DISTRICT COURT, DENVER COUNTY, COLORADO 520 W. Colfax Denver, Colorado 80204	DATE FILED: September 30, 2022 5:39 PM FILING ID: 65625C7980CAF 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 RESPONSE TO PEOPLE'S WRITTEN ARGUMENTS ON DEFENDANT'S MOTIONS TO SUPPRESS

On September 22, 2022, the government filed Written Arguments on Defendant's Motions to Suppress, following additional briefing by Mr. Seymour, *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], [Def-37]*, and a hearing on August 19, 2022, with witnesses from Google and the Denver Police Department. *See* Tr. 8/19/22 ("Tr."). Mr. Seymour, through counsel, now submits this reply brief in support of his motion to suppress evidence from a reverse "keyword warrant," as well as his motions to

suppress evidence unlawfully obtained regarding his accounts, his cellphone records, his cellphone data, his home, and his social media. *See Motion to Suppress Evidence From a Keyword Warrant & Request for a Veracity Hearing*, *Motion To Suppress Evidence Unlawfully Obtained (Accounts) [Def-25]*, *Motion to Suppress Evidence Unlawfully Obtained (Cellphone Records) [Def-26]*, *Motion to Suppress Evidence Unlawfully Obtained [Cellphone Data] [Def-27], Motion to Suppress Evidence Unlawfully Obtained (Home) [Def-29],* and *Motion to Suppress Evidence Unlawfully Obtained (Social Media) [Def-30]*. Mr. Seymour states as follows:

I. The Keyword Warrant

A. Fourth Amendment Interests

1. The government felt the need to obtain a warrant for the search history data in this case—in fact, they sought three of them. They also conceded, at least initially, that a "search" occurred. *See People's Written Arguments on Defendant's Motions to Suppress* at 3 ("[t]he People are not suggesting that this was not a search at all."). Yet they now argue that no warrant was required because Mr. Seymour did not have an expectation of privacy in his search terms. *See Id.* at 2.

2. The government asserts that the keyword warrant was somehow not a search because it involved a "computer [that] provided a list of accounts" from a "database." *See Id.* at 3. The government is wrong. There is no "computer inquiry"-exception to the Fourth Amendment. *Id.* at 5. And that is especially true when the database in question is full of the search history belonging to billions of Google users, including Mr. Seymour.

3. In the digital world, all that exists are "ones and zeroes." *See Id.* at 3. But that does not deprive those digital bits of their Fourth Amendment protections. *See Riley v. California*, 573 U.S. 373, 395–96 (2014), *Carpenter v. United States*, 138 S. Ct. 2206, 2210 (2018). A warrant is required to search one's private papers and effects, and that commandment does not disappear by dint of describing documents as mere ink on paper. The same is true of one's digital papers and effects, even if they amount to a heap of zeroes and ones on a server. In *Riley*, the Supreme Court specifically identified "Internet search and browsing history" as an example of private data stored on a cell phone that requires a warrant to search. 573 U.S. at 395–96. The Court recognized that it "could reveal an individual's private interests or concerns" and was precisely the sort of information that the Fourth Amendment should protect. *Id.*

4. The fact that the same search data may also be stored in a user's Google account does not diminish their Fourth Amendment interests in it. On the contrary, the Supreme Court has repeatedly emphasized that digital data deserves constitutional guarantees suited to the digital era. And as a result, the Court has been clear that judges are not to "mechanically apply" the third-party doctrine in the digital context. *Carpenter*, 138 S. Ct. at 2210; *see also United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (describing the third-party doctrine as "ill suited to the digital age").

5. The government now cites to Google's Privacy Policy as support for its position, but it ignores Google's testimony that search history *is* a part of a user's "account contents," Tr. at 27; 31, just like email messages, documents, and photos. Moreover, the documents the government cites are Google's current policies, not the ones in place at the time Mr. Seymour created his account. In fact, Mr. Seymour was still a child—twelve years old—when he created his Google account in 2016. And as Mr. Seymour has previously noted, Google's own terms require individuals to be at least 13 years old to create an account, meaning that Mr. Seymour could not have provided voluntary or meaningful consent. Google, *Age Requirements on Google Accounts*, https://perma.cc/Z6XG-N795 (last visited June 30, 2022).

6. Additionally, Mr. Seymour has a possessory interest in his search history data. Mr. Seymour has repeatedly made this argument to the Court in detail. *See* MTS at 15-17; Def. Reply at 3-6. The government, however, has failed to respond to it in any way. Instead, the government continues to mischaracterize the nature of the search, calling it a mere "database" search. This ignores the fact that the data in that database belongs to billions of individual users like Mr. Seymour. It does not belong to Google. Google stores it for their users, but at the end of the day, it is a part of an individual's "account contents," like email or photos. Tr. at 27, 31. Users retain the right to exclude others from it and they also retain the right to delete it. *See* Def. Reply at 3-6. Consequently, searching Mr. Seymour's search history was a trespass under the Fourth Amendment, just as it was for the billions of other Google users who also have a property interest in their data. It does not matter that the government did not search the "full accounts of Google users," *People's Written Arguments on Defendant's Motions to Suppress* at 3, because any intrusion into Mr. Seymour's Google data, even a small one, is a Fourth Amendment trespass.

7. Finally, the fact that Google employees use an automated process to execute the keyword warrant only heightens Fourth Amendment concerns. The government argues that it somehow lessens the intrusion because Google employees do not personally review the contents of each user account. *Id.* at 3. But as the Supreme Court recognized in *Carpenter*, a central aim of the Fourth Amendment was "to place obstacles in the way of a too permeating police surveillance." 138 S. Ct. at 2214. Thus, it mattered to the Supreme Court in *Jones* that it was cheap and easy to track a car using GPS. To achieve the same effect without technology would have required a "constable" to have "secreted himself somewhere in a coach and remained there for a period of time," *id.* at 420 (Alito, J., concurring), a feat which "would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience." *Id.* at 420 n3. And in *Carpenter*, the Court found it significant that, "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection," but "because location information is continually logged for all of the 400 million devices in the United States," "… [w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years." 138 S. Ct. at 2218. Here, the fact that there is a record of nearly all Google searches, stretching untold years, that can be quickly and automatically searched, provides the government with the same kind of "retrospective" information that would be "otherwise unknowable." *Id.*

8. Accordingly, this Court should "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," *id.* at 2214, and recognize that Mr. Seymour had both privacy and possessory interests in his Google search history data.

B. Overbreadth & Lack of Particularity

9. The keyword warrant here was a digital general warrant. It was unconstitutional in any iteration, no matter how many steps were involved. The "staged" process Google describes, *Exhibit – Attachment to Notice of Declaration of Legal Investigations Support Analyst Nikki Adeli (Google Declaration)* at ¶ 3, does not cure the warrant's fundamental constitutional defects: the absence of probable cause to search Mr. Seymour's data (or anyone else's), and a profound lack of particularity with respect to the accounts to be searched and the data to be seized.

10. The government attempts to obscure these defects by calling the search a "database inquiry," but the reality of what occurred is not so benign. It is not as if a Google employee looked at a user's search history and then repeated that search a billion times. It is far worse because it can be done automatically in the blink of an eye. It does not require the kind of resources and manpower that would have made such a search impossible in centuries past. It is easy, and that is the concern.

11. The fact remains that this "database inquiry" entailed scanning the private search history belonging to billions of Google users, including Mr. Seymour, over the course of 15 days. And critically, the government cannot point to a single account that it had probable cause to search, let alone Mr. Seymour's. Even Det. Sandoval admitted that before executing the keyword warrant, he did not have probable cause to search Mr. Seymour's Google account. *See* Tr. at 83 ("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.").

12. Because the government had no probable cause to search Mr. Seymour's data, they rely on the "staged" warrant process and the fact that the house was "not on a corner lot." *People's Written Arguments on Defendant's Motions to Suppress* at 4. But the warrant process is no substitute for probable case and the location of the house only gave rise to a "hunch" that the address "could have possibly been searched." Tr. at 83. In short, the government lacked probable cause to search of anyone's Google data and it should not be permitted to pretend that a digital dragnet, however pointed, is a constitutional replacement.

13. With respect to particularity, the government focuses on the object of the search but ignores the that the place to be searched is Google Headquarters instead of specifying individual accounts. As Mr. Seymour has argued, it does not matter how precisely the government can describe what it is looking for if they cannot identify where to search. *See Defendant's Reply to People's Responses to Motion to Suppress Evidence From a Keyword Warrant and Motions to Suppress Evidence Unlawfully Obtained* at 7-8. Supplying the street address for a company that stores the personal data for billions of users is not sufficiently particular. Like a warrant to search an apartment in a multi-family dwelling, it is critical to identify the

individual accounts to be searched. *See id.* It is not enough to identify a suspect after searching every apartment in the building, even if the intrusion was just a quick check of residents' cell phones for evidence of specific search activity.

14. Furthermore, the government does not challenge the fact that some of the data returned by Google does not match the terms in the keyword warrant, indicating that either the warrant was executed improperly or that it failed to adequately specify the data to be seized. *See* Gov. Arg. at 4. In fact, just five of the 61 searches produced by Google matched the search terms in the warrant—45 contained additional terms and 11 had no terms at all. *See Motion to Suppress Evidence From a Keyword Warrant* at 9-10; *Defendant's Reply to People's Responses to Motion to Suppress Evidence From a Keyword Warrant and Motions to Suppress Evidence Unlawfully Obtained* at 10. The government asserts that the Court should not consider this information because, it contends, it "does not bear on the constitutional or statutory requirements for a search warrant" and it is not "contained within the four corners of the warrant." *Written Arguments on Defendant's Motions to Suppress* at 4. On the contrary, the failure to adequately specify the things to be seized is basic grounds for invalidating a warrant and the fact that the government's conduct is not described in the warrant is no obstacle to challenging the scope and execution of the search. *See People v. Staton*, 924 P.2d 127, 131 (Colo. 1996) (finding the warrant failed to delineate the evidence to be seized but that the incorporated affidavit was sufficiently particular); *People v. Donahue*, 750 P.2d 921, 923 (Colo. 1988) (failing to specify the items to be seized); *People v. King*, 292 P.3d 959, 961 (Colo. App. 2011) (scope of warrant exceeded); *United States v. Young*, 263 F. App'x 710, 716 (10th Cir. 2008) (same).

C. Good Faith / Veracity

15. The government misstates Mr. Seymour's position with respect to the good faith doctrine. Mr. Seymour's argument is *not* "based solely on what he claims are 'omissions' in the affidavit." *People's Written Arguments on Defendant's Motions to Suppress* at 5. Rather, as Mr. Seymour made clear in his original motion to suppress, the good faith exception should not apply here for three reasons: (1) the warrant was based on Det. Sandoval's knowing or recklessly false statements; (2) the warrant affidavit lacked a substantial basis to determine probable cause; and (3) no officer could reasonably presume the warrant was valid. *See Motion to Suppress Evidence From a Keyword Warrant* at 23; *Defendant's Reply to People's Responses to Motion to Suppress Evidence From a Keyword Warrant and Motions to Suppress Evidence Unlawfully Obtained* at 11; *see also Leon*, 468 U.S. at 926. The government chooses to respond only to the first argument, but Mr. Seymour has thoroughly briefed the other two and reiterates that the good faith doctrine should not apply for any of these three reasons.

16. With respect to Det. Sandoval's affidavit, the government does not dispute that he failed to inform Judge Zobel that the warrant would involve the search of a billion accounts. *People's Written Arguments on Defendant's Motions to Suppress* at 5. Instead, the government contends that Det. Sandoval should be off the hook because "he had never prepared a keyword search warrant before and he did not know how the search would be conducted." *Id.*

17. But Det. Sandoval asked Judge Zobel to rely on his "training and experience"—of which he had none for keyword warrants. *See Attachment 3 to Motion to Suppress Evidence From a Keyword Warrant (Keyword SW 3)* at 2-3; *see also* Tr. at 144. That was reckless. Det. Sandoval knew he had no experience with keyword warrants, but instead mislead the judge to believe he understood what he was asking for. Had he understood, and had he conveyed that information to Judge Zobel, there is little doubt that the application would have been rejected. The fact that Google rejected the first two keyword warrants should have been a red flag as well. But instead, Det. Sandoval forged ahead with a new judge and recklessly omitted critical facts about the search.

18. Had Det. Sandoval included these facts, it would have become apparent that the warrant was an impermissible general warrant. It would have been obvious that the affidavit lacked a substantial basis for probable cause to search Mr. Seymour, and that the warrant did not identify a single Google account out of the billions it sought to search. *See Motion to Suppress Evidence From a Keyword Warrant* at 26-28; *Defendant's Reply to People's Responses to Motion to Suppress Evidence From a Keyword Warrant and Motions to Suppress Evidence Unlawfully Obtained* at 11-14.

19. Furthermore, had Det. Sandoval properly informed the court, it also would have become clear that the Stored Communications Act simply does not apply to dragnet searches like this one. The Dictionary Act does not control because here, "the context indicates otherwise." 1 U.S.C. §1. The SCA also prohibits the government from obtaining records that are not "relevant and material" to the ongoing criminal investigation. *See* 18 U.S.C. § 2703(d). And at minimum, the "relevant and material" requirement under the SCA is more demanding than the mere "relevance" standard governing, for which courts have consistently required the government show an actual connection to a particular investigation. *See, e.g.*, *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951) (invalidating a subpoena's "catch-all provision" on the grounds that it was "merely a fishing expedition to see what may turn up"). Courts have also rejected or narrowed subpoenas that, because they fail to identify the outer bounds of the categories of records they seek, cover large volumes of *irrelevant* documents. *See In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993*, 846 F. Supp. 11, 12 (S.D.N.Y. 1994) (Mukasey, J.) (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"). Where, as here, the government indiscriminately seeks records implicating the privacy of billions of individuals in one fell swoop, it cannot possibly meet the standard in establishing a "relevant and material" need for *all* of those records. A keyword warrant is plainly not the kind of search authorized by the SCA and Det. Sandoval should have known or disclosed that.

II. The Motions to Suppress: Accounts, Cellphone Records, Cellphone Data, Home, and Social Media

20. The People again rely on the "nexus" sections contained in the affidavits associated with each warrant. These warrants lack a sufficient nexus between the alleged criminal activity, the data and items to be seized, and the places to be searched.

21. The People argue that the particularity requirement was satisfied for each of the warrants because the data to be searched for and seized or to be provided to law enforcement was described with "sufficient detail that the persons executing the search knew exactly what data they were authorized to seize/provide." *People's Written Arguments on Defendant's Motions to Suppress* at 6. This is not, as the People contend, "all that is required" by *People v. Roccaforte*, 919 P.3d 799, 802 (Colo. 1996). *See Id.* at 6.

22. *Roccaforte* provides instead that an "all records" warrant is not sufficiently particularized unless 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." *Id*. There is a significant difference between the facts in *Roccaforte* and the facts in this case. Despite the People's argument regarding nexus, there is no nexus between the requested information in the search warrants and the alleged offense.

23. The People also again rely on the fact that most people today possess and use cellphones, despite the fact that the surveillance videos do not show anyone using a cellphone before, during, or after the arson.

24. Lastly, the People again argue that the evidence collected needs to be attributed to its source. The People originally made this argument in relation to Mr. Seymour's cellphone data. Mr. Seymour's cellphone was taken from him when he was arrested. There was no dispute over who had possession of his cellphone, and pursuant to *People v. Herrera*, 357 P.3d 1227, 1228 (Colo. 2015), a warrant authorizing a search of all data which "tends to show possession" over a cellphone transforms the warrant into a general warrant violative of the Fourth Amendment.

CONCLUSION

WHEREFORE, Mr. Seymour moves this Court to order to suppress all evidence obtained from the November 19, 2020, keyword warrant, as well as fruits thereof, as well as his motions to suppress evidence unlawfully obtained regarding his accounts, his cellphone records, his cellphone data, his home, and his social media.

Respectfully submitted,

Dated this day: September 30, 2022

/s/ Jenifer Stinson

_____

Attorney: Jenifer Stinson, #35993

_____

Attorney: Michael S. Juba, #39542

_____

Attorney: Michael W. Price, #22PHV6967

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

_____

Signature