Anne Taylor Law, PLLC
Anne C. Taylor, Attorney at Law
PO Box 2347
Coeur d'Alene, Idaho 83816
Phone: (208) 512-9611
iCourt Email: info@annetaylorlaw.com

Jay W. Logsdon, First District Public Defender
Idaho State Public Defender
1450 Northwest Blvd.
Coeur d'Alene, Idaho 83814
Phone: (208) 605-4575

Elisa G. Massoth, PLLC
Attorney at Law
P.O. Box 1003
Payette, Idaho 83661
Phone: (208) 642-3797; Fax: (208)642-3799

Assigned Attorney:
Anne C. Taylor, Attorney at Law, Bar Number: 5836
Jay W. Logsdon, First District Public Defender, Bar Number: 8759
Elisa G. Massoth, Attorney at Law, Bar Number: 5647

IN THE DISTRICT COURT OF THE FOURTH JUDICIAL DISTRICT OF THE STATE OF IDAHO, IN AND FOR THE COUNTY OF ADA

STATE OF IDAHO **Plaintiff,** **V.** **BRYAN C. KOHBERGER,** **Defendant.**	**CR01-24-31665** **MOTION TO SUPPRESS AND MEMORANDUM IN SUPPORT** **RE: GOOGLE WARRANTS DATED 1-3-23, 1-24-23, and 2-24-23**

COMES NOW, Bryan C. Kohberger, by and through his attorneys of record, and submits the following Memorandum in support of his contemporaneously filed Motion for an Order suppressing all data found by law enforcement from its search for Google data obtained from three warrants dated January 3, 2023, January 23, 2023, and February 24, 2023. That data includes

emails, personal contacts, financial information, documents, PowerPoint presentations, photos, IP addresses and more.

The Motion and documents in Support of a *Franks v. Delaware* 438 U.S. 154 (1978) hearing are hereby incorporated into this Memorandum. The proffer with supportive documentation regarding *Franks* are filed under seal. For that reason they are not set forth in full detail here, but instead are incorporated.

ISSUES

I. The Affidavit Submitted in Support of the Application for the Issued Search Warrants Recklessly or Intentionally Omitted Material Information.

II. The Affidavits Submitted in Support of the Applications for the Issued Search Warrants Included Information that Must be Excised.

- **a. All information in the affidavit was gathered because of law enforcement's unconstitutional and intentionally omitted use of Investigative Genetic Genealogy, and thus nothing in the warrant should remain.**
- **b. Information gathered about Mr. Kohberger via previous invalid warrants must also be excised.**

III. The search warrants are duplicative and fail to command law enforcement to search the Google accounts.

IV. The search warrants fail to provide specific particularization of what law enforcement could search.

V. Mr. Kohberger has a privacy interest in his Google information and email accounts, protected by Art. I Sec. 17 of the Idaho Constitution and the Fourth Amendment.

FACTS

Pennsylvania law enforcement, along with officers from Idaho and the FBI, arrested Mr. Kohberger on December 30, 2022. Subsequent to Mr. Kohberger's arrest, many warrants were executed. On January 3, 2023, Moscow Police Detective Mowery began work on Google warrants. He obtained Google Warrant One on January 3, 2023, a search warrant for all data available in a Google Account in connection with the email BryanChristopher1994@gmail.com plus two phone numbers and an IMEI number. (Exhibit A) On January 25, 2023 Mowery obtained a Google Warrant Two, a search warrant for all data available in a Google Account in connection with yewsrineighm@gmail.com. (Exhibit B) No specific nexus is mentioned in the second warrant for the new email account other than it was identified. On February 24, 23 Mowery obtained Google Warrant Three, seeking all data available in relation to Mr. Kohberger. (Exhibit C) No reference is made in the affidavit to a nexus between Kohberger and bk5781@gmail.com. Google Warrant Three adds the email account bk5781@deslaes.edu without explanation. (Exhibit C) The warrants have no limiting language in the search and no justification for duplication. Google Warrant three return, signed by Payne March 14, 2023, references a warrant return only for the wrong email: Bryanchistopher@gmail.com instead of bryanchristopher1994@gmail.com; (Exhibit D) the receipt and inventory, also signed by Payne references Bryanchristopher@gmail.com and yewsirneighm@gmail.com but the return or the receipt and inventory report nothing about bk5781@desales.edu. (Exhibit E) This is particularly noteworthy because email communication between Mowery and Google on January 4, 2022 reference Google not producing data on non-personal accounts (*i.e.* desales.edu), Mowery indicates, "they [Desales] are going to be able help us with their end of the process. So that should be taken care of." (Exhibit F) Yet, bk5781@deslaes.edu found its way into Google Warrant Three without any nexus or explanation on February 24. 2022.

The information in the warrants was cut and pasted from an affidavit originally bearing the signature of Moscow Police Department Sgt. Blaker, at other times Cpl. Payne and now Mowery. The Google specific information in Google Warrant One referenced the United States and government as well as the search of a phone for single decedent (*i.e.* looking for the location of a decedent), indicating it was cut and pasted without edits. Google Warrants Two and Three remove the United States language, reference to the government, and the single decedent language.

The basic facts Mowery used to support the searches were those listed in Exhibit B, which are those that had been used to support arrest. Exhibits B to the three Google warrants were different versions of the arrest warrant and:

1. Details about Google as a company and what it stores based on Mowery's "personal knowledge"
2. A request for any accounts associated with Kohberger for any time periods
3. Kohberger was observed entering a CVS in Pennsylvania on December 16, 2022 and his email account Bryanchristopher1994@gmail.com and phone number was somehow obtained by law enforcement.
4. For Google Warrant Two, January 24, 2023 a new email is referenced as having been found in Google warrant one data return: yewsirneighm@gmail. *See* Exhibit B
5. Also added was "a high probability a VPN was identified in Google return 1/3/23. *See* Exhibit B
6. For Google Warrant Three, a new email, bk5781@desales.edu is incorporated into the third warrant without any supporting explanation. *See* Exhibit C.

ARGUMENT

I. The Affidavit Submitted in Support of the Application for the Issued Search Warrant Recklessly or Intentionally Omitted Material Information.

"The Fourth Amendment states unambiguously that "no warrants shall issue, but upon probable cause, supported by Oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Groh v. Ramirez,* 540 U.S. 551, 557 (2004) (quoting U.S. Const. Amend. IV.). 'Probable cause' exists when, given all the circumstances set forth in the affidavit, "there is a fair probability that contraband or evidence of a crime will be found *in a particular place*." *Illinois v. Gates,* 462 U.S. 213, 238 (1983) (emphasis added).

"For a search warrant to be valid, the judge issuing the warrant must rely on an affidavit or affidavits sworn to before the judge or by testimony under oath and recorded that establish the grounds for issuing the warrant." *State v. Nunez,* 138 Idaho 636, 640, 67 P.3d 831, 835 (2003). "Any discrepancy between the items for which there was probable cause and their description in the search warrant requires suppression." 23 C.J.S. *Criminal Procedure and Rights of Accused* § 887 (2022). "It is clear that the issuing Magistrate himself, if he is to fulfill the constitutionally mandated function of interposing an independent intelligence between the law enforcement officer and the citizen, must actually and in fact, draw the inferences from the evidence presented to him." *People v. Potwora,* 48 N.Y.2d 91, 94, 397 N.E.2d 361, 363 (Ct. App. 1979). "It is for this reason that the courts have insisted that the full facts from which inferences might be drawn, and information necessary to determine their reliability, be placed before the issuing magistrate." *Potwora,* 48 N.Y.2d at 94, 397 N.E.2d at 363.

Finally, "[a] criminal defendant may challenge the veracity of an affidavit used to obtain a search warrant." *State v. Peterson,* 133 Idaho 44, 47, 981 P.2d 1154, 1157 (Ct. App. 1999). Upon a preliminary showing of a warrant's deficiency, the defendant must prove, by a preponderance of

the evidence, "that intentional or reckless falsehoods were included in the warrant affidavit and were material to the magistrate's finding of probable cause, or that material exculpatory information was deliberately or recklessly omitted." *Peterson,* 133 Idaho at 47, 981 P.2d at 1157. "An omission of exculpatory facts is "material" only if there is a substantial probability that, had the omitted information been presented, it would have altered the magistrate's determination of probable cause." *Id.* "Whether an omission was intentional or reckless might be inferred, in part, from the relative importance of the information and its exculpatory power." *Id.,* 133 Idaho at 48, 981. P.2d at 1158.

In this case, law enforcement either intentionally or recklessly omitted exculpatory evidence as to almost every facet of its affidavit for this warrant. Thus, it will require suppression.

II. The Affidavits Submitted in Support of the Application for the Issued Search Warrants Included Information that Must be Excised.

Where information in a warrant was obtained via a violation of the constitution, Idaho courts excise that information. *See, e.g*., *State v. Johnson*, 110 Idaho 516, 526 (1986); *State v. Bunting*, 142 Idaho 908 (Ct.App.2006)*; State v. Buterbaugh*, 138 Idaho 96, 101 (Ct. App.2002).

a. All information in the affidavit was gathered because of law enforcement's unconstitutional use of Investigative Genetic Genealogy, and thus nothing in the warrant should remain.

Mr. Kohberger has argued in a separate Motion that the genetic genealogy investigation in this matter was done in violation of the constitution. Additionally, he argues there would be no investigation into him without that original constitutional violation. It is not that the results of the IGG sped up the investigation. Instead, they focused the investigation on Mr. Kohberger, a person whose only connection to the case was his mode of transportation and the shape of his eyebrows, two identifications of little to no value. *See Franks* Motion filed simultaneously. As the Idaho

Supreme Court has explained, while the initial burden in showing a factual nexus between the illegality and the evidence, the State must show it would have been discovered anyway. *State v. Maahs*, 171 Idaho 738, 752 (2022). The State cannot make this showing. Without IGG, there is no case, no request for his phone records, surveillance of his parents' home, no DNA taken from the garbage sitting in his driveway, in a gated community, subject to a garbage removal ordinance. Because the IGG analysis is the origin of this matter, everything in the affidavit should be excised.

b. Information gathered about Mr. Kohberger via previous invalid warrants must also be excised.

Separately, the information gathered via the various other warrants should be excised for the reasons set out in the *Franks* proffer and as argued in the other motions to suppress such as the ATT and trap and trace data.

III. The search warrants fail to command law enforcement to search the Google Accounts.

The warrants in this matter fail to actually provide a command to search the Google account. They state::

(1) there are grounds for issuing a search warrant

(2) there are grounds to believe the property referred to and sought in or upon said premises consists of information related to investigation of crimes… on the Google account of…"

(3) the command is made to search the premises for the property and seize it. The premises is Google LLC at 1600 Amphitheater Parkway Mountain View, CA 94043

(4) there is no incorporating language for the search warrant affidavit.

The Idaho Supreme Court found in *Adamcik v. State*, 163 Idaho 114, 124-25 (2017):

> The Fourth Amendment to the United States Constitution requires that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." However, decisions must "reflect the recognition that the Fourth Amendment's commands, like all constitutional requirement, are practical and not abstract." *United States v. Ventresca*, 380 U.S. 102, 108, 85 S.Ct. 741, 13 L.Ed.2d

> 684 (1965). The circuit courts are nearly uniform in allowing an affidavit to support the particularity requirement when the warrant suitably references the affidavit, and the affidavit accompanies the warrant. *See, e.g.*, *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 699–700 (9th Cir. 2009); *United States v. Waker*, 534 F.3d 168, 172 (2d Cir. 2008); *Rodriguez v. Beninato*, 469 F.3d 1, 5 (1st Cir. 2006); *United States v. Ortega-Jimenez*, 232 F.3d 1325, 1329 (10th Cir. 2000). The Supreme Court has acknowledged "that a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Groh v. Ramirez*, 540 U.S. 551, 557–58, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004). In *SDI Future*, the Ninth Circuit held that a statement on the face of the warrant noting "the supporting affidavit(s)" was sufficient as a suitable reference and incorporation. 568 F.3d at 700.

The court relied on these findings to dismiss a post-conviction claim, finding the defendant would not have been successful had he challenged the fact that the computer searched was omitted from items to be searched in the "command" section of the warrant. *Id.* at 124.

In this case, however, there is no reference to the affidavit, only to "proof". In *Adamcik*, the Court found the warrant explicitly reference the affidavit. In *SDI Future*, the court relied on a reference to "*Upon the sworn complaint made before me*" (emphasis in original). 568 F.3d at 700. The word "proof" does not specify that the Court relied on the affidavit for its probable cause determination. Additionally, there is no evidence that the warrants and affidavits were attached to each other. Thus, the warrants did not permit the searches.

IV. The search warrants fail to provide specific particularization of what law enforcement could search on the Google Accounts.

The Fourth Amendment and Article I § 17 of the Idaho Constitution do not permit email and its attachments to be searched without a valid warrant. There is a subjective expectation of privacy in email and attachments that society is prepared to recognize as reasonable. *Kyllo v. United States*, 533 U.S. 27, 33, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) and *United States v. Wilson* 13 F.4th 961 (9th Cir. 2021). The United States Supreme Court "when confronting new concerns wrought by digital technology, … has been careful not to critically extend existing precedents."

Wilson . citing *Capenter*, 138 S.Ct. at 2222. A warrant is not a magical wand that grants access to anything a Google account contains. Courts have long required that warrants be sufficiently particular to allow a government agent to know what may be seized, viewed, or searched, and what may not. *See, State v. Yoder*, 96 Idaho 651, 653 (1975).

> A search warrant must be particular enough so that " [a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States,* 275 U.S. 192, 196, 48 S.Ct. 74, 76, 72 L.Ed. 231, 237 (1927). However, this statement is not to be read literally. [*State v.] Weimer,* 133 Idaho [985,] 449, 988 P.2d [927,] 223 [(Ct.App.2008)]; 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 4.6(a), at 605 (4th ed.2004). Instead, the "warrant must enable the searcher to reasonably ascertain and identify the things which are authorized to be seized." *United States v. Cook,* 657 F.2d 730, 733 (5th Cir.1981); *see also United States v. Betancourt,* 734 F.2d 750, 754 (11th Cir.1984). The specific evil that the particularity requirement guards against "is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings." *Weimer,* 133 Idaho at 449, 988 P.2d at 223. A warrant accomplishes this objective by requiring a particular description of the things to be seized. *Id.*

State v. Teal, 145 Idaho 985, 991 (Ct.App.2008).

In striking a balance between law enforcement interests and rights of individuals to be free of unreasonable searches and seizures, "the process of segregating electronic data that is sizeable from that which is not must not become a vehicle for the government to gain access to data which it has not probable cause to collect". *Comprehensive Drug Testing, Inc*. 579 F.3d 989, 1177 (9th Cir. 2009). There must be some threshold showing before the government may "seize the haystack to look for the needle." *U.S. v. Hill,* 59 F.3d 966 (9th Cir. 2006).The three Google warrants lack appropriate particularization for three separate email accounts, two phone numbers and one IMEI number. They list the following as possibly existing on the accounts:

- Google Account subscriber information, as defined in 18 U.S.C. § 2703(c)(2);
- Google Account recent activity logs and connected devices;
- Google email messages (Gmail) including drafts and those in the trash;
- Google Pay- Account information and transactions;
- Calendar- calendar events;
- Contacts - people contact files;

• Photos- photos, videos and albums, and associated metadata;
• Drive- documents, spreadsheets, presentations and files, and associated metadata;
• Keep- titles and the notes;
• Hangouts and Chats- messages, including attachments such as photos;
• Location History- location data and deletion records;
• My activity- searches and browsing history, including activity from Web & App Activity, Google Assistant, and Google Home;
• Google Voice- Google Voice information, including Google Voice basic subscriber information, call logs, forwarding number, text messages, and voicemails;
• YouTube- Registration email, channel ID, display name, IP logs, and account registration information;
• Android- records for Android Devices, to include subscriber information, other associated accounts, cellular ~carrier information, and device/hardware information;
• Google Play- Google Play purchases made and Google Play applications Downloaded.

The data compilation is too broad in that it makes no attempt at narrowing and results instead in a blanket request for everything available in a Goggle account, which is akin to the search of all electronic records, an entire computer, or all data on a cell phone. It is a request for the full "haystack."

Jurisdictions across the nation agree that such broad warrants are problematic but found that trying to fix that issue via more particularized warrants has its own issues. Still, this case presents a warrant that is overbroad under the long-standing principles of Article I Section 17 and the Fourth Amendment.

First, this Court should review what Idaho courts have already held about particularity. In *State v. Caldero*, 109 Idaho 80 (Ct.App.1985), the Court of Appeals found:

The requirements of probable cause and particularity serve different purposes.

> [There are] two distinct constitutional protections served by the warrant requirement. First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause.... The second, distinct objective is that those searches deemed necessary should be as limited as possible. Here, the specific evil is the "general warrant" abhorred by the colonists, and the problem is not that of intrusion *per se,* but of a general, exploratory rummaging in a person's belongings.... The warrant accomplishes this second objective by requiring a particular description of the things to be seized.

Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 (1971).

> In our view, the particularity requirement is as important today as it was to the framers of the fourth amendment. It protects all citizens from unduly broad intrusions upon the privacy of their persons, houses, papers and effects by government agents. As noted by one distinguished authority:
>
> > If the police, upon obtaining entry to a house under a search warrant, were permitted to seize any item, regardless of its connection with crime and regardless of whether they knew the item was on the premises, the requirement that a warrant particularly describe the items to be seized, and that only items for which probable cause exists be seized, would be meaningless. In effect, a warrant to enter the premises to search would be a general warrant in actual execution, if not in form.
>
> W. RINGEL, SEARCHES & SEIZURES, ARRESTS AND CONFESSIONS § 6.5(a),at 6–24 to –25 (1979 with 1984 Supp.).

In that case, the court considered a filing cabinet not mentioned in the warrant. *Id.* The state argued that the cabinet could be searched under the plain view doctrine. *Id.* The court disagreed, holding:

> More fundamentally, the fourth amendment does not countenance the seizure of a container, such as the file cabinet, which is outside the scope of any warrant and which bears no outwardly apparent connection with any crime, simply for the purpose of searching it later.

Id. at 85. However- the court also noted in *dicta*:

> We have considered the possibility that Caldero's personal papers inside the file cabinet might have furnished the necessary link to criminal activity. It would have been permissible for the officers to look inside the cabinet for items, such as a manuscript, listed in the search warrants. Had they done so, the personal papers would have been discovered.

Id. To be clear, what the court held was that the warrant controlled the discretion of the officers performing the search as to what was to be seized, but not what might be searched to locate the items listed.

Consider the practicalities of what the court has held- if it is not listed in the warrant, it cannot be seized, but you may search to your heart's content for the things listed in the premises named. Then, try and compare this to searching a cell phone. In the words of the Supreme Court:

> That is like saying a ride on horseback is materially indistinguishable from a flight to the moon… Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

Riley v. California, 573 U.S 400, 393 (2014)

In *U.S. v. Comprehensive Drug Testing, Inc*., 579 F.3d 989, 1176 (9th Cir. 2009), the court found:

> This pressing need of law enforcement for broad authorization to examine electronic records, so persuasively demonstrated in the introduction to the original warrant in this case, see pp. 1167–68 supra, creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.

This concern grew in the aftermath of *Riley*, with a number of jurists *See, e.g., State v. Mansor*, 421 P3d 323, 345 (Or.2018); *Wheeler v. State,* 135 A.3d 282, 299 (Del.2016). In the words of one:

> Of course, *Riley* requires that officers first get a warrant, 573 U.S. at 403, 134 S.Ct. 2473, but if the fact that the arrestee was carrying a cell phone at the time of arrest is sufficient to support probable cause for a search, then the warrant requirement is merely a paperwork requirement. It cannot be that *Riley's* holding is so hollow.

U.S. v. Morton, 46 F.4th 331, 340 (2022) (HIGGISON, CJ, concurring).

In *State v. Castagnola*, 46 N.E.3d 638, 656 (Ohio, 2015), the court rejected that in the case of a computer it was enough to state the offense charged and the items to be searched for. In that case, the search warrant commanded a computer be searched for "records and documents" which "if found,… will be seized and used as evidence of" and provided the crimes alleged. *Id.* at 657. The court found that:

> A search warrant that includes broad categories of items to be seized may nevertheless be valid when the description is " ' "as specific as the circumstances and the nature of the activity under investigation permit." ' " *Guest v. Leis,* 255 F.3d 325, 336 (6th Cir.2001), quoting *United States v. Henson,* 848 F.2d 1374, 1383 (6th Cir.1988), quoting *United States v. Blum,* 753 F.2d 999, 1001 (11th Cir.1985). Warrants that fail to describe the items to be seized with as much

> specificity as the government's knowledge and the circumstances allow are "invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized." *United States v. Fuccillo,* 808 F.2d 173, 176 (1st Cir.1987).

Id. The court then found that the warrant failed the test in two respects. First, it left to the discretion of the investigator what was relevant to the crimes alleged. *Id*. at 658. Second, it made no attempt to delineate the types of files that court be relevant to what the police believed they would find in that particular case- evidence that the defendant had made an online search of his alleged victim's address. *Id.* In those circumstances, there was no reason to go looking at videos and pictures. *Id.*

Thus, returning to our analogy, the Ohio Supreme Court found the warrant failed as to where (category) and what (description of the file sought). As the Court noted, the where and what can be named with more specificity based on what is known to law enforcement. In this case the things to be seized are an exhaustive list of everything that is available in Google accounts—not once but three separate times. Law enforcement was certainly capable of greater specificity in all three instances, but instead gave itself an overbroad mandate permitting it complete access to everything from Mr. Kohberger's Google accounts.

Another example of a court cracking down on overbroad digital warrants is *Wheeler v. State,* 135 A.3d 282 (Del. 2016). In *Wheeler*, investigators used a warrant with several parts, including one explaining terminology, one explaining that digital information basically never becomes stale, and one setting out the facts of the case and explaining that additional emails or text messages. *Id*. at 288. The warrant, however, commanded law enforcement to collect any device that contained data, and any data found thereon. *Id.* at 289. The Delaware Supreme Court found the warrant overbroad. *Id*. at 295.

The court began by recalling the hatred of the colonists towards general warrants. *Id.* at 297. The court then noted that the United State Supreme Court had found that warrants for the

digital contents of a cellphone gave the government access to more information than a house. *Id.* at 299. The court acknowledged the difficulties in specifying what categories of data are sought when criminals are known to hide data in files. *Id.* at 301 (*citing U.S. v. Stabile*, 633 F.3d 219, 237 (3rd Cir. 2011) (*citing U.S. v. Burgess*, 576 F.3d 1078, 1092-94 (10th Cir. 2009)). The court then reviewed both *U.S. v. Riccardi*, 405 F.3d 852 (10th Cir. 2005) and *Castagnola*, noting in both cases the courts found digital warrants overbroad where no limitation was included as to what to seize.

The Court then held:

> We hesitate to prescribe rigid rules and instead reiterate that warrants must designate the things to be searched and seized as particularly as possible. Striking the correct balance when protecting against generality and overbreadth requires vigilance on the part of judicial officers who are on the front lines of preserving constitutional rights while assisting government officials in the legitimate pursuit of prosecuting criminal activity. Where, as here, the investigators had available to them a more precise description of the alleged criminal activity that is the subject of the warrant, such information should be included in the instrument and the search and seizure should be appropriately narrowed to the relevant time period so as to mitigate the potential for unconstitutional exploratory rummaging.

Wheeler, 135 A.3d at 305 (*citing United States v. Bright*, 630 F.2d 804, 812 (5th Cir.1980) (*citing James v. United States*, 416 F.2d 467, 473 (5th Cir.1969), *cert. denied,* 397 U.S. 907 (1970)); *United States v. Ford,* 184 F.3d 566, 576 (6th Cir.1999).

The *Wheeler* case is important to this case for the principle that the government must make the warrant as particular as it knows how to make it. In the case at bar, the government is investigating a quadruple homicide in Idaho. Does it make sense to see if there is some hint at wanting to fight someone from two years prior? Five years? Ten? What of everything else that may be relevant to what the police knew- the contents of his phone, computers, Ka-Bar sheath and the Elantra? For that matter, what of the victims themselves? Their sororities and fraternities? The

warrant *could* have specified what was to be seized and searched, but it did not. The court in *Wheeler* condemns government attempts to cast too broad a net under these circumstances.

The warrant issued for Mr. Kohberger's Google accounts were unconstitutionally overbroad. Law enforcement had the ability to be more specific both as to the contents and the category of the digital files it sought, and it chose not to be specific because what it wanted, and what it got, was a general warrant. Therefore, everything found in the search of the Google accounts must be suppressed.

CONCLUSION

Mr. Kohberger requests this Court suppress all evidence obtained by police via the three searches of his Google accounts. As explained above, the warrants used lacked probable cause as written, given its heavy reliance on conclusions reached by law enforcement without the details necessary for the magistrate to draw its own conclusions, because the warrants omitted exculpatory information and information that put into question the reliability of the facts upon which it relies, because the affidavits relied on evidence gained in violation of the constitution, and the warrants lacked particularity making them general warrants. This was all in violation of the Fourth Amendment and Art. I Sec. 17 of the Idaho Constitution.

DATED this 13th day of November, 2024.

BY: /s/ Elisa G. Massoth
Elisa G. Massoth

CERTIFICATE OF DELIVERY

I hereby certify that a true and correct copy of the foregoing was personally served as indicated below on the ___14____ day of November, 2024 addressed to:

Latah County Prosecuting Attorney –via Email: paservice@latahcountyid.gov
Elisa Massoth – via Email: legalassistant@kmrs.net
Jay Logsdon – via Email: Jay.Logsdon@spd.idaho.gov
Jeffery Nye, Deputy Attorney General – via Email: Jeff.nye@ag.idaho.gov
Ingrid Batey, Deputy Attorney General – via Email: ingrid.batey@ag.idaho.gov

Exhibits A through F

Motion to Suppress and Memo in Support RE: Google

Filed Under Seal with the Court on 11/18/24