts sent or received by Mr. Seymour. *Id*.

105. The People's only other argument regarding probable cause is that "[o]ther portions of the nexus are based on reasonable inferences from the facts set forth in the warrant as well as common sense understandings about how individuals use their phones." *Id*.

106. Again, the fact that cellphones are nearly ubiquitous is not a sufficient nexus to show probable cause to search a specific person's cellphone for evidence of a crime, particularly when law enforcement seeks a complete "dump" of all information contained within the phone, with no temporal limitation.

(b) Particularity

107. The People's response is, again, largely the same as the responses filed regarding the motions to suppress Mr. Seymour's account information and his cellphone records.

108. Here, despite noting that cellphones store a massive amount of personal, private data, the People repeat, verbatim, the same argument that the breadth of a warrant does not necessarily mean that it is not sufficiently particular, again citing the same authority. *Id., pp. 5*.

109. The People state that "[e]ven where a warrant authorizes the search of an entire phone, this is appropriate so long as it is supported by probable cause." *Id., pp. 6*. To support this proposition, the People cite *United States v. Rankin*¸442 F.Supp. 2d 225 (E.D. Pa. 2006), *People v. Goynes*, 927 N.W. 2d 346, and *United States v. Gatto*, 313 F.Supp. 551 (S.D.N.Y. 2018). *Id*. *Gatto*'s inapplicability is already discussed above. In *Rankin*, law enforcement searched a home for a long list of items for evidence of tax crimes and is also inapplicable here.

110. In *Goynes*, the court stated that to satisfy the particularity requirement, a warrant must "be sufficiently definite to enable the searching officer to identify the property to be seized" and that "the broader the scope of a warrant, the stronger the evidentiary showing must be to establish probable cause." 313 F.Supp. at 355. The court also stated that "a warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search." *Id*.

111. In *Goynes*, to establish the defendant's involvement, the affidavit for the search warrant for the defendant's cellphone stated that a witness heard shots fired and gave officers the description of a man she saw holding a handgun, walking towards a white, four-door sedan. *Id*. at 349-50. The officers located surveillance video showing the same sedan. *Id*. at 350. The officers then conducted interviews with two witnesses who told officers that they observed the shooting, knew the identity of the suspect, and named the defendant. *Id*. One of these witnesses was the defendant's cousin. *Id*. She positively identified all of the involved parties in photographic lineups and stated that she was "'100% sure' Goynes was the shooter." *Id*. at 351.

112. The court compared the affidavit for Goynes' cellphone to the affidavit in *State v. Henderson*, 854 N.W.2d 616. *Id*. at 354. In that case, the affidavits "established that there was a fair probability that the defendant…was involved in the shootings and that he had a cell phone in his possession when he was taken into custody *shortly after the shootings*." *Id*. (emphasis added).

113. The court noted that "[a]lthough the content of the affidavits pertaining to how suspects use cell phones standing alone may not always be sufficient probable cause, when considered with all the facts recited above…the affidavit provided a substantial basis to find probable cause existed to search the cell phone data." *Id*. at 355.

114. The facts in *Goynes* differ from the facts here. In that case, law enforcement had multiple witnesses to the crime, one of whom identified the defendant as the shooter. The court cited another case where the defendant was arrested with his phone shortly after a shooting, and that made it reasonably more likely that he was carrying that cellphone during the shooting itself.

115. Here, on the other hand, all law enforcement had was results from a keyword search warrant showing that the address of the arson was entered into a Google search bar, as opposed to the type of background facts present in *Goynes*. Furthermore, although Mr. Seymour was carrying his cellphone at the time of his arrest, he was arrested long after the arson occurred.

116. The People here admit that "the categories listed do encompass the entirety of the cellphone." *People's Response, pp. 7*. However, the People allege that "[t]he particularity requirement was met here because the warrant lists with specificity the categories within the device that are subject to search and seizure." *Id*.

117. This dichotomy is precisely the issue. The People cannot claim particularity due to the categories being specified when those categories are the sum of the entire device.

118. Lastly, the People contend that "any relevant/incriminating" data would need to be "attributed to its source." *Id., pp. 12*. The People argue that this is "not simply a search for 'evidence of ownership,' which was deemed improper under *Herrera*. *Id*.

119. In *People v. Herrera*, 357 P.3d 1227, 1228 (Colo. 2015), a warrant authorized a search of the defendant's cellphone for text messages between the defendant and an underaged girl, as well as for "indicia of ownership." There, "[t]he People contend[ed] that the warrant thus permitted a search of text messages" contained in a particular folder on the phone "because any message found there would reveal Herrera as the owner of the phone." *Id*. at 1230. The court stated that "the People argue that any piece of data on the phone, including any text message on the phone, would have the possibility of revealing Herrera's ownership of the phone," and that "rationale transforms the warrant into a general warrant that fails to comply with the Fourth Amendment's particularity requirement." *Id*. This was also unnecessary because "the phone was seized from Herrera during his arrest, and he never disputed ownership of the phone." *Id*. at 1231.

120. As was the case in *Herrera*, Mr. Seymour's cellphone was taken from him when he was arrested, and he has never disputed ownership of the phone. Despite this, the warrant authorized the search of all "[d]ata which tends to show possession, dominion and control over said equipment," transforming the warrant into a general warrant in violation of Fourth Amendment.

D. Home [DEF-29]

121. In this Motion to Suppress, counsel addressed the January 26, 2021, warrant authorizing a search of Mr. Seymour's home. In the affidavit, Detective Sandoval stated that law enforcement should be able to search the home because Mr. Seymour carries a cellphone, and analysis of the cellphone could show where the cellphone was at a particular time. The warrant also authorized law enforcement to look for accelerants, several items of clothing, firearms evidence, surveillance equipment, any electronic devices capable of storing location information, any material evidence tending to establish the motive or identity of any suspect or witness, and any articles of personal property tending to establish the identity of the person in control or possession of the place.

122. The People contend that there was a sufficient nexus between the place to be searched and the item to be seized because "probable cause" existed that Mr. Seymour was involved in the offense, and that items worn on the night of the arson or electronic devices used to search for the address could be located inside. *People's Response to Motion to Suppress Evidence Unlawfully Obtained (Home) [Def-29]*.

123. The People also argue that due to the fact that Mr. Bui was engaged in narcotics distribution and possessed weapons, and the fact that Mr. Bui and Mr. Seymour were close, Mr. Seymour "may as well be someone who would possess a firearm." *Id., pp. 6-7*.

124. This warrant is precisely the type of general search warrant prohibited by cases such as *Eirish*, 165 P.3d at 854. The warrant described two specific items of clothing, and then listed general categories, including *any* material evidence developed by a thorough crime scene investigation, *all* articles of personal property that would establish identification, and *all* electronic devices. As to "material evidence" and "articles of

personal property," the number of possible items that could be swept up in that net is endless, giving no direction to law enforcement about which items to seize.

125. The warrant affidavit also contained no information that Mr. Seymour was involved in dealing narcotics or in possessing firearms, and the People's post hoc assertions that Mr. Seymour may carry a firearm because he is friends with Mr. Bui are insufficient to establish probable cause.

126. Lastly, the People argue that for the firearms evidence and surveillance evidence, the court may sever deficient portions of the warrant. The motion does not become "moot and irrelevant," as the People contend, just because no firearms or surveillance evidence were located. Although the court may sever deficient *portions* of a search warrant without invalidating the entire warrant, that principle does not apply if the entire warrant itself is violative of the Fourth Amendment.

127. Law enforcement cannot be unable to name what items they are seeking in a defendant's house but still execute a warrant because there could be something in the house linking the defendant to a crime. That is what occurred here, and that is insufficient under the Fourth Amendment standard.

E. Social Media [DEF-30]

128. Lastly, in this Motion to Suppress, counsel addressed the December 31, 2020, warrant directed at Mr. Seymour's Instagram for a 183-day period, the January 4, 2021, warrant directed at Mr. Seymour's Facebook account, for a 188-day period, and the January 12, 2021, warrant directed at Mr. Seymour's Snapchat account for a 196-day period.

(a) Standing

129. The People first contend that Mr. Seymour does not have standing to challenge the constitutionality of search warrants for data contained in accounts belonging to others. *People's Response to Motion to Suppress Evidence Unlawfully Obtained (Social Media) [Def-30], pp. 3-4*. Mr. Seymour is not challenging the constitutionality of the search warrants as they pertain to data belonging to Mr. Bui and D.S. Mr. Seymour's accounts were targeted in those warrants, and as such he is challenging the warrants' constitutionality as they pertain to his accounts.

(b) Probable Cause

130. The People again argue that there was probable cause to believe that the three defendants in this case were the three people seen on surveillance video on the day of the arson. *Id., pp. 8*. The People also argue that there were "reasonable grounds" to believe that these accounts would contain evidence relevant to the offense in the form of communication between the individuals, location data, photos and videos such as news videos captured after the incident, and metadata. *Id., pp. 9*.

131. The People also argue that patterns of usage of the accounts can establish attribution for substantive content. *Id., pp. 9-10*.

(c) Particularity

132. To no surprise, the People's response to this motion is nearly identical to the other People's other filed responses, and the People do not provide any case law regarding the application of the particularity requirement to social media accounts in support of their argument.

133. The People rely on the same broad argument that the warrants described the data sought from all of the accounts within a specified time period, again stating that the particularity requirement was met because the warrant lists the categories of data within the accounts that are subject to seizure.

134. As with all of the other warrants in this case, the social media warrants request every piece of information contained in the accounts for very lengthy time periods. Law enforcement again went through massive amounts of data to look for what they think could later be relevant to their case. There is no nexus between the results of the keyword search warrant, which at the time was the only evidence naming Mr. Seymour as a suspect, and his social media accounts, particularly when the warrants authorized a search of the entire accounts.

F. Good Faith Exception

135. In each response, the People allege that the good faith rule must rescue each deficient warrant, because it was not entirely unreasonable for the affiants to rely on the warrants issued in this case

136. "When evidence is obtained in violation of the Fourth Amendment, the judicially developed exclusionary rule usually precludes its use in a criminal proceeding against the victim of the illegal search and seizure." *Illinois v. Krull*, 480 U.S. 340 (1987). However, if the evidence was "obtained in objectively reasonable reliance" on the "subsequently invalidated search warrant," it should not be suppressed. *United States v. Leon*, 468 U.S. 897, 922 (1984). In short, "the exclusionary rule should not automatically apply every time a Fourth Amendment violation is found; rather, it should apply only in those circumstances where its remedial objectives are actually served by suppression." *People v. Gutierrez*, 222 P.3d 925, 941 (Colo. 2009).

137. "For this exception to apply, the affidavit must contain 'a minimally sufficient nexus between the illegal activity and the place to be searched.'" *Brown*, 828 F.3d at 385.

138. "[A]n officer's reliance on a warrant is not always objectively reasonable." *Id*. There are "four situations in which an officer's reliance on a warrant would not be objectively reasonable and suppression would therefore continue to be an appropriate

remedy: (1) where a warrant is based on knowingly or recklessly made falsehoods; (2) where the issuing magistrate wholly abandons his judicial role; (3) where the warrant is so lacking in specificity that the officers could not determine the place to be searched or the things to be seized; or (4) where the warrant is so lacking in indicia of probable cause that official belief in its existence is unreasonable – in other words, a warrant issued on the basis of a 'bare-bones' affidavit." *Id*., citing *Leon*, 468 U.S. 897 (1984).

139. "An affidavit is considered 'bare-bones' and therefore an officer cannot reasonably rely on it, where the affidavit fails to establish a 'minimally sufficient nexus between the illegal activity and the place to be searched.'" *Id*., citing *United States v. Carpenter*, 360 F.3d 591, 596 (6th Cir. 2004). "An affidavit that provides the details of an investigation, yet fails to establish a minimal nexus between the criminal activity described and the places to be searched, is nevertheless bare-bones." *Id*.

140. "Blanket suppression is an extraordinary remedy that should be used only when the violations of search warrant requirements are so extreme that the search is essentially transformed into an impermissible general search." *Eirish*, 165 P.3d 848, citing *United States v. Uzenski*, 434 F.3d 690 (4th Cir. 2006).

141. As to Mr. Seymour's home, the warrant was so lacking in specificity regarding, for example, what evidence of "motive" law enforcement was entitled to seize.

142. Furthermore, the affidavits for the other warrants are "bare-bones" affidavits. Each affidavit made sure to recount every detail of the investigation, without establishing <u>any</u> nexus, much less a minimal nexus, between the arson and the places, or the massive amounts of personal data, to be searched.

143. These warrants and "bare-bones" affidavits were so lacking in indicia of probable cause that official belief in their existence was unreasonable. It is clear, just from looking at the warrants and affidavits, that they were asking for every single piece of information from every account that Mr. Seymour could have feasibly had, without the necessary probable cause and particularity.

144. Although blanket suppression is an extraordinary remedy, these violations of search warrant requirements are so extreme that the searches were transformed into impermissible general searches. These searches cast the widest net possible, and enabled law enforcement to comb through all of Mr. Seymour's accounts, so that law enforcement could later pick out what could be relevant to their case.

145. These searches were so violative of the Fourth Amendment that suppression of the evidence gathered as a result of the warrants is the only just result. The good faith exception cannot save these warrants that were so lacking in indicia of probable cause and particularity.

146. Mr. Seymour therefore requests this Court order to suppress all evidence obtained from these search warrants as well as fruits thereof.

III. Motion to Suppress Statements and Observations [Def-37]

147. Mr. Seymour moves this Court to suppress all statements made during the police interrogation of Gavin Seymour on January 27, 2021, prior to advising Mr. Seymour of his *Miranda* rights, including the statement of his mother regarding his cell phone carrier.

A. Admitting the Statement of Gavin Seymour's Mother Made During the Custodial Interrogation of Her 16-Year-Old-Son Would Subvert the Purpose of the Additional Protections of Colorado Children's Code Provision C.R.S. 19-2.5-203(1)

148. In addition to the constitutional protections afforded to every accused person, the Colorado Children's Code provides the additional protection to children under the age of 18 that no statement or admission of juvenile during custodial interrogation by law enforcement is admissible unless (1) a parent, guardian or legal custodian is present, and (2) the juvenile and the parent or guardian are advised of the child's *Miranda* rights. C.R.S. 19-2-511(now located at C.R.S. 19-2.5-203(1)); *People v. Knapp*, 505 P.2d 7 (Colo. 1973)(provision rooted in the 5th and 6th amendments of the U.S. Constitution); *People v. Blankenship*, 119 P.3d 552 (Colo. App. 2005)(19-2-511 doesn't diminish the 5th and 6th amendments, but provides additional protection to children). The legislative purpose of this provision is to safeguard the privilege against self-incrimination and is designed to provide a child parental guidance during police interrogation, thereby providing at least some assurance that the child's waiver of rights is knowing and voluntary. *People v. Raibon*, 843 P.2d 46 (Colo. App. 1992).

149. C.R.S. 19–2.5–203(1)'s requirement of the presence of a parent or guardian during the child's *Miranda* advisement and interrogation serves 2 purposes. First, this requirement codifies *Gault* by extending *Miranda* to juveniles. *People in the Interest of A.L.-C.*, 382 P.3d 842, 845 (Colo. 2016), *citing People v. Legler,* 969 P.2d 691, 694 (Colo. 1998). Second, the requirement provides "an additional and necessary assurance that the juvenile's Fifth Amendment right against self incrimination…will be fully afforded to him." *Id., quoting People v. Saiz*, 620 P.2d 15, 19-20 (Colo. 1980).

150. In this case, 16-year-old Gavin Seymour's parents were only present at his in-custody interview for the purpose of fulfilling the requirement that a parent be present for the *Miranda* advisement and interrogation. The objective of the attempted interview was to speak with Gavin Seymour about his involvement in the case, and the presence of Gavin's mother, was solely to extend *Miranda* to Gavin and to fully afford him his constitutional rights. To distort that purpose by using Gavin's mother's statement identifying his cell phone carrier would subvert the very legislative intention of having her present at the interview in the first place.

B. Gavin Seymour's Statement was Not Voluntary

151. A defendant's statements must also be suppressed if they are involuntarily given. To be admissible, a defendant's statements must be voluntarily given without the

influence of coercive police activity. *Colorado v. Connelly*, 479 U.S. 157 (1986); *People v. Mendoza-Rodriguez*, 790 P.2d 810, 816 (Colo. 1990); *People v. Breidenbach*, 875 P.2d 879 (Colo. 1994). To be voluntary, "[s]tatements must not be the result of official coercion, intimidation, or deception. Official coercion includes any sort of threats, or any direct or implied promises or improper influences, however slight." *People v. Blankenship*, 30 P.3d 698, 703 (Colo. App. 2000), *citing Colorado v. Connelly*, 479 U.S. 157 (1986); *People v. May*, 859 P.2d 879 (Colo.1993); *People v. Mendoza–Rodriguez*, 790 P.2d 810 (Colo.1990). A defendant's mental condition is a factor to be considered in determining whether he may be susceptible to coercion. *People v. Parks*, 579 P.2d 76 (Colo. 1978).

152. The prosecution has the burden of establishing the voluntariness of the statement by a preponderance of the evidence. *People v. Mounts*, 784 P.2d 792 (Colo. 1990) Voluntariness of a statement is determined on the basis of the totality of the circumstances under which it is given, including events and occurrences surrounding the statement and the mental condition of the maker. *Id.*

153. In this case, sixteen-year-old Gavin Seymour, who had never before been arrested or accused of a crime, was awakened and arrested from his home very early in the morning. Following the arrest, police took Mr. Seymour to a small interrogation room where he was confronted by two police officers who began asking him questions before advising him of his *Miranda* rights despite their awareness of their obligation to *Mirandize* the teen. Gavin Seymour's young age, inexperience with police, arrest from his home, and detention in a small room in the presence of two law enforcement officers who chose to begin interrogating him before informing him of his rights combined to make his statements involuntary. Therefore, Gavin's statements should be suppressed as involuntary.

C. Custodial interrogation about Gavin Seymour's phone number must be suppressed because police did not advise him of his Miranda rights prior to the statement.

154. It is undisputed that police formally arrested Gavin Seymour at his home and subsequently subjected him to express questioning, an interrogation, while in-custody at the Denver Police Department.

155. Before advising Mr. Seymour of his Miranda rights, Detective Sandoval asked Gavin Seymour to confirm his phone number, which Gavin did in direct response to the question. Right *after* obtaining this statement, Detective Sandoval then advised Gavin Seymour of his *Miranda* rights.

156. Importantly, Gavin Seymour immediately and unambiguously exercised his right to remain silent after being advised of those rights. In response to Detective Sandoval's question "with these rights in mind, are you willing to answer any questions at this time?" Gavin replied, "No, sir." This evidences not only that Gavin Seymour did not wish to talk

about the specific incident, but that he did not want to answer *any* questions, which would include questions about his phone number.

157. Police in this very interview asserted their belief of the importance of cell phone records to the evidence in the case inasmuch as they described to Gavin their belief that his cell phone records were one of the primary reasons that they believed he was involved in the crimes that were the subject of the interview. Far from being a mere confirmation of basic identification, questioning Gavin Seymour about his cell phone number without a *Miranda* advisement was a substantive violation of his constitutional and statutory rights to remain silent and to have a lawyer present.

158. Therefore, Gavin Seymour's statement regarding his phone number must be suppressed.

WHEREFORE, Mr. Seymour moves this Court to suppress all evidence derived from the keyword search warrant, all evidence derived from the search warrants for his accounts, cellphone records, cellphone data, home, and social media, and all evidence derived from his unlawful interrogation.

Respectfully submitted,

Dated this day: September 16, 2022

/s/ Jenifer Stinson

_____

Attorney: Jenifer Stinson, #35993

_____

Attorney: Michael S. Juba, #39542

_____

Attorney: Michael W. Price, #22PHV6967

I hereby certify that on this 16th day of September, 2022, a true and correct copy of this motion was served upon all counsel of record.

Signature