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,**<br><br>**Plaintiff,**<br><br>**V.**<br><br>**BRYAN C. KOHBERGER,**<br><br>**Defendant.** | **CASE NUMBER CR01-24-31665**<br><br>**MOTION TO SUPPRESS AND MEMORANDUM IN SUPPORT**<br><br>**RE: AT&T FIRST WARRANT** |

COMES NOW, Bryan C. Kohberger, by and through his attorneys of record, and hereby submits the following Memorandum in support of his contemporaneously filed Motion for an Order suppressing all data found by law enforcement from its search of his AT&T account.

## ISSUES

**I. Mr. Kohberger has a privacy interest in his AT&T account information protected by Art. I Sec. 17 of the Idaho Constitution and by the Fourth Amendment.**

**II. The Affidavit Submitted in Support of the Application for the Issued Search Warrant Recklessly or Intentionally Omitted Material Information and fails to provide probable cause for the requested search.**

**III. The Search Warrant fails to provide specific particularization of what law enforcement could search and seize in Mr. Kohberger's AT&T account.**

**IV. The Affidavit Submitted in Support of the Application for the Issued Search Warrant Included Information that Must be Excised.**

**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.**

## FACTS

On December 23, 2023, Cpl. Payne of the Moscow Police Department requested a warrant to search the contents Mr. Kohberger's AT&T account for information regarding his phone's whereabouts between November 12, 2023 and November 14, 2023, as well as messages and phone calls during that period.

The affidavit for the warrant was signed by Cpl. Payne.

The basic facts Cpl. Payne used to support the search are discussed in a separate motion for *Franks* hearing pursuant to *Franks v. Delaware* 438 US 154, (1978) and are incorporated but not repeated here.

The affidavit requested:

1. All customer/subscriber information, including any listed addresses, other listed telephone number(s), social security number(s), dates of birth, name(s), address(es), any other customer identifying information, mobile handset or device identifiers/serial numbers (MEID, ESN, IMSI, IMEI, SUPI), activation date and deactivation date, and point of purchase or location device was purchased if applicable;

2. Device Purchase Information. This is specifically to include the Date, Time and Location of where the device or any pre-paid refill cards were purchased as well as any information maintained about the purchase to include store name, store number, terminal number, and amount of purchase;

3. Any email addresses associated with the account or with the device that is currently on file and stored in the normal course of business of the Service Provider;

4. Call detail records, including detailed information in reference to all known outgoing and incoming calls associated with the account, dates and times calls were made, and duration of all calls made or received. This is to include any other pertinent call detail records including special features codes, or any other codes that are maintained in the normal course of business for the Service Provider, of any ce1lular numbers identified in the course of the investigation. In addition to voice calls, this would also include any detail records showing text messages, MMS messages, or data activity;

    a. In the event the requested Call Detail Records contain other Service Provider customer numbers, identified as either incoming or outgoing calls, the Service Provider will provide subscriber information to the specific numbers identified, if requested.

5. Cell site information, to include all known cell towers associated with outgoing and incoming calls (Call Detail Records). This information is to include any sector information, azimuth for each identified sector, cell site location, handoff tower and sector, time on tower information, and any other related material that would be necessary to identify the location and sector in reference to the cell site information associated with the call detail records. In the event text messages, MMS messages, Data activity, including IP sessions and destination addresses that were produced, these records are also included in this request;

6. Cell site locations for all Service Provider Cell Sites, sector information, including azimuth headings, in the regional market associated with the requested cell site information;

7. Location information, to include any estimated or known longitude and latitude of the cellular device's current location, or approximate location, information

received by cell tower(s) in reference to direction and distance from the tower a device may be located (timing and triangulation information). Radio Frequency signal strengths, direction, and transmission information. The geographical constraints of location information will be limited to the United States;

8. Location information can be in the form of historical records. This would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, estimated margin of error, direction and distance from the tower, and other location related information commonly referred to as Real Time Tool (RTT), Timing Advance Information, Location Database of Record (LocDBoR). This further includes any other report similar in nature that would provide an estimate of the cellular phone on the Service Provider's network;

9. All text message and/or MMS messages, including message content, currently stored in the normal course of business for the Service Provider, to include any cloud services which allow for the long-term storage of both voicemails and SMSIMMS messages;

10. Cloud Data, any content that may have been backed up to Cloud Storage for the listed dates/times. If said Cloud Storage has been provided by a third-party provider, please provide relevant contact information for that provider;

In the Exhibit attached to the warrant, however, law enforcement indicates only wanting "historical phone records between the hours of November 12, 2022[,] at 12:00 a.m. and November 14, 2022[,] at 12:00 a.m." and well as "prospective phone records".

## ARGUMENT

### I. Mr. Kohberger has a privacy interest in his AT&T account information protected by Art. I Sec. 17 of the Idaho Constitution and by the Fourth Amendment.

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, 104, 100 S.Ct. 2556, 65 L.Ed.2d 633, 641 (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, 106 S.Ct. 1809, 1811–12, 90 L.Ed.2d 210, 215–16 (1986); *State v. Donato,* 135 Idaho 469, 473, 20 P.3d 5, 9 (2001).

Here, at stake are records of a telephone account. The records the State sought included:

1. Identifying information about account owner and their devices;

2. Device purchase information;

3. Email addresses associated with the account;

4. Call detail records including text messages and data activity;

5. Cell site information;

6. Historical location information;

7. Cloud data.

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 the AT&T records was to "aid in determining the location of the 8458 phone and the white Elantra in efforts to determine whether the white Elantra is the same vehicle identified" in the surveillance videos. Pursuant to *Carpenter*, to the extent that information was

being gather for the movements of the vehicle, Mr. Kohberger has a privacy right protected by both the Fourth Amendment and Art. I Sec. 17.

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 in this matter, it had to have a valid warrant.

## II. 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.

The challenge pursuant to this section of the motion is separately laid out in Mr. Kohberger's motion for hearing *under Franks*. The motion and proffer are incorporated but not repeated herein.

## III. The Search Warrant fails to provide specific particularization of what law enforcement could search and seize in Mr. Kohberger's AT&T account.

The Fourth Amendment and Article I § 17 of the Idaho Constitution do not permit a cell phone to be searched incident to arrest. *Riley v. California*, 573 U.S. 373 (2014). Rather, the police must seek a warrant. *Id*. A warrant, however, is not a magical wand that grants access to anything a cell phone contains. As the Supreme Court found, cell phones can contain enormous amounts of information that is private and may not be viewed by the government. *Riley*, 573 U.S. at 403. 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).

The warrant for the Mr. Kohberger's AT&T account lacks appropriate particularization. It lists all the following that could be found in the account:

- All identifying information of the account holder;
- All information about the creation of the account;
- All information about the accounts maintenance;
- All call records;
- All text messages, MMS messages, or "data activity";

- The devices historical and prospective locations;
- Any data now in the Cloud.

The warrant and the affidavit are not only all encompassing, they are duplicative, often repeating things to be searched and seized. The only limitation in scope is that the property be related to the homicides in this matter.

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, 84 (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. 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*, 573 U.S. at 393.

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 first thing to be seized was "[d]ata complication relating to or containing information indicating, suggesting, or related to violence, a fight, or motive/hostility for any of the same…", but then it permits the entire contents, i.e., every category of data, on the cellphone to be searched. The limiting description of the data is not repeated in the remaining eight requests to search *categories* of data. Therefore, in the case at bar, law enforcement was certainly capable of greater specificity in both instances, but instead gave itself an overbroad mandate permitting it complete access to everything from Mr. Kohberger's phone.

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). On this basis, the court found the warrant was overbroad for lacking any temporal limitation. *Id. See, also United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017), *cert. denied*, 138 S.Ct. 1580, 200 L.Ed.2d 767 (2018); *United States v. Lazar,* 604 F.3d 230, 238 (6th Cir. 2010), cert. denied, 562 U.S. 1140, 131 S.Ct. 973, 178 L.Ed.2d 757 (2011); *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995); *see also, e.g., In re 650 Fifth Avenue and Related Properties*, 830 F.3d 66, 100 (2d Cir.

2016); *United States v. Otero*, 563 F.3d 1127, 1133 (10th Cir.), cert. denied, 558 U.S. 924, 130 S.Ct. 330, 175 L.Ed.2d 218 (2009); *Buckham v. State*, 185 A.3d 1, 19 (Del. 2018); *Burns v. United States*, 235 A.3d 758, 774 (D.C. 2020); *People v. Thompson*, 178 App.Div.3d 457, 458, 116 N.Y.S.3d 2 (1st Dept. 2019); *People v. Melamed,* 178 App.Div.3d 1079, 1081, 116 N.Y.S.3d 659 (2d Dept. 2019); *In re Search Warrant*, 193 Vt. 51, 89, 71 A.3d 1158, cert. denied, 569 U.S. 994, 133 S.Ct. 2391, 185 L.Ed.2d 1104 (2013); *see also, e.g., Commonwealth v. Holley*, 478 Mass. 508, 525, 87 N.E.3d 77 (2017); *State v. Short,* 310 Neb. 81, 139, 964 N.W.2d 272 (2021); *State v. Castagnola*, 46 N.E.3d 638, 659 (Ohio 2015); *State v. Mansor*, 363 Or. 185, 218, 421 P.3d 323 (2018). The court went on in *dicta* to note the various other inconsistencies with that the government knew it was looking for and its overbroad demand. *Id.* at 306-07.

The *Wheeler* case is important to this case not simply for the concept of a temporal limitation on the information to be sought, but 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 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, but it did not. The court in *Wheeler* condemns government attempts to cast too broad a net under these circumstances.

Recently, in Georgia, their Supreme Court determined that a warrant for digital contents of a cellphone that permits the police to seize every bit of data is unconstitutionally lacking in particularization in a murder case like the one at bar. *State v. Wilson*, 884 S.E.2d 298, 300-01 (Ga. 2023). In that case, the court upheld the suppression of the fruits of a warrant where:

> The magistrate [ ] issued a warrant that authorized a forensic search of Wilson's cell phones "to be completed in order to obtain any and all stored electronic information, including but not limited to; user account information, stored phone information, images, text messages, videos, documents, e-mails, internet activity, call logs, contact information, phonebook, or any deleted data." The warrant further included preprinted form language stating that "[t]he foregoing described property, items, articles, instruments, and person(s) to be searched for and seized constitute evidence connected with the foregoing listed crime(s) and is/are: (check ALL that are applicable) (OCGA § 17-5-21)3." The swearing officer then checked four boxes on the preprinted form, indicating that investigators believed the cell phones were: "intended for use in the commission of the crime(s) herein described;" "used in the commission of the crime(s) herein described;" "tangible, corporeal or visible evidence of the commission of the crime(s) set forth above;" and "intangible, incorporeal or invisible evidence of the commission of the crime(s) set forth above."
>
> 3 This Code section does not reference criminal activity. Instead, it lists the process by which law enforcement officers must abide when seeking a warrant.

*Id.* at 613-14 (footnotes omitted). The government acknowledged the breadth of the warrant, but claimed it was particularized. *Id.* at 300. The court disagreed, finding there was nothing limiting about the language in the warrant:

> As the State acknowledges, the search warrant broadly authorizes the seizure of "any and all stored electronic information" on the phones, "including but not limited to" various kinds of electronic information. The State points to the preprinted form language following this sweeping authorization as "limiting" in nature. However, that language clearly states that "[t]he foregoing described property"—that is, "any and all stored electronic information" on the phones—"constitutes evidence connected with the crimes." This language cannot plausibly be read, as the State suggests, to limit the otherwise limitless authorization to search for and seize any and all data that can be found on Wilson's cell phones.

*Id.* at 300-01. The Georgia Supreme Court went on to note that it would likely have upheld the warrant had it merely limited the search to digital evidence pertaining to the commission of the murder. *Id.* at 301.

More noteworthy than finding a warrant that failed to limit what sort of evidence was to be seized was overbroad was the concurrence by Justice Peterson, which five other justices joined (Georgia's Supreme Court has nine justices). Justice Peterson found:

> [t]he Supreme Court in *Andresen* [*v. Maryland*, 427 U.S. 463 (1976)] held only that an otherwise particularized warrant was not made unconstitutionally general by the presence of residual language — instead*, the residual clause* had to be read in the light of the language before it. 427 U.S. at 480-482, 96 S.Ct. 2737. But the inverse does not follow; the logic of *Andresen* does not support the idea that an otherwise general warrant, lacking particularity in the places to be searched or things to be seized, can be saved by this sort of boilerplate language.[5] Taking the warrants in this case as an example, a warrant that fails to give any parameters "for a forensic examination" of cell phones is not narrowed by the empty assurance that the search will only be looking for evidence of a particular crime. Perhaps such a warrant may once have been sufficient, when cell phones had a fraction of the functionality and storage capacity that they do now. But today, a caveat that the search is limited to evidence of a particular crime might narrow the *object* of the search, but it gives little or no clarity to an officer as to where to look, for what to look, or how to look for it. See *Hourin* [*v. State*], 301 Ga. [835,] 844 (3), 804 S.E.2d 388 [2017].
>
> 5 This misstep may have stemmed from a slight ambiguity in the wording of *Reaves*. We held that "[t]he residual clauses in the search warrants at issue in this case limit the items which may be seized to evidence of cruelty to children and ... murder." 284 Ga. [181,] 185 (2) (d), 664 S.E.2d [211] 215 [(2008)]. In context, that meant that the residual clauses *themselves* were limited to evidence of those crimes. See id. But it's easy enough to see how one might mistakenly read this language — specifically the direct object, "items" — to mean the *list* of items *preceding* the residual clauses. And indeed, that seems to be what we've done in recent years.

*Id*. at 303 (PETERSON, J. concurring).

The concurrence in *Wilson* is worth noting in this case because the "residual clause" in this warrant, if it exists at all, comes in the opening paragraph. But as the concurrence notes, this "residual clause" does not truly do much to keep the warrant from becoming a general warrant. If anything, it merely shows how much more particular the warrant could have been had it been done correctly.

Most recently, in *People v. Carson*, 2024 WL 647964, at *8 (Mich.Ct.App. 2024), the court found a warrant lacked particularization where the warrant:

> was a general warrant that gave the police license to search *everything* on defendant's cell phone in the hopes of finding anything, but nothing in particular, that could help with the investigation. This warrant did not place any limitations on the permissible scope of the search of defendant's phone. The only hint of

> specificity was the opening reference to "the investigation of Larceny in a Building and Safe Breaking," but this small guardrail was negated by the ensuing instruction to search for such items by searching and seizing the entirety of the phone's contents.

The court went on to find that to avoid being overly broad, in this case, police could have said they expected to find communications between the defendant and a co-defendant, and therefore look at SMS messages and other messaging applications. *Id.* The Court found, "many states have joined in our conclusion that that the particularity requirement disallows the issuance of warrants authorizing police to search the entirety of a person's cell phone contents for evidence of a particular crime; the massive scale of the personal information people store on their mobile devices means that there must be some limits to the scope of the search." *Id.* at *9 (*citing Richardson v State*, 481 Md. 423, 468, 282 A.3d 98 (Md. Ct. App. 2022); *Wilson*, *supra*).

To conclude: the warrant issued for Mr. Kohberger's AT&T account was unconstitutionally overbroad. Law enforcement had the ability to be more specific both as to the content and the category of the data 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 AT&T account must be suppressed.

## IV. The Affidavit Submitted in Support of the Application for the Issued Search 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).

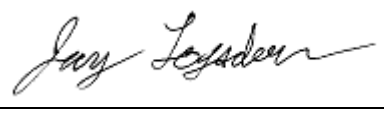
### a. All information in the affidavit was gathered because of law enforcement's unconstitutional use of Investigative Genetic Genealogy, and thus nothing in the warrant should remain.

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 has argued 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 previously argued. 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 out front. Because the IGG analysis is the origin of this matter, everything in the affidavit should be excised.

**CONCLUSION**

Mr. Kohberger requests this Court suppress all evidence obtained by police via the warrant for his AT&T phone records. As explained above, this warrant 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, and because the warrant omitted exculpatory information and information that put into question the reliability of the facts upon which it relies, and finally because the affidavit and warrant do not specify what data could be searched and seized, all in violation of the Fourth Amendment and Art. I Sec. 17.

DATED this ___13___ day of November, 2024.



JAY WESTON LOGSDON
FIRST DISTRICT PUBLIC DEFENDER

ANNE C. TAYLOR
ANNE TAYLOR LAW, PLLC

**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