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.**	**CASE NUMBER CR01-24-31665** **MOTION TO SUPPRESS AND MEMORANDUM IN SUPPORT** **RE: APPLE ACCOUNT FEDERAL GRAND JURY SUBPOENA AND SEARCH WARRANT DATED AUGUST 1, 2023**

COMES NOW, Bryan C. Kohberger, by and through his attorneys of record, and submits the following Memorandum with exhibits in support of his contemporaneously filed Motion for an Order suppressing all data found by law enforcement from its search of his Apple accounts, primarily his iCloud account.

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. Mr. Kohberger has a privacy interest in his Apple account information protected by Art. I Sec. 17 of the Idaho Constitution and the Fourth Amendment, requiring a valid warrant.

II. The Affidavit Submitted in Support of the Application for the Issued Search Warrant Recklessly or Intentionally Omitted Material Information, relies on information gained in violation of the constitution, and fails to provide probable cause for the requested search.

- **a. The Affidavit Submitted in Support of the Application for the Issued Search Warrant Included Information that Must be Excised.**
- **b. 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.**
- **c. Information gathered about Mr. Kohberger via previous invalid warrants must also be excised.**

III. The Search Warrants Fail to Command Law Enforcement to Search the Apple Accounts or Contents of the iCloud.

IV. The Search Warrants Fail to Provide Specific Particularization of What to Search.

FACTS

On December 21, 2022, the FBI issued a preservation request letter to Apple Inc. (Exhibit A). On December 30, 2022, Pennsylvania law enforcement, along with officers from Idaho and the FBI, raided Mr. Kohberger's parents' home at 119 Lamsden Drive, in Albrightsville, Pennsylvania, and arrested him.[1] An iPad was located at the parents' home; but it was not seized because it was found in a common area. During a subsequent search of Mr. Kohberger's vehicle, a receipt was located for an Apple iPad.[2] Based on incomplete[3] records available to the defense, FBI served a Grand Jury Subpoena on Apple on January 12, 2023, and Apple produced responsive data on January 27, 2023, for Apple Accounts DSID 1012112549 and DSID 10616147671. (Exhibit B). The data was shared with Cpl. Brett Payne of the Moscow Police Department. Subsequently, Apple sent an email to FBI Tactical Specialist Maria Tyndall acknowledging receipt of a preservation request on April 6, 2023. (Exhibit C). Over the next few days, Detective Mowery of the Moscow Police Department was included in an email chain discussing Apple's response to the preservation request. The communications reference "setting up a chat" with Apple's point of contact to discuss issues that need clarified or resolved. The communications also include Apple telling law enforcement which accounts do or don't exist for Mr. Kohberger.

Perhaps recognizing that subpoenaing Mr. Kohberger's records was a violation of the United States and Idaho Constitutions, on August 1, 2023, Cpl. Payne of the Moscow Police requested a warrant for the same information subpoenaed from Apple Inc. by the FBI (Apple Accounts DSID 1012112549 and DSID 10616147671), admitting in his affidavit that the FBI had

[1] Exhibit D, p. 23.
[2] Exhibit D, pp. 23 and 30.
[3] Grand Jury subpoenas issued by the government have been the subject of a motion to compel. There is an order to compel their production "if available" or at a minimum for the state to provide dates. The state has done neither. Order on Defendant's 4th and 5th Motions to Compel June 14, 2024. The issues in the memorandum are among the reasons a copy of the subpoenas are necessary. It is unclear what the subpoena asked for or its scope. The subpoena return identifies two iCloud accounts.

already subpoenaed the requested information. (Exhibit D). Cpl. Payne served the subpoena later that day via email. On August 7, 2023, Apple sent an email to Cpl. Payne responding to the warrant and providing access to the responsive data. On August 9, 2023, Cpl. Payne, and Detective Mowrey downloaded the data provided by Apple in response to the search warrant. (Exhibit E). The data was inventoried, and a return of search warrant was prepared. (Id.).

The August 1, 2023, Affidavit for Search Warrant was signed by Cpl. Brent Payne. (Attached hereto as Exhibit D). However, most of the information in the warrant was cut and pasted from an affidavit originally bearing the signature of Moscow Police Department Sgt. Blaker, but according to Payne, now the sworn statement of Cpl. Payne.

The basic facts Payne used to support the search beyond those included in the arrest affidavit were:

1. His knowledge of Apple and what data it maintains with an Apple ID.
2. The method that iCloud uses to "create, store, access, share, and synchronize data" on any internet connected device, including back up of "devices data."
3. On January 7, 2023 Apple had responded to the federal grand jury subpoena that a "full iCloud account under the name Bryan Kohberger was in Active status" and another account wifiarmyowns@yahoocom was inactive.
4. Using the information produced in the federal grand jury subpoena Cpl. Payne "determined" that the "AMS Subscirber_Account" was linked to bkohberger@spartan.northahmpton.edu.
5. Timing of account access, as searched by Cpl. Payne, was around December 20, 2022, when Payne knew Kohberger was in Pennsylvania "still accessing the Apple account with a known iCloud before the homicides and then days before his arrest."
6. Cpl. Payne requested a very broad time frame of October 7, 2016 to December 30, 2022 and for any and all Apple accounts linked.

ARGUMENT

I. Mr. Kohberger has a privacy interest in his Apple account information protected by the Fourth Amendment of the United States Constitution and Art. I Sec. 17 of the Idaho Constitution, requiring a warrant.

Both the Fourth Amendment and Art. I Sec. 17 protect people's interest in privacy. A person challenging a search has the burden of showing that he or she had a legitimate expectation of privacy in the item or place searched. *Rawlings v. Kentucky,* 448 U.S. 98 (1980); *State v. Cowen,* 104 Idaho 649, 651, 662 P.2d 230, 232 (1983). That involves a two-part inquiry: (1) Did the person have a subjective expectation of privacy in the object of the challenged search? and (2) Is society willing to recognize that expectation as reasonable? *California v. Ciraolo,* 476 U.S. 207, 211, (1986); *State v. Donato,* 135 Idaho 469, 473 (2001).

Here, at stake is data collected by Apple Inc. through Apple accounts and/or iCloud accounts associated with Mr. Kohberger. The records the State sought included[4]:

1. All records or other information regarding the identification of the account to include identifying information about the account owner;
2. Information regarding the devices associated with or used in connection with the account;
3. The contents of all emails associated with the account including stored or preserved copies of emails sent to and from the account;
4. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages;

[4] Exhibit D, Affidavit for Search Warrant, pp. 1-2.

5. The contents of all files and other records stored on iCloud, including all iOS device backups;
6. All activity, connection and transactional logs for the account;
7. All records and information regarding locations where the account or devises associated with the account were accessed;
8. All records pertaining to the types of service used;
9. All files, keys, or other information necessary to decrypt and data produced in an encrypted form.

The Fourth Amendment has generally refused to acknowledge a privacy interest in records held by a corporation about communications they facilitate. *See generally Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). *See also*, *Johnson v. Duxbury, Massachusetts*, 931 F.3d 102, 107 (1st Cir.2019) (compiling cases and concluding, "[e]very circuit to have considered the question has held that an individual has no reasonable expectation of privacy in a phone service provider's records of the phone number he has dialed or from which he has received calls.").

However, in *Carpenter v. U.S.*, 585 U.S. 296, 310-12 (2018), the Supreme Court declined to extend the third party doctrine to historical cell-site records and cell site location information (CSLI).

In this matter, Cpl. Payne specified in his request that the purpose for gathering the information from Apple Inc. was a belief that the Apple accounts would provide "information concerning Kohberger's plans, thought process, research, locations, photos or other pertinent information stored on his Apple account, including his iCloud account." Pursuant to *Carpenter*, to the extent that information gathered included information from an Apple account created in 2016 and an iPad purchased in 2018. Such information included device backups, private emails,

documents, photos, and videos that pre-dated the applicable time frame that Mr. Kohberger was in the Moscow-Pullman area. Mr. Kohberger has a privacy right protected by both the Fourth Amendment and Art. I Sec. 17. This was in essence a cell phone search.

In the wake of *Carpenter* and the Court's recognition of the abundant records maintained on everyone in modern society, it is questionable whether the third party doctrine is still good law. However, this Court need not consider whether the Fourth Amendment needs updating, because Idaho has already recognized an expectation in the privacy of whom we dial and the content of text messages we send. *See*, *State v. Thompson*, 114 Idaho 746, 749 (1988); *State v. Branigh*, 155 Idaho 404, 411 (Ct.App.2013).

Therefore, to collect the records law enforcement requested from Apple, it had to have a valid warrant and that valid warrant could not rely on a records produce by a federal grand jury subpoena or a search warrant that recklessly and intentionally omitted material facts.

This case is not about bank records, but about data collected by a third party (Apple) from devices associated with Mr. Kohberger's Apple Accounts, which backup or duplicate his internet connected devices, including cellphone data. From the standpoint of the Fourth Amendment, the data Apple collects can provide a massive amount of information about a person's private life. In his affidavit supporting the issuance of the search warrant, Cpl. Payne acknowledged that Apple products often require the creation of an Apple account to use their products. Further, Cpl. Payne noted that[5]:

- Apple accounts provide access to email, iMessage, Facetime, game center and location services among others.
- Apple captures information associated with the creation and use of an Apple ID including basic personal information such as the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple.
- Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including

[5] Exhibit D, Affidavit for search warrant, pp. 23-26.

whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

- Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website.
- Apple also maintains information about the devices associated with an Apple ID.
- Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number.
- Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with use of iCloud connected services, including: email ; images and videos; documents, spreadsheets, presentations, and other files; and web browser settings and Wi-Fi network.
- iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data.
- iCloud Backup allows users to create a backup of their device data. Productivity apps enable iCloud to be used to create, store, and share documents, spreadsheets, and presentations.
- iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

See also Matt Burgess, *All the Data Apple Collects About You—and How to Limit It*, WIRED (Jan. 16, 2023) (available at https://www.wired.com/story/apple-privacy-data-collection). Given the sheer amount of information Apple retains, the Fourth Amendment as understood in *Carpenter* requires a warrant before the government can access such information.

And as for Idaho, there can be no doubt that Art. I Sec. 17 requires a warrant before law enforcement can access Idahoan's online records. Apple Inc. is heavily regulated[6] and guarantees its customers' privacy. *See*, Apple Privacy Policy, https://www.apple.com/legal/privacy/en-ww/ (last updated Sept. 18, 2024).

[6] Apple is subject to the provisions of the federal Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523. The ECPA governs how Apple can disclose customer data.

To the extent that this court might see this as a third party doctrine issue, the arguments made in Mr. Kohberger's memorandum in support of suppressing Amazon records fully argue that doctrine and are incorporated here. Idaho's constitutional exclusionary rule, protects privacy. *See State v. Guzman*, 122 Idaho 981, 992 (1992).

For these reasons, this Court should find a warrant is required to access such information. The FBI's subpoena gathering the information from Mr. Kohberger's account violated his rights, and its results must be suppressed.

II. The Affidavit Submitted in Support of the Application for the Issued Search Warrant Recklessly or Intentionally Omitted Material Information, relies on information gained in violation of the constitution, and fails to provide probable cause for the requested search.

"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.

a. The Affidavit Submitted in Support of the Application for the Issued Warrant 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).

b. 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. 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 in his driveway, in a gated community, where an garbage collection ordinance applies. Because the IGG analysis is the origin of this matter, everything in the affidavit should be excised.

c. 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 in the *Franks* motion and other motions to suppress.

III. The Search Warrants Fail to Command Law Enforcement to Search the Apple Accounts or Contents of the iCloud.

The warrant in this matter fails to actually provide a command to search for a particular Apple account or the contents of the iCloud. It orders seizure and it has no time frame. The dates

in Cpl. Payne's affidavit never made it into the warrant and the affidavit was not incorporated into the warrant. Instead the warrant said generally:

(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 Apple account of…"

(3) the command is made to search the premises for the property and seize it. The premises is One Apple Park Way, Cupertino, CA

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

(5) there is no timeframe, it is "all" for every paragraph (a-i)

(6) paragraphs a-i have much broader and extensive language than the 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 referenced 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 to Search.

The United States Supreme Court "when confronting new concerns wrought by digital technology, … has been careful not to critically extend existing precedents." *United States v. Wilson* 13 F.4th 961 (9th Cir. 2021) citing *Capenter*, 138 S.Ct. at 2222. A warrant is not a magical wand that grants access to anything an Apple 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 form that which is to

just 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 data compilation requested in the Apple warrant is too broad in that it makes no attempt at narrowing and results instead in a blanket request for everything available in two Apple accounts with iCloud, 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" without any temporal restrictions.

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 S.Ct. 2022, 2038, 29 L.Ed.2d 564 (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 or in this case iCloud backup of 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 Apple accounts. Law enforcement was certainly capable of greater specificity, but instead gave itself an overbroad mandate permitting it complete access to everything from Mr. Kohberger's Apple accounts.

Another example of a court cracking down on overbroad digital warrants it *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. This includes a time frame. 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.

CONCLUSION

Mr. Kohberger requests this Court suppress all evidence obtained by police via the subpoenas and warrants that permitted them to search his Apple and iCloud accounts. As explained above, this search warrant affidavit contained information related to the illegal search of law enforcement on data produce pursuant to a subpoena. The Search Warrant itself orders seizer, not search and is overbroad. The probable cause as written, omitted exculpatory information and information that put into question the reliability of the facts upon which it relies, and finally because the affidavit relied on evidence gained in violation of the constitution, all in violation of the Fourth Amendment and Art. I Sec. 17.

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 E

Motion to Suppress and Memo in Support RE: Apple

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