

FEB 19 2025

IN THE DISTRICT COURT OF THE FOURTH JUDICIAL DISTRICT OF

TRENT TRIPPLE, Clerk
By ANNA MEYER
DEPUTY

THE STATE OF IDAHO, IN AND FOR THE COUNTY OF ADA

STATE OF IDAHO,

Plaintiff,

v.

BRYAN C. KOHBERGER,

Defendant.

Ada County Case No. CR01-24-31665

**ORDER ON DEFENDANT’S MOTIONS
TO SUPPRESS RE: AT&T, GOOGLE,
USB, APPLE AND AMAZON**

I. INTRODUCTION

Defendant is charged with one count of Burglary and four counts of Murder in the First Degree in connection with the stabbing deaths of four University of Idaho students in the early morning hours of November 13, 2022. As part of law enforcement’s investigation, the Federal Bureau of Investigation (FBI) issued federal grand jury subpoenas to Apple, Inc. and Amazon, Inc. to obtain information from accounts linked to Defendant. The FBI provided responsive information to detectives from the Moscow Police Department, who requested and received search warrants for the Apple and Amazon accounts. In addition, detectives sought and obtained search warrants for Defendant’s Google accounts, a USB drive containing Defendant’s cell phone data and for information held by Defendant’s cellular carrier, AT&T.

Before the Court are Defendant’s motions to suppress the information obtained through the subpoenas and the AT&T, Google, Apple and USB search warrants. Defendant argues the FBI’s issuance of the subpoenas constituted a warrantless search that violated his privacy interests under both the Fourth Amendment and Article I, § 17 of the Idaho Constitution. He further argues that the search warrants fail to command a search and/or lack particularity.¹

¹ Defendant also argued that the AT&T, Apple, Amazon, USB and Google search warrants were invalid under *Franks v. Delaware*, 438 U.S. 154 (1978) due to claims of recklessly or intentionally false or omitted material information and/or because they were based on law enforcement’s allegedly unconstitutional use of Investigative Genetic Genealogy (IGG). On these arguments, Defendant incorporated by reference his arguments in his Motion for a *Franks* Hearing and his Motion to Suppress re: Genetic Information. The Court incorporates herein its rulings denying both motions. Consequently, this Order only addresses the arguments still at issue.

The State responds that Defendant relinquished any privacy interest he had in the Amazon and Apple materials and, further, contends the remaining warrants are proper and sufficiently particular.

A suppression hearing on the portion of Defendant's motions at issue in this Order² was held on January 24, 2025, during which the Court received testimony from Detective Corporal Brett Payne and Detective Lawrence Mowery, both from the Moscow Police Department. The Court found both detectives to be credible and reliable. Following argument, the Court took the matter under advisement. The Court finds suppression is not warranted because: 1) Defendant relinquished any privacy interest he had in the records subpoenaed from Amazon and Apple pursuant to the third-party doctrine, and; 2) the remaining search warrants are valid.

II. STANDARD

The standard of review of a motion to suppress is bifurcated. The power to assess the credibility of witnesses, resolve factual conflicts, weigh evidence, and draw factual inferences is vested in the trial court. *State v. Valdez-Molina*, 127 Idaho 102, 106, 897 P.2d 993, 997 (1995). A trial court's ruling on a motion to suppress evidence combines the issue of law and fact, and the trial court's factual findings will not be overturned unless they are clearly erroneous. *State v. Conant*, 143 Idaho 797, 799, 153 P.3d 477, 479 (2007). When a decision on a motion to suppress is challenged, the application of constitutional principles to the facts found will be freely reviewed. *State v. Veneroso*, 138 Idaho 925, 928, 71 P.3d 1072, 1075 (2003).

² Evidence and argument on the *Franks* motion and IGG motion were heard on January 23, 2025. The balance of motions to suppress was taken up the following day.

III. FINDINGS OF FACT³

On November 13, 2022, an officer from the Moscow Police Department responded to a residence located at 1122 King Road in Moscow, Idaho where he discovered the bodies of Madison Mogen, Kaylee Goncalves, Ethan Chapin, and Xana Kernodle. Each appeared to have been stabbed to death. The investigation that ensued was a multi-agency affair involving members of the Moscow Police Department, the Idaho State Police and the FBI, among others.

For purposes of the investigation, a command team consisting of several investigators from each of these agencies was set up at the Moscow Police headquarters. The command team included, among others, Detective Brett Payne and Detective Lawrence Mowery of the Moscow Police Department, as well as Special Agent Nicholas Ballance of the FBI, all of whom were co-located on the second floor of the Moscow Police Department. The command team met twice daily for several weeks to review, analyze, and organize the information gathered in the investigation. Pertinent information was transmitted into a working probable cause affidavit that could be—and was—incorporated by law enforcement into their various search warrant affidavits. All investigators had access to the search warrant affidavits issued during the investigation.

³ The Court’s findings are based on suppression hearing testimony provided by Detectives Payne and Mowery as well as the following documentary evidence: For First AT&T Warrant: Defendant’s Exhibit A attached to Reply to State’s Objection to Defendant’s Motion to Suppress and Memorandum in Support Re: AT&T First Warrant (Dec. 19, 2024) (admitted as Exhibit S-2.1 at suppression hearing) and State’s Exhibits S1 and S2 attached to its Objection to Defendant’s Motion to Suppress and Memorandum in Support Re: AT&T First Warrant (Dec. 6, 2024) (“First AT&T Objection”); For AT&T Pen Trap and Trace Warrant: Defendant’s Exhibits A through C attached to Reply to State’s Objection to Defendant’s Motion to Suppress and Memorandum in Support Re: Pen Trap and Trace Device (Dec. 19, 2024) (“Pen Trap Reply”) (Exhibits A and C were admitted as Exhibits S-2.2 and S-2.3, respectively, at suppression hearing) and State’s Exhibits S-1 and S-2 attached to its Objection to Defendant’s Motion to Suppress and Memorandum in Support Re: Pen Trap and Trace Device (Dec. 6, 2024) (“Pen Trap Objection”); For Apple subpoena and warrant: Defendant’s Exhibits A through E in support of his Motion to Suppress re: Apple Account Federal Grand Jury Subpoena and Search Warrant Dated August 1, 2023 (Nov. 18, 2024) (“Apple Motion”) and the State’s Exhibits S-1 through S-4 attached to its Objection to Defendant’s Motion to Suppress re: Apple (Dec. 6, 2024) (“Apple Objection”); For Amazon subpoena and warrant: Defendant’s Exhibit A in support of his Motion to Suppress re: Amazon Account Federal Grand Jury Subpoena and Search Warrants Dated April 26, 2023 and May 8, 2023 (Nov. 18, 2024) (“Amazon Motion”) and the State’s Exhibits S-1 through S-4 attached to its Objection to Defendant’s Motion to Suppress re: Amazon (Dec. 6, 2024) (“Amazon Objection”); For Google warrants: Defendant’s Exhibits A through F in support of his Motion to Suppress re: Google Warrants Dated 1/3/23, 1/24/23, and 2/24/23 (Nov. 18, 2024) (“Google Motion”), and; For USB warrant: Defendant’s Exhibit A in support of his Motion to Suppress re: Moscow Police Forensic Lab Warrant Dated January 9, 2023 (Nov. 18, 2024) (“USB Motion”).

Among the initial search warrants sought in the investigation were two to AT&T, the cellular carrier for a phone number that law enforcement had linked to Defendant. Detective Payne applied for and received both warrants on December 23, 2022. As Detective Payne was not an expert in cell phone data, he relied “heavily” upon Agent Ballance, who is a member of the FBI’s Cellular Analysis Survey Team (“CAST”) and specializes in cell records analysis. Agent Balance aided Detective Payne in both drafting the search warrant affidavits for the AT&T warrants and analyzing the returned information.

Within a week of obtaining the AT&T warrants, law enforcement obtained a warrant for Defendant’s arrest. The arrest was effectuated on December 30, 2022 at his parents’ home in Pennsylvania. At that time, law enforcement seized Defendant’s cell phone pursuant to a search warrant for the home. To preserve the phone’s data, the FBI copied the contents of the cell phone onto a USB drive, but did not review the contents. Law enforcement also had a warrant to search Defendant’s vehicle, which was located in the garage of his parents’ home. During the search of the vehicle, a receipt for an Apple iPad was found.

Following Defendant’s arrest, the FBI obtained and served two federal grand jury subpoenas: one to Apple, Inc. and one to Amazon, Inc. In addition, Detectives Payne and/or Mowery obtained search warrants for records from Google, Inc., Apple, Inc., Amazon, Inc. and for the contents of the USB drive.

A. First AT&T Warrant

The first AT&T warrant Detective Payne applied for sought nine categories of records associated with Defendant’s cell phone: 1) customer/subscriber information; 2) device purchase information; 3) associated email addresses; 4) call detail records; 5) cell site information; 6) cell site locations; 7) location information for the cell phone; 8) text and MMS messages, and; 9) Cloud data. *See*, Exh. S-1 to First AT&T Objection. Each of these categories was narrowed by a detailed description of the specific information sought. The information requested was temporally limited to a 48-hour period: November 12, 2022 at 12:00 a.m. PST through November 14, 2022 at 12:00 a.m. PST.

In his accompanying search warrant affidavit, Detective Payne set forth in detail the circumstances of the crime and the scope and results of the investigation as of that date, including evidence linking Defendant to the suspect vehicle seen on surveillance videos around the time of the murders. *Id.* Detective Payne indicated how each of the categories of information

sought would aid the investigation, including in determining whether the phone's activity was consistent with the suspect vehicle's route of travel as seen on the surveillance videos, whether the phone was in the vicinity of the murders during or prior to its occurrence as part of planning the crime, and why Defendant's phone was not reporting to the network during the estimated time the crime occurred.⁴ *Id.*

Based on Detective Payne's search warrant affidavit, the magistrate issued a search warrant for the records sought therein. The warrant stated, in relevant part:

Brett Payne, having given me proof, upon oath, this day showing probable cause establishing grounds for issuing a search warrant and probable cause to believe property consists of certain evidence regarding the investigation into the crime(s) of homicide at 1122 King Road in Moscow, Idaho is on the AT&T account associated with the phone number 509-592-8458 between November 12, 2022 at 12:00 a.m. PST to November 14, 2022 at 12:00 a.m. PST.

See, Exh. S-2 to First AT&T Objection ("First AT&T Warrant").

The warrant then set forth each of the categories of information defined by Detective Payne in his search warrant affidavit. It was served by Detective Mowery upon AT&T via email. *See*, Exh. S-2.1. As was Detective Mowery's practice, he did not include Detective Payne's search warrant affidavit with the warrant when serving it. AT&T emailed a return of the requested information back to Detective Mowery later that day. *Id.* The returned information was immediately turned over to Agent Ballance for review and analysis. In reviewing the information, Agent Ballance had access to and knowledge of Detective Payne's search warrant affidavit supporting the First AT&T Warrant.

B. AT&T Pen Trap and Trace Warrant

Within hours of receiving the return on the First AT&T Warrant, Detective Payne applied for a second warrant to AT&T, this time to obtain records associated with Defendant's cell phone number for the prior six months, as well as for the installation of a pen register and trap and trace device⁵ for the number. *See*, State's Exh. S-1 to Pen Trap Objection. The records sought were call detail records with cell sites for all voice, sms and data connections. These

⁴ An earlier search warrant had revealed that Defendant's cell phone did not appear to be reporting to the network for the hour before and hour after the homicides occurred.

⁵ Pen registers capture the outgoing phone numbers, email addresses and other dialing or routing information transmitted by a cell phone. Trap and trace devices capture similar information that is received by the cell phone (incoming).

records were further defined to include subscriber account information, device identifying information, usage and location information to include cell site positions information, addresses of cell towers used by the device and subscriber identity information for customers who contact or are contacted by the device. *Id.*

Again, Detective Payne's search warrant affidavit set forth in great detail the circumstances of the crime and the scope and results of the investigation as of that date, including an analysis of the data received from the First AT&T Warrant. This information, according to Detective Payne, showed that the estimated locations for Defendant's cell phone during the 48 hours before and after the homicides were consistent with the movement of the suspect vehicle seen in the various surveillance videos. He stated:

Based on my training and experience, and the facts of the investigation thus far, I believe that Kohberger, the user of the 8458 Phone, was likely the driver of the white Elantra that is observed departing Pullman, WA and that this vehicle is likely Suspect Vehicle 1. Additionally, the route of travel of the 8458 Phone during the early morning hours of November 13, 2022 and the lack of the 8458 Phone reporting to AT&T between 2:47 a.m. and 4:48 a.m. is consistent with Kohberger attempting to conceal his location during the quadruple homicide that occurred at the King Road Residence. As a result, I am seeking historical CSLI from June 23, 2022 to current, prospective location information, and a Pen Register/Trap and Trace on the 8458 Phone to aid in efforts to determine if Kohberger stalked any of the victims in this case prior to the offense, conducted surveillance on the King Road Residence, is in contact with any of the victim's associates before or after the alleged offense, any locations that may contain evidence of the murders that occurred on November 13, 2022, the location of the white Elantra registered to Kohberger, as well as the location of Kohberger.

Id.

A search warrant for the information requested by Detective Payne was issued by the magistrate later that same day. The warrant stated, in relevant part:

Brett Payne, having given me proof, upon oath, this day showing probable cause establishing grounds for issuing a search warrant and probable cause to believe there are records related to the crime(s) of homicide at 1122 King Road in Moscow, Idaho and are currently under the control of AT&T for historic call detail records for the telephone number 509-592-8458 with cell sites for all voice, sms, and data connections between June 23, 2022, to present[.]

See, State's Exh. S-2 to Pen Trap Objection ("Pen Trap Warrant").

The warrant then set forth each of the categories of data outlined by Detective Payne in his search warrant affidavit. In addition, the warrant authorized investigators to install and use a pen register, trap and trace device and cell site simulator in accordance with I.C. § 18-6719, *et seq.*

Once issued, Detective Payne sent the Pen Trap Warrant to the FBI for service since the FBI hosted the pen register portion of the warrant. *See*, Exh. S2.2. Agent Ballance then served the warrant on AT&T on behalf of the Moscow Police Department. *See*, Def's Exh. B to Pen Trap Reply. Detective Payne's search warrant affidavit supporting the Pen Trap Warrant was not served with the warrant; however, the return was provided to Agent Ballance, who had access to the search warrant affidavit in reviewing the return. *See*, Exh. S-2.3.

C. Google Warrants

Detective Mowery applied for and was issued three different warrants to Google, Inc. between January 3, 2023 and February 24, 2023. Each of the three warrants began with the following language:

Lawrence Mowery, having given me proof, upon oath, this day showing probable cause establishing grounds for issuing a search warrant and there is probable cause to believe that the property referred to and sought in or upon said premises consists of information related to the investigations into the crime(s) of homicide at 1122 King Road, Moscow, Idaho on the Google account of Bryan C. Kohberger...

See, Def's Exh. A-C to Google Motion.

Each warrant requested information in connection with email accounts, phone numbers and International Mobile Equipment Identifier (IMEI) numbers that the investigation had revealed were associated with Defendant. The Google warrant issued January 3, 2023 ("Google Warrant One") requested "business records and subscriber information" in connection with bryanchristopher1994@gmail.com plus two phone numbers and an IMEI number. The Google warrant issued January 24, 2024 ("Google Warrant Two") requested "business records and subscriber information" in connection with yewsirneighm@gmail.com. The Google warrant issued February 24, 2023 ("Google Warrant Three") requested data in connection with "all Gmail accounts linked by recovery email, cookie, Android ID, Creation IP or phone number associated with" all of the accounts listed in Google Warrants One and Two, as well as for bk5781@desales.edu.

Each of the three warrants were temporally limited to January 1, 2021 through December 30, 2022. In addition, all three warrants listed the following sixteen specific items to seize:

- 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.

Id.

These warrants were each supported by search warrant affidavits executed by Detective Mowery. In these affidavits, Detective Mowery set forth a statement describing in detail the scope and results of the investigation to date, how the accounts and phone numbers identified in each warrant were discovered and how they were connected to Defendant. He also included a detailed explanation as to how Google works and why each of the sixteen items listed in the warrants could be relevant to the investigation.

Upon receiving each Google warrant, Detective Mowery served it on Google electronically through its law enforcement portal. As was his practice, Detective Mowery did not serve his search warrant affidavit in addition to each warrant. The returns for each Google warrant were submitted to law enforcement as a digital file available through Google's law

enforcement portal. Detective Payne downloaded each return upon receipt, after which he prepared a Receipt and Inventory of Warrant. Detective Mowery then reviewed the downloaded material to ensure it contained information for the correct accounts identified in the warrants before disseminating the returns to other investigators in the command team to process. Each member of the team had access to the search warrant affidavits supporting the respective warrant. Thus, in processing the returns on the three Google warrants, the reviewing investigator was able to refer to the particular search warrant affidavit.

D. USB Search Warrant

After the content of Defendant's cell phone was copied onto the USB drive—but not reviewed—by the FBI, the USB was sent to Detective Mowery, who stored it in the forensics lab at the Moscow Police Department. Detective Mowery then applied for a warrant to search the contents of the USB. In his search warrant affidavit, Detective Mowery set forth in detail the circumstances of the crime, the investigation to date and his probable cause to suspect Defendant's cell phone contained evidence of the homicides. *See*, Def's Exh. A to USB Motion. A warrant was issued that stated in pertinent part:

Lawrence Mowery, having given me proof, upon oath, this day showing probable cause establishing grounds for issuing a search warrant and probable cause to believe property consisting of a Seagate 2TB External USB Drive with Serial Number #NA87T1GN for evidence regarding the investigation into the crimes of homicide of Madison Mogen, Kaylee Goncalves, Xana Kernodle, and Ethan Chapin at 1122 King Road, Moscow, Idaho, including:

- Data Compilations relating to or containing information indicating, suggesting, or related to violence, a fight, or motive/hostility for any of the same, to include without limitation ledgers, papers, lists, books, notes, letters, calendars, diaries, tapes, photographs, audio, videos, or other media or similar documents or items, computer and communications devices capable of storing electronic data, other electronic storage devices and media, and access to contents of all of the above;
- Records of communications;
- Written/text communications including emails, SMS text messages, MMS messages, and other communications, including but not limited to, third-party applications such as Kik, Whatsapp, Facebook, Instagram;
- Contacts stored;
- Location information;

- Location information stored in any cloud account associated with the phone if [sic] said account credentials can be obtained from the forensic image of the phone;
- Internet history, bookmarks, and/or associated cloud accounts;
- Written and audio recorded notes or any cloud account associated with the device;
- Indicia of residency in, or ownership or possession of, the premises and any of the above items[.]

located in or upon the following described premises, located in Latah County, State of Idaho:

The Moscow Police Department is located as 155 Southview, in Moscow, Idaho. The Forensics Lab is located on the second floor of the Moscow Police Department.

YOU ARE THEREFORE COMMANDED TO SEARCH the above-described premises for the property described above, TO SEIZE it is found and bring it promptly before the Court above-named.

Id. at pp. 24-25 (“USB Warrant”).

The USB Warrant was served by Detective Mowery in person at the forensics lab. He then obtained the USB and prepared an inventory documenting his seizure of the USB and “Bryan Kohberger’s Phone data.” He submitted the return to the magistrate who, in a subsequent order, authorized the property to be “delivered to any person or laboratory or laboratories for the purpose of conducting or obtaining any tests, analysis, or identification of said property . . .” *Id.* at pp. 26-32. The data on the USB was subsequently processed by other investigators on the team, all of whom had access to Detective Mowery’s supporting search warrant affidavit.

E. Apple Subpoena and Search Warrant

The FBI served a federal grand jury subpoena upon Apple, Inc. on or about January 12, 2023.⁶ Apple responded on January 27, 2023 by providing subscriber information for two Apple accounts associated with Defendant: bkohberger@spartan.northhampton.edu, which Apple indicated was “Active”, and wifiarmyowns@yahoo.com, which Apple indicated was “Locked.” *See*, State’s Exh. S-4 to Apple Objection. Both accounts were created on October 7, 2016. The subscriber information provided by Apple also revealed the Active account had last been

⁶ The FBI’s subpoena is not in the record.

accessed on December 20, 2022, just days before Defendant's arrest.⁷ On or about April 6, 2023, the FBI issued a preservation request to Apple for these two accounts.⁸ *See*, Def's Exh. C to Apple Motion, p. 2.

The FBI shared the information received from the Apple subpoena with Detectives Payne and Mowery. On August 1, 2023, Detective Payne applied for a search warrant for "all Apple accounts and associated or linked accounts associated" with the two above-identified Apple accounts from October 7, 2016 to the date of Defendant's arrest. *See*, State's Exh. S-1 to Apple Objection. His search warrant affidavit discussed in detail the circumstances of the crime, the results of the investigation to date and why Defendant was arrested and charged. Detective Payne also conveyed that Defendant was seeking an advanced degree in criminology and had studied cloud-based forensics prior to the crimes. The affidavit discussed how Defendant had attempted to conceal his location during the period immediately before and after the crime was committed.

Detective Payne also included a detailed explanation about what types of information Apple captures and maintains from users of Apple accounts and that he believed the information sought from Apple 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." A search warrant for Apple was issued that same day. *See*, State's Exh. S-2 to Apple Objection ("Apple Warrant"). It stated, in relevant part:

Corporal Brett Payne, having given me proof, upon oath, this day showing probable cause establishing grounds for issuing a search warrant and probable cause to believe property consisting of there is probable cause to believe that the property referred to and sought in or upon such premises consists of information related to the investigation into burglary and/or homicides as 1122 King Road in Moscow, Idaho on or about November 13, 2022, on the Apple account and/or iCloud accounts associated with the following identifiers: Apple ID: bkohberger@spartan.northhampton.edu (DSIS 10616147671) and/or Apple ID: wifiarmyowns@yahoo.com.(DSID 1012112549)[.]

Id.

⁷ The information produced by Apple in response to the FBI's subpoena is contained on a thumb drive submitted by the State as Exhibit S-4 to the Apple Objection.

⁸ The FBI's preservation request also listed other email accounts it determined might be associated with Defendant, but Apple's response to the request indicated it had no records associated with those accounts.

The Apple Warrant set out nine categories of information sought by Detective Payne in his affidavit, as summarized: 1) account identification records; 2) records regarding devices associated with the accounts; 3) contents of emails associated with the accounts; 4) the contents of IMs associated with the accounts; 5) the content of stored iCloud files; 6) activity, connections and transactional logs for the accounts; 7) locations where the accounts were accessed; 8) records pertaining to the types of service used, and; 9) information necessary to decrypt any data. *Id.* Other than its reference to the date of the crime being investigated, the Apple Warrant was not temporally limited.

The Apple Warrant was served electronically by Detective Payne through Apple's law enforcement's email portal. As is his practice, he did not include his search warrant affidavit when serving the Apple Warrant.

Approximately one week later, Detectives Payne and Mowery downloaded the return provided by Apple and prepared and filed an inventory of the return with the magistrate. *See*, Def's Exh. E to Apple Motion. Subsequently, the magistrate issued an order allowing for the returned information to be "delivered to any person or laboratory or laboratories for the purpose of conducting or obtaining any tests, analysis, or identification of said property which is deemed necessary by the custodial law enforcement agency or jurisdictional prosecuting attorney without further order of this Court." *See*, State's Exh. S-3 to Apple Objection. Detective Payne disseminated the returned information to other members of the investigative team for processing, namely Detective Mowery and Special Agent Nicholas Ballance. Both of these individuals had access to Detective Payne's search warrant affidavit in support of the Apple Warrant.

F. Amazon Subpoena and Search Warrant

At some point in the investigation, the FBI located an Amazon account associated with Defendant. It served a federal grand jury subpoena upon Amazon, Inc. seeking order history records.⁹ Amazon responded by providing the FBI with Defendant's Amazon subscription information and purchase history from January 1, 2022 to December 13, 2022. *See*, State's Exh. S-4 to Amazon Objection.

After receiving this information, Detective Mowery applied for and received a search warrant for records retained by Amazon for Defendant's account regarding customer click activity, details of items added or deleted from his cart, all suggestions made to the account,

⁹ The FBI's subpoena is not in the record.

advertising data, device identification information and linked accounts, with a date range of March 20 through 30, 2022 and November 1, 2022 through December 6, 2022. *See*, State's Exhs. S-1 to S-3 to Amazon Objection.

IV. CONCLUSIONS OF LAW

Having already dispensed with Defendant's arguments regarding whether the warrants at issue in the four suppression motions addressed herein were invalid under *Franks* and/or as a result of law enforcement's IGG investigation, the remaining issues are as follows: 1) whether the grand jury subpoenas violated Defendant's privacy interests in his Apple and Amazon accounts under both the Fourth Amendment and Article I, § 17 of the Idaho Constitution; 2) whether the AT&T, Google, USB and Apple search warrants were sufficiently particular, and; 3) whether the Google, USB and Apple search warrants properly command a search. The Court finds suppression is not warranted on any of these issues.

A. Defendant Does Not Have A Privacy Interest In the Subpoenaed Records Protected by the Fourth Amendment or Art. I § 17 of the Idaho Constitution.

The Fourth Amendment to the United States Constitution and Article I, § 17 of the Idaho Constitution prohibit unreasonable searches and seizures. Warrantless searches and seizures are presumed to be unreasonable. *State v. Weaver*, 127 Idaho 288, 290, 900 P.2d 196, 198 (1995). However, 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. *State v. Pruss*, 145 Idaho 623, 626, 181 P.3d 1231, 1234 (2008) (citing *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980)). That involves a two-part inquiry: Did the person have a subjective expectation of privacy in the object of the challenged search? Is society willing to recognize that expectation as reasonable? *Id.* The first inquiry is a question of fact; the second, a question of law. *Id.*

1. The subpoenas did not violate Defendant's Fourth Amendment rights.

Pursuant to the third-party doctrine, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979). This is true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *United States v. Miller*, 425 U.S. 435, 443 (1976). "As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Carpenter v. United States*, 585 U.S. 296, 308 (2018.)

In *Miller*, the United States Supreme Court applied the doctrine to bank records. In investigating tax evasion, the government subpoenaed the defendant's banks, seeking cancelled checks, deposit slips, and monthly statements. 425 U.S. at 438–39. The Court rejected the defendant's Fourth Amendment challenge because he could “assert neither ownership nor possession” of these “business records of the banks.” *Id.* at 440. Moreover, the defendant's purported expectation of privacy was unavailing in light of the nature of the bank records. The checks were “not confidential communications but negotiable instruments to be used in commercial transactions”; and the bank statements were “exposed to [bank] employees in the ordinary course of business.” *Id.* at 442. Having “take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government,” the Court found the defendant relinquished any Fourth Amendment protection. *Id.* at 443.

In *Smith*, the United States Supreme Court applied the doctrine to information conveyed to a telephone company. 442 U.S. at 737–46. The Court held that the government's warrantless use of a pen register was not a “search.” *Id.* at 745–46. Relying largely on *Miller*, the Court concluded:

[P]etitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.

....

We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not ‘legitimate.’

Smith, 442 U.S. at 745.

As Defendant notes, the third-party doctrine has come under increased scrutiny in the digital age. *United States v. Moalin*, 973 F.3d 977, 992 (9th Cir. 2020) (noting “commentators and two Supreme Court Justices have questioned the continuing viability of the third-party doctrine under current societal realities.”) In her concurring opinion in *United States v. Jones*,¹⁰ Justice Sotomayor noted the doctrine is “ill suited to the digital age, in which people reveal a

¹⁰ At issue in *Jones* was GPS monitoring of a vehicle.

great deal of information about themselves to third parties in the course of carrying out mundane tasks.” 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

Later, in *Carpenter*, the United States Supreme Court rejected application of the third-party doctrine to government collection of historical CSLI. 585 U.S. at 315. In so doing, the Court found the two rationales underpinning the doctrine—first, whether the nature of the material revealed to third-parties indicates a “reduced expectation of privacy,” and, second, whether there was “voluntary exposure” of the information to others—were not fulfilled when applied to CSLI. *Id.* at 314-315.

With regard to the first rationale, the Court noted that although one normally does not have an expectation of privacy in his movement on public streets, the “pervasive” tracking of movements revealed by historical CSLI was different because it provided “a detailed chronicle of a person's physical presence compiled every day, every moment, over several years.” *Id.* at 315. “There is a world of difference between the limited types of personal information addressed in *Smith and Miller*” and the “exhaustive chronicle of location information casually collected by wireless carriers today.” *Id.* With regard to the second rationale, the Court found CSLI is “not truly ‘shared’ as one normally understands the term.” *Id.* at 315. Rather, it is data that is generated by the user simply turning on the cell phone. *Id.* Noting that carrying a cell phone “is indispensable to participation in a modern society,” the Court found that “in no meaningful sense does the user voluntarily ‘assume[] the risk’ of turning over a comprehensive dossier of his physical movements.” *Id.* (quoting *Smith*, 442 U.S. at 745).

The Court was careful to limit its holding in *Carpenter* to the facts before it, expressly declining to “disturb the application of *Smith and Miller*” in other contexts. *Id.* at 315. While Defendant recognizes this limitation, he argues that his purchase records from Amazon and data associated with his Apple accounts provide the same type of extensive private information that CSLI does.¹¹ Additionally, he points out that both Amazon and Apple are heavily regulated and contends that they guarantee their users’ privacy. Consequently, he asserts that, under *Carpenter*, a warrant is required for law enforcement to access this information.

However, unlike in *Carpenter*, the dual rationales underpinning third-party doctrine support its application to Defendant’s Amazon and Apple information. First, the nature of

¹¹ Defendant sets forth a laundry list of all the types of information Amazon and Apple collect on its users.

information obtained from the subpoenas cannot be compared to the “exhaustive chronicle” of location information at issue in *Carpenter*. The Amazon records consisted of his purchase history and associated account information for one year. The Apple records were even more limited, consisting of account subscriber information and the date the account was opened. While both Amazon and Apple are certainly capable of obtaining far more information by its users, the information specifically sought and obtained here through the subpoenas was extremely limited.

Moreover, this information was not generated by simply passively powering on a phone, as was the CSLI in *Carpenter*; it was voluntarily conveyed to third parties. The Apple subscriber information was generated by Defendant’s affirmative conduct in opening Apple accounts.¹² The Amazon purchase records were likewise generated by Defendant’s affirmative act in visiting the Amazon website, shopping for items, placing them in a shopping cart and arranging for delivery and payment. Had he been shopping in a physical store, there is no question that, under *Miller*, the security video footage of him shopping and the transaction records could be obtained without implicating the Fourth Amendment. The fact that he was in a virtual store does not change the analysis.

In addition, any subjective expectation of privacy he may have had in his Amazon purchase records and Apple subscriber information is unreasonable given—according to the policies cited by Defendant—both Amazon and Apple notify their customers that the personal information collected may be shared with other third-parties and third-party providers.¹³ Consequently, having considered both the nature of the information obtained and its voluntary exposure to other parties, the Court finds no reason to depart from the third party doctrine as applied in *Miller* and *Smith* and concludes suppression is not warranted under the Fourth Amendment.

¹² Federal courts “uniformly” hold that subscriber information and other personally identifiable information disclosed to third parties are considered fair game under *Miller* and *Smith*. 2 Wayne R. LaFave, *Criminal Procedure* §4.4(b) (4th ed) (Nov. 2024 update).

¹³See generally: Amazon.com Privacy Notice (Updated March 31, 2024): <https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010> (last accessed February 7 2025); Apple Privacy Policy (Updated Sept. 18, 2024): <https://www.apple.com/legal/privacy/en-ww/> (last accessed February 7, 2025). Both policies were cited by Defendant in his suppression motions though, notably, not the policies as they existed at the time of the search.

2. Article I, § 17 of the Idaho Constitution affords no greater protection than the Fourth Amendment.

At times, Idaho’s appellate courts have extended protections under Art. 1 § 17 of the Idaho Constitution beyond that provided by the Fourth Amendment. This greater protection has been based on an analysis of three factors: “the uniqueness of our state, our Constitution, and our long-standing jurisprudence.” *State v. Donato*, 135 Idaho 469, 470–71, 20 P.3d 5, 6–7 (2001).

With regard to the third-party doctrine, Idaho’s appellate courts have determined—with one exception—that protection under Article I, § 17 of the Idaho Constitution is coextensive with the Fourth Amendment. That exception arose in *State v. Thompson*, where the Idaho Supreme Court rejected the majority reasoning in *Smith* and held that the use of a pen register constituted a search under Article I, § 17 of the Idaho Constitution. 114 Idaho 746, 760 P.2d 1162, 1163 (1988). In recognizing “a legitimate and reasonable expectation of privacy in the phone numbers that are dialed[.]” the Court—without any additional explanation or analysis—adopted and excerpted the reasoning of Justices Stewart and Marshall in their dissenting opinions in *Smith*. *Id.* at 749-51, 760 at 1164-66.

In his excerpted dissent, Justice Stewart recognized the “vital role” telephones played in everyday life, the “intimate details of one’s life” dialed phone numbers may reveal, as well as the fact that a telephone call cannot be made without third-party involvement. *Id.* (quoting *Smith*, 442 U.S. at 746-48 (Stewart, J., dissenting)). Justice Stewart argued that constitutional protection should apply to dialed numbers as it was private information gained from surveillance and the information emanated from private conduct within a person's home or office, both of which are constitutionally protected places. *Id.* Justice Marshall’s dissent focused on societal concerns. He noted that “[p]rivacy in placing calls is of value not only to those engaged in criminal activity. The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide.” *Id.* (quoting *Smith*, 442 U.S. at 750-52 (J. Marshall, dissenting)).

Thompson was later extended by the Idaho Court of Appeals to apply to the content of text messages stored by a service provider. *State v. Branigh*, 155 Idaho 404, 411, 313 P.3d 732, 739 (Ct. App. 2013). There, the Court reasoned that if a protected privacy interest exists in dialed phone numbers then, by logical extension, it must also exist in the contents of text messages, which are “far more intimate and private[.]” *Id.*

However, *Thompson* has not been extended to recognize protected privacy interests in other third-party contexts. In *Donato*, the Idaho Supreme Court found the reasoning in *Thompson* did not justify broadening the protection under Article I, § 17 to prohibit the warrantless search of garbage left at the curb for collection. 135 Idaho at 473, 20 P.3d at 9. The Court reasoned that, unlike numbers dialed on a telephone—which a person can assume will be recorded solely for the phone company’s business purpose—trash left out for collection is knowingly exposed to public view. *Id.* at 474, 20 P.3d at 10.

In *State v. Kluss*, the Idaho Court of Appeals considered whether the defendant had a reasonable expectation of privacy under Article I, § 17 in his power consumption records held by a public utility company. 125 Idaho 14, 19-20, 867 P.2d 247, 252-53 (Ct. App. 1993). In finding he did not, the Court noted that power records do not reveal discrete information about a person’s activities; they simply identify the amount of power usage, which could be caused by any one of numerous factors. *Id.* at 21, 867 P.2d at 254. Thus, the Court found no constitutional basis for suppression when the utility company voluntarily disclosed these records to law enforcement. *Id.*

Finally, in *State v. Mubita*, the Idaho Supreme Court declined to extend *Thompson* to a defendant’s laboratory reports he voluntarily released to a public health department to obtain HIV services, as well as the health department’s own forms the defendant executed in seeking services. 145 Idaho 925, 188 P.3d 867 (2008), abrogated on other grounds by *Verska v. St. Alphonsus*, 151 Idaho 889, 265 P.3d 502 (2011)). In doing so, the Court found the records analogous to the bank records in *Miller*. *Id.* at 935, 188 P.3d at 876. By voluntarily turning over his lab reports to the health department and executing business records with the health department, the Court found the defendant assumed the risk that this information would be further disclosed by the health department. *Id.*

Defendant posits that the massive amount of private information obtained by Amazon and Apple through user activity distinguishes this case from *Donato*, *Kluss* and *Mubita* and fits squarely within the confines of *Thompson*. However, in determining privacy interests, the Court must necessarily look to the information actually obtained, not what could have been obtained. What was obtained here was extraordinarily limited, as discussed *supra*. Further, from a privacy perspective, the information is readily distinguishable from an individual’s communications made from private phones. Purchases do not become deserving of constitutional protection

simply because they are conducted through an on-line platform with third parties. Likewise, there is nothing private about subscriber information a person voluntarily conveys to a third party in order to use its services. Indeed, if a person's health care records voluntarily conveyed to the health department containing intimate information about the person's sexually transmitted disease were found undeserving of protection under Article I, § 17 of the Idaho Constitution, purchase history and subscriber information—which is far less private—falls well outside its protection. Consequently, suppression is not warranted under the Idaho Constitution.

B. The Warrants Are Sufficiently Particular.

The Fourth Amendment to the United States Constitution and Article I, section 17 of the Idaho Constitution prohibit the issuance of a warrant unless it “particularly describe[s] the place to be searched and the person or thing to be seized.” U.S. Const. Amend. 4; Idaho Const. art. 1, § 17. “The purpose of this guarantee is to safeguard the privacy of citizens by insuring against the search of premises where probable cause is lacking.” *Teal*, 145 Idaho at 989, 188 P.3d a, 931. While a search conducted pursuant to a warrant is typically reasonable, so-called “general warrants”—which permit “a general, exploratory rummaging in a person's belongings”—are prohibited. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). To prevent such “rummaging,” the Fourth Amendment requires “a ‘particular description’ of the things to be seized.” *Id.* at 467.

The purpose of the particularity requirement is to prevent the seizure of one thing under a warrant describing another and to prevent the exercise of discretion by the officer executing the warrant. *Teal*, 145 Idaho at 991, 188 P.3d at 933. Its objective is to render as limited as possible those searches deemed necessary based on the magistrate's probable cause determination. *Id.* “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.’” *Id.* (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)). This statement, however, is “not to be read literally.” *Id.* (citation omitted). Rather, the warrant must allow the searcher to “reasonably ascertain and identify the things which are authorized to be seized.” *Id.* (citations omitted). To determine if a description is sufficiently particular, the court looks to:

- (1) whether probable cause exists to seize all items of a particular type described in the warrant;
- (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and
- (3) whether the government was able to describe the items more

particularly in light of the information available to it at the time the warrant was issued.

Id. (quoting *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986)).

“The specificity required in a warrant varies depending on the circumstances of the case and the type of items involved. Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible.” *Spilotro*, 800 F.2d at 963. It is the defendant's burden to show a particularity problem on the face of the warrant. *United States v. Carhee*, 27 F.3d 1493, 1496 (10th Cir. 1994); *State v. Kelly*, 106 Idaho 268, 275, 678 P.2d 60, 67 (Ct. App. 1984) (where search has been made pursuant to warrant, it is defendant burden to show search was invalid).

If the four corners of a search warrant are found not to be sufficiently particular, a search warrant affidavit may “cure” such particularity deficiencies “when the warrant suitably references the affidavit, and the affidavit accompanies the warrant.” *Adamcik v. State*, 163 Idaho 114, 124–25, 408 P.3d 474, 484–85 (2017) (citing *Groh v. Ramirez*, 540 U.S. 551, 557–58 (2004)). No magic words are needed to suitably reference an affidavit; it can be accomplished simply by a statement on the face of the warrant noting “the supporting affidavit(s).” *Id.* (citing *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 700 (9th Cir. 2009)). The “accompany” requirement means that the affidavit may either be attached physically to the warrant or simply be available to the search team for reference. *SDI Future Health, Inc.*, 568 F.3d at 700.

Defendant’s challenges to the warrants at issue regard searches for digital data associated with Defendant’s cell phone and Google and Apple accounts. While the particularity requirement is not usually difficult to apply to a physical world, courts recognize it is more challenging to apply to the digital world. As observed by the United States Supreme Court, cell phones—with their immense storage capacities akin to powerful “minicomputers”—have become repositories of nearly every aspect of a person’s life. *Riley v. California*, 573 U.S. 373, 393-94 (2014). “Vigilance in enforcing the probable cause and particularity requirements is ... essential to the protection of the vital privacy interests inherent in virtually every modern cell phone and to the achievement of the ‘meaningful constraints’ contemplated in *Riley*.” *Burns v. United States*, 235 A.3d 758, 773-74 (D.C. 2020) (quoting *Riley*, 573 U.S. at 399).

Electronic data can be hidden in multiple formats and places in a cell phone or computer; consequently, it can be difficult for law enforcement to specify in advance the sections of the

device that should be searched. Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 Vand. L. Rev. 585, 599 (2016).

Typically, particularity violations are found with regard to electronic information search warrants in two situations: 1) where the search warrant does not state on its face what crime the search is being conducted to find evidence of, and; 2) where the search warrant contains overbroad, catch-all language. *Id.*

Defendant's challenges to the search warrants at issue focus on the latter situation. As he notes, a search warrant that simply provides an unbounded description authorizing the search and seizure of any and all digital data will typically not satisfy the particularity requirement. In *State v. Wilson*, relied upon by Defendant, the Georgia Supreme Court considered a search warrant for a forensic examination of a murder suspect's cell phones that broadly authorized the search of "any and all stored electronic information" on the phones, "including but not limited to" various kinds of electronic information. 884 S.E.2d 298, 300–01 (Ga. 2023). The search warrant included preprinted boilerplate 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..." followed by check boxes where the affiants could choose among preprinted statements generally describing how the object of the search was relevant.¹⁴ *Id.* In opposing the defendant's suppression motion, the state relied on this preprinted form language as "limiting" what it acknowledged to be otherwise sweeping authorization. The court noted that while such broad language may be permissible where the warrant contains a "residual clause" or other limiting language constraining the search to evidence of a specific crime, the preprinted language provided no such limit. *Id.*¹⁵

¹⁴ In the warrant at issue in *Wilson*, the officer checked boxes stating that the cell phones at issue 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.'" *Id.* at 299-300.

¹⁵ Defendant points out that, in a concurring opinion in *Wilson*, one justice questioned whether the inclusion of a residual clause would save the warrant from overbreadth stating: "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." *Id.* at 303 (Peterson, J., concurring). However, the weight of authority recognizes that if warrants for cell phone searches are affirmatively limited to evidence of a specific crime or specific types of material, the particularity requirement is met. 2 Wayne R. LaFave, *Criminal Procedure*, § 3.4(e)

As recognized in *Wilson*, broad language may be permissible where the warrant constrains the search to evidence of a specific crime rather than allow a fishing expedition for all criminal activity. *See, e.g., United States v. Bishop*, 910 F.3d 335, 336-37 (7th Cir. 2018); *United States v. Bass*, 785 F.3d 1043, 1049-50 (6th Cir. 2015). The rationale for holding that such warrants are sufficiently particular and not overbroad is that “[c]riminals don’t advertise where they keep evidence.” *Bishop*, 910 F.3d at 336. Indeed, “[a] warrant authorizing the search of a house for drugs permits the police to search everywhere in the house, because ‘everywhere’ is where the contraband may be hidden.” *Id.* at 336-37. Moreover, in the context of electronic devices such as computers and cell phones, “criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity [such that] a broad, expansive search of the [device] may be required.” *Bass*, 785 F.3d at 1049-50 (citations omitted). Because law enforcement cannot know in advance how a suspect may label or code files containing evidence of criminal activity, “by necessity government efforts to locate particular files will require examining many other files to exclude the possibility that the sought after data are concealed there.” *People v. English*, 52 Misc. 3d 318, 321-22, 32 N.Y.S.3d 837 (N.Y. Sup. Ct. 2016).

However, as Defendant notes, the inclusion of a residual clause or other limiting language is not a green light for law enforcement to search in electronic files where evidence of the crime is unlikely to be. *See, United States v. Winn*, 79 F. Supp. 3d 904, 919 (S.D. Ill. 2015) (“The major, overriding problem with the description of the object of the search—‘any or all files’—is that the police did not have probable cause to believe that *everything* on the phone was evidence of the crime of public indecency.”). For example, if there is probable cause to believe that evidence of a crime will be found in text messages, but not in photos, videos, or any other applications on a particular device, then a warrant allowing officers to access all the data in the device would violate the particularity requirement. *See, Gershowitz* at 633.

If the circumstances of the investigation allow officers to narrow the search, a limitless search warrant is unacceptable. To this end, Defendant cites to *State v. Castagnola*, where the Ohio Supreme Court found overbroad a search warrant commanding a search for “records and documents stored on computers” without any limitation on what records or documents could be searched. 46 N.E.3d 638, 656 (Ohio 2015). This language, the court noted, did not serve to

(4th ed.) (Nov. 2024 update) (collecting cases).

“guide and control” the searcher’s judgment as to what was to be seized on the computer and included items that were not subject to seizure. *Id.* at 658. Importantly, the court observed that the detective was able to articulate at the suppression hearing the specific records and documents he expected to find on the computer, yet he did not include those details in the search warrant affidavit. *Id.* The Court found “this degree of specificity was required, since the circumstances and the nature of the activity under investigation permitted the affiant to be this specific.” *Id.*

Likewise, if circumstances allow officers to include temporal restrictions for a search of digital data, it may also satisfy the particularity requirement. In *Wheeler v. State*—also cited by Defendant—the Supreme Court of Delaware held that where there were no facts in the search warrant affidavit that the crime at issue occurred prior to July of 2013, a warrant authorizing a search of the defendant’s computer without any temporal limit was impermissibly overbroad. 135 A.3d 282, 304-05 (Del. 2016). Moreover, even after determining that the computer had not been powered on since September of 2012, the searcher nevertheless “sifted through [the defendant’s] digital universe” despite the fact that the search would not have contained relevant material. *Id.* As in *Castagnola*, the court observed that although general classifications in a warrant are permissible where a more precise description is not possible, if investigators are able to be more specific, such specificity should be included in the probable cause affidavit so as to appropriately narrow the warrant and “mitigate the potential for unconstitutional exploratory rummaging.” *Id.* See also, *Commonwealth v. Snow*, 160 N.E.3d 277, 288 (Mass. 2021) (“The magnitude of the privacy invasion of a cell phone search utterly lacking in temporal limits cannot be overstated.”).

1. The AT&T Warrants

With regard to both AT&T warrants, Defendant asserts they are “all encompassing,” duplicative” and their only limitation is that “the property be related to the homicides in this matter.” The State responds that the warrants are sufficiently particular, pointing out the subject matter and temporal limits therein. It further argues that any deficiency in particularity is cured by Detective Payne’s search warrant affidavits, which the State contends are incorporated into the warrants.

The Court finds the AT&T warrants, even without supplementation by their respective supporting affidavits, satisfy the particularity requirement. While the warrants covered a broad array of digital information held by AT&T, they did not authorize a fishing expedition for “any

and all” data as was the case in *Wilson*. 884 S.E. 2d at 300. First, they were bounded by subject matter limitations. They were limited to a single identified cell phone number and contained a residual clause limiting the evidence sought to the specific crime (and address) being investigated. In addition, the warrants defined specific categories of data to search and seize, which did not include all of the possible data AT&T could have provided. Far from an “any and all” type of warrant, these warrants prescribed careful limits to ensure there was no question as to what electronic data was subject to the search.

Second, the warrants were subject to significant temporal limitations. Unlike in *Wheeler*, which was devoid of any temporal limit, the information sought in the first AT&T warrant was limited to a 48-hour period immediately before and after the homicides being investigated. The second AT&T warrant was limited to the preceding six months, which was intended to capture information about whether Defendant stalked or surveilled the victims.

Collectively, these subject matter and temporal limitations served to narrow the scope of the search and guide the discretion of the search team, thus avoiding unwarranted searches. Moreover, while Defendant claims that law enforcement was “capable of greater specificity” in the warrants as to what could be seized, he provides absolutely no support or explanation for this conclusory statement. Consequently, the Court finds that—standing alone—the warrant satisfies the *Teal* test and suppression is not warranted.

Moreover, to the extent the warrants—standing alone—suffer from a deficiency in particularity, the Court finds Detective Payne’s search warrant affidavits were sufficiently incorporated therein. As mentioned, for a search warrant affidavit to supplement particularity, the warrant must “suitably” reference the affidavit and the affidavit must “accompany” the warrant. *Adamcik*, 163 Idaho at 124, 408 P.3d at 484. The AT&T warrants reference the affidavit by noting: “Brett Payne, having given me proof, upon oath, this day showing probable cause...” Language very similar to this has been held sufficient to “suitably reference” the search warrant affidavit. *See, United States v. Vesikuru*, 314 F.3d 1116, 1120 (9th Cir. 2002) (warrant stating “upon the sworn complaint made before me” adequately referenced the search warrant affidavit). In addition, the returns from AT&T were provided by Detective Payne to Agent Ballance for analysis. Agent Ballance both aided Detective Payne in drafting his AT&T search warrants and had access to them during his analysis. This is sufficient for the search warrant affidavits to

“accompany” to warrants. *Id. SDI Future Health, Inc.*, 568 F.3d at 700 (the “accompany” requirement met if search warrant affidavit is available to the search team for reference).

In his search warrant affidavits, Detective Payne discussed at length the circumstances of the crime, the results of the investigation to date and why Defendant was a suspect. He included a detailed explanation about what types of information a cellular carrier retains—specifically regarding the location of a cellular device—and why that information could provide valuable evidence in the investigation of the case. Thus, to the extent the AT&T warrants were lacking in specificities, the search warrant affidavits cured it. Suppression is not warranted.

2. The Apple Warrant

With regard to the Apple Warrant, Defendant asserts it cast too broad a net, effectively allowing the search and seizure of all data from the two accounts. The State responds that, particularly when considered with Detective Payne’s supporting search warrant affidavit, the Apple Warrant imposed subject matter and temporal restrictions that were as narrow as could be reasonably expected given the nature of the investigation and the object of the search, i.e., electronic records.

The Court finds, standing alone, the Apple Warrant satisfies the particularity requirement. To this end, the Court finds two cases to be instructive. The first is *United States v. Pelayo*, where the Ninth Circuit recently rejected a similar challenge to a warrant authorizing a search of a defendant’s iCloud account. 2023 WL 4858147, at *1 (9th Cir. July 31, 2023). The warrant identified the accounts to be searched by phone number and Apple ID. It also described the data to be disclosed by Apple and the evidence that the government could search for and seize. *Id.* Although the warrant ordered Apple to produce “the entirety of Pelayo’s iCloud account,” the search and seizure of the evidence was limited to the identified crimes (i.e., drug-related crimes) and twenty-one specific types of evidence that the government could seize. *Id.* It was also limited temporally to evidence after January of 2013.

The Ninth Circuit found the warrant was “not a general warrant, because it did not allow the executing officer to rummage through Pelayo’s iCloud account without discretion.” *Id.* (citing *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). Further, the court rejected the defendant’s argument that the government could have narrowed the warrant by excluding allegedly “unnecessary” information such as iTunes or iGames. *Id.* at *2. It noted these accounts could have possibly contained evidence of a crime but, “even if they did not, the search and

seizure of data that was obtained from Apple was limited to evidence of the specified crimes.”
Id.

Conversely, in *United States v. Pilling*, cited by Defendant, Idaho’s federal district court found a warrant authorizing a search of a defendant’s Apple accounts for the same information sought here was overbroad. 721 F.Supp.3d 1113 (2024). The only limitation in *Pilling* was that the search of the account was limited to “fruits, contraband, evidence, and instrumentalities of violations” of five federal statutes: the Clean Air Act, conspiracy to defraud the United States, false statements, obstruction of agency proceedings and witness tampering and destruction/alteration of evidence. *Id.* at 1119. The court noted the warrant did not include the identity and nature of items to be seized and did not describe “the items one commonly expects to find on premises used for the criminal activities in question.” *Id.* at 1126 (citation omitted). In addition, the court found the warrant could have more specific by: 1) ensuring the search warrant affidavit—which provided ample particularity—was incorporated into and accompanied the search warrant when executed, and; 2) describing the kinds of things authorized to be seized, such as emails and text messages related to the specific circumstances of the case. *Id.* at 1127.

Although the Apple warrant here is not as limited as that in *Pelayo*, it is more specific than that in *Pilling*. To satisfy particularity, the warrant must “at least minimally confine[] the executing officers’ discretion by allowing them to seize only evidence of a particular crime.” *United States v. Dickerson*, 166 F.3d 667, 693 (4th Cir. 1999), *rev’d on other grounds*, 530 U.S. 428 (2000). *Dickerson* distinguished between evidence of a “particular crime” and “general criminal activity” to wit:

A warrant authorizing a search for evidence relating to ‘a broad criminal statute or general criminal activity’ such as ‘wire fraud,’ ‘fraud,’ ‘conspiracy,’ or ‘tax evasion,’ is overbroad because it ‘provides no readily ascertainable guidelines for the executing officers as to what items to seize’.... In contrast, a warrant authorizing a search for evidence relating to ‘a specific illegal activity,’ such as ‘narcotics,’ or ‘theft of fur coats’ is sufficiently particular.

Id. at 694.

The only limiting factor in the *Pilling* warrant was that it was specific to evidence related to a violation of five very broad federal statutes. False statements, obstruction, witness tampering and destruction of evidence can cover a wide array of activities that do not generate distinctive digital evidence and can exist virtually anywhere. By contrast, the warrant here was limited to

information “related to the investigation into burglary and/or homicides as 1122 King Road in Moscow, Idaho on or about November 13, 2022[.]” Murder and burglary are specific activities, the planning and commission of which can generate distinct evidence. Further, while the warrant was not subject to a temporal limitation, the Court does not find this fatal to particularity. Namely, the subject matter of the warrant was limited to evidence of the “burglary and/or homicides ... on or about November 13, 2022.” This necessarily limited the time frame concerned and, therefore, the discretion of the searchers.

Moreover, the Apple Warrant only authorized the search of nine specific categories of information from the Apple accounts. While these categories covered a wide array of information, some of the broader categories were subject to modifying provisions, such as contents of emails “in order to locate any materials referencing the planning or commission of the above offense”; contents stored on iCloud “in order to locate any potential source material or material created after the commission of the above offenses,” and; all activity logs for the accounts “in order to locate any additional connectivity between the suspect and the victims in this case.” In *Pilling*, by contrast, there was no indication that the same nine categories of information were similarly constrained.

Defendant asserts law enforcement could have been more specific as to what could be seized and searched, he does not explain how. As many courts have correctly observed, electronic data can be hidden in numerous and varied formats to conceal criminal activity. Consequently, it would be unduly restrictive to require law enforcement to identify file names or craft key word searches. “[I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files.” *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009). This is particularly true here, where law enforcement knew Defendant was seeking an advanced degree in criminology at the time of the homicides and had studied cloud-based forensics prior to the crimes. Thus, he was a highly sophisticated user and could—and likely would—attempt to cover his digital tracks.

Moreover, to the extent the warrant—standing alone—suffers from a deficiency in particularity, the Court finds Detective Payne’s supporting search warrant affidavit was sufficiently incorporated therein. The Apple Warrant references the affidavit by noting: “Corporal Brett Payne, having given me proof, upon oath, this day showing probable cause...”

In addition, the return from Apple was provided by Detective Payne to Detective Mowery and Agent Ballance for processing, both of whom had access to Detective Payne's search warrant affidavit. This was sufficient for the search warrant affidavit to "accompany" to warrant.

In his search warrant affidavit, Detective Payne discussed at length the circumstances of the crime, the results of the investigation to date and why Defendant was a suspect. He included a detailed explanation about what types of information Apple captures and maintains from users of Apple accounts and why he believed the information sought in the Apple warrant 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." He also identified a temporal range for the search of "October 7, 2016 (dates accounts were created) to December 30, 2022 (date Kohberger's arrest)." Thus, to the extent the Apple Warrant was lacking in specificities, the search warrant affidavit cured it. Suppression is not warranted.

3. The Google Warrants

Defendant challenges the Google warrants as representing "an exhaustive list of everything that is available in Google accounts" without any attempt to narrow, despite the fact that he asserts law enforcement could have done so. He also argues—in a conclusory fashion—that not all of the information sought in the Google warrants was supported by probable cause. However, Defendant has not identified anything specifically not supported by probable cause. The State responds that, particularly when considered with Detective Payne's search warrant affidavits, the Google warrants imposed subject matter and temporal restrictions that were as narrow as could be reasonably expected given the nature of the investigation and the object of the search, i.e., electronic records. Further, it argues the search warrant affidavit provided sufficient probable cause for the information sought.

a. The search warrant affidavits provide probable cause.

With regard to the probable cause challenge, it is the search warrant affidavit that informs the analysis, regardless of whether they were properly incorporated into the warrants themselves. *Hutton*, 169 Idaho at 759, 503 P.3d at 975. "A warrant may be considered so lacking in indicia of probable cause if the applicant files merely a bare bones affidavit, one which contains only wholly conclusory statements and presents essentially no evidence outside of such conclusory statements." *State v. Short*, 964 N.W.2d 272, 313 (Neb. 2021).

Here, Detective Mowery’s search warrant affidavits in support of the Google warrants were far from “bare bones.” They provided an extensive explanation as to how Defendant was connected to the homicides, how each email account, phone number and IMEI at issue in the warrants was discovered, how they were linked to Defendant, and why the Google data associated therewith could produce evidence of the homicide.¹⁶ In the affidavit for Google Warrant One, Detective Mowery discussed how the investigation led to the discovery of the two phone numbers, the IMEI and bryanchristopher1994@gmail.com. Def’s Exh. A to Google Motion, pp. 26, 28. He then outlined why, in his training and experience, he believed the various Google records for each account could “determine any time periods that devices associated with Kohberger were in the vicinity of the King Road Residence” and “identify other devices that Kohberger has used or is using that may contain evidence of the described offense as well as any Google account activity that would show Kohberger’s activity as it related to the planning, communications, execution, and disposal of evidence related to the named offense.” *Id.*, p. 29.¹⁷

In the affidavit supporting Google Warrant Two, Detective Mowery explained that his review of the information returned on Google Warrant One revealed a “recovery email” of yewsirneighm@gmail.com and showed a login had occurred on that account at 4:49 a.m. on November 13, 2022—soon after the homicide occurred—through what was likely a VPN server. Def’s Exh. B to Google Motion, p. 41. He stated his request for the warrant was to “establish Bryan Kohberger’s previous contacts, locations, correspondence, purchases, and any other information which could aid the investigation into the homicides” of the four victims. *Id.* He again provided a detailed explanation as to how the information sought in Google Warrant Two for this additional email address could reveal evidence relevant to the homicides. *Id.* at pp. 2-19.

Google Warrant Three further sought Gmail accounts linked by “recovery email, cookie, Android ID, Creation IP or phone number” associated with the identifiers that were the subject of the prior two emails.¹⁸ In his affidavit, Detective Mowery explained that Google users “can

¹⁶ The sole exception is the email address: bk5781@desales.edu which is the subject of Google Warrant Three. There is no explanation in the search warrant affidavit as to how law enforcement identified that account. However, as the State points out, nothing was returned on that account and, therefore, there would be nothing to suppress if probable cause was not found.

¹⁷ Detective Mowery provided an even more detailed description of how each separate Google service works and why it could reveal evidence relevant to the homicides. Def’s Exh. A, pp. 2-19.

¹⁸ Google Warrant Three also added bk5781@desales.edu but, as discussed, there was no return on this account.

create multiple Gmail accounts that may be accessed via web browsers or other devices” and was requesting the warrant “[i]n an effort to search for any and all other Gmail accounts possible associated with Kohberger[.]” Def’s Exh. C to Google Motion, p. 30. He again provided a detailed explained as to how the information sought in Google Warrant Three for linked Gmail accounts could reveal relevant evidence. *Id.* at pp. 1-20.

Based on Detective Mowery’s extensive search warrant affidavits, it was reasonable for the magistrate to conclude that relevant evidence would likely be found within the files associated with the identified accounts. Further, the warrants’ scope did not exceed their probable cause confines. Indeed, other than arguing in a conclusory fashion that the warrants lacked probable cause, Defendant has not articulated in what specific ways probable cause is lacking.

b. The Google warrants are sufficiently particular.

The Court further finds the three Google warrants, even without reference to their respective search warrant affidavits, were sufficiently particular. They clearly identified the place to be searched, i.e., the identified accounts located at Google, and the information to be seized, i.e., data from the sixteen identified Google services. They were each subjected a significant temporal restriction from January 1, 2021 to December 30, 2022, which could reasonably capture activity leading up to the November 13, 2022 homicides through Defendant’s arrest. In addition, the search prescribed was for data “related to the investigations into the crime(s) of homicide at 1122 King Road, Moscow, Idaho.” This was not, as Defendant claims, an exhaustive search of “everything available” on a Google account. It was tailored to the probable cause established by Detective Mowery.

While Defendant claims that law enforcement was capable of greater specificity, he does not explain how. As Detective Mowery explained in his search warrant affidavits, the evidence he was seeking could be in multiple formats and areas. He was not looking for a specific file; he was looking for evidence of a connection between Defendant and the homicides, which could be in any of the sixteen different Google services identified in the warrant. Under these circumstances, it is unreasonable to require more narrowing than what was already provided. *See, e.g., Bass*, 785 F.3d at 1050 (warrant describing categories of data to be searched in cell phone where officers did not know where specific evidence of the crime would be located or in what format was reasonable).

To the extent the Google warrants are not sufficiently particular standing alone, the search warrant affidavits cure any deficiencies. Each of the Google warrants referenced its respective search warrant affidavit (i.e., “Lawrence Mowery, having given me proof, upon oath, this day showing probable cause...”). Additionally, the search team processing the returns had access to the search warrant affidavits. Thus, the affidavits were incorporated into the Google warrants. In these affidavits, Detective Mowery set forth a statement describing in detail the scope and results of the investigation to date, how the accounts and phone numbers identified in each warrant were discovered and how they were connected to Defendant. He also included a detailed explanation as to how Google works and why each of the sixteen items listed in the warrants could be relevant to the investigation. When considered with the Google warrants, there can be no dispute that particularity is met.¹⁹ Suppression is, therefore, not warranted.

4. The USB Warrant

With regard to the USB Warrant, Defendant contends that law enforcement was capable of providing greater specificity in the warrant, yet instead sought and obtained permission for a limitless search of the contents of his cell phone. He notes that although the “data compilation” category is limited to information “indicating, suggesting, or related to violence, a fight, or motive/hostility for any of the same,” that limit is rendered illusory by the remaining categories of data. Those remaining categories, he argues, are necessarily included in the “data compilation” category, yet they are not similarly limited, effectively allowing a search of all the contents of the cell phone. He further notes the USB warrant fails to delineate the type of digital files that can be searched, instead opting for broad categories of data. The State responds that, particularly when considered with Detective Mowery’s search warrant affidavit, the USB warrant imposed subject matter and temporal restrictions that were as narrow as could be reasonably expected given the nature of the investigation and the object of the search, i.e., electronic records. Further, it argues the search warrant affidavit provided sufficient probable cause for the information sought.

The USB Warrant not as limitless as Defendant claims. First, while it is not temporally limited, the object of the search was specifically to “evidence regarding the investigation into the crimes of homicide of Madison Mogen, Kaylee Goncalves, Xana Kernodle, and Ethan Chapin at

¹⁹ Indeed, Defendant has not argued that if the search warrant affidavits were considered, particularity would still not be met.

1122 King Road, Moscow, Idaho.” Therefore, unlike in *Wilson*, where the court rejected a warrant for “any and all” data on the seized cell phone without any residual clause limiting it to the evidence of the crime at issue, the warrant here was specifically limited to evidence of the homicides of four identified victims at a particular location. Therefore, in performing the search, the agents’ discretion was limited to data that could establish a connection between Defendant and these specific victims and the specific crime of homicide committed on a specific date. Further, when the purpose of the search is to look for some motive or connection between a suspected murderer and his victims, imposing a more narrow limit likely could have the real effect of excluding relevant evidence.

Defendant’s claim that law enforcement could have been more specific as to the content and category of digital files sought but failed to do so likewise lacks merit. Under the circumstances, particularity did not demand such technical precision. Law enforcement was looking for evidence of any connection between Defendant and the four individuals he was suspected of killing, not a specific item. Without knowing precisely what evidence existed, law enforcement did not know, nor could they have known, the precise location within Defendant’s cell phone the evidence would be found. In such cases, listing categories of data as opposed to specific digital files is sufficient. *Compare Bass*, 785 F.3d at 1050 (warrant describing categories of data to be searched in cell phone where officers did not know where specific evidence of the crime would be located or in what format was reasonable) and *Winn*, 79 F.Supp.3d at 919-921 (warrant describing category of data rather than specific items not particular enough where police knew precise identity and content of evidence sought).

Moreover, the categories of data were not a laundry list of everything that can possibly be contained in a cell phone. The “data compilations” section was limited to information relating to “violence, a fight, or motive/hostility for any of the same[.]” The following eight sections are specific to communications, stored contacts, location information, internet activity, notes and indicia of ownership/possession of the data. Thus, a reasonable effort was made to limit the search and seizure to digital information contained in Defendant’s cell phone that would reveal a connection between Defendant and the homicides of the four identified victims.

Again, to the extent the USB warrant alone is deficient, the search warrant affidavit supporting it can supplement particularity given that was referenced within the USB warrant and

available to members of the search team processing the information. Consequently, the Court finds particularity is met and suppression is not warranted.

C. Any Deficiency in the Warrants' Command to Search is Not a Basis for Suppression.

Defendant's final challenge to the warrants is that they do not properly command a search of the information seized. The Court does not find the warrants are deficient in this regard and, even if they are, it is not a basis for suppression.

Pursuant to ICR 41(d), a warrant must identify the property to be searched through name or description, be directed to an authorized peace officer, and command the officer to search within a specific period of time. As observed by the Idaho Court of Appeals, "[s]earch warrants are not deeds or tax notices. They are not subject to technical drafting requirements. They should be interpreted in 'a commonsense and realistic fashion.'" *State v. Holman*, 109 Idaho 382, 388, 707 P.2d 493, 499 (Ct. App. 1985) (quoting, *United States v. Ventresca*, 380 U.S. 102, 108 (1965)).

Defendant's challenge is based on an over-technical reading of the warrants. The Apple warrant identifies the two Apple accounts to be searched and the specific information from those accounts to be seized, all of which is located at Apple, Inc.'s premises. The command then states: "You are therefore commanded to search the above-described premises for the property described above, to seize it if found and bring it promptly before the court above named." Likewise, the Google warrants identify the accounts to be searched and the specific information from those accounts to be seized, all of which is located at Google's premises. The same search command as in the Apple warrant appears in the Google warrants. A reasonable reading of this command is the "premises" of Apple and Google are to be searched for the accounts identified and the specific data identified within each account is to be seized. There is nothing about the command that would cause confusion as to the property to be searched and seized.

The USB warrant, however, appears to command a search of the Moscow Police Department Forensics Lab and seizure of the USB, not a search of the USB. However, any confusion in this regard was clarified by the magistrate's subsequent order authorizing the USB to be "delivered to any person or laboratory or laboratories for the purpose of conducting or obtaining any tests, analysis, or identification of said property...." Further, it is simply not

reasonable, when considering the USB warrant as a whole, to interpret it as authorizing a search of the forensics lab as opposed to the USB.

More importantly, any deficiencies in the commands to search are not of constitutional dimension. First, it is well settled in the federal arena that a violation of Rule 41, F.Crim.R.P.,²⁰ alone does not require suppression of evidence if the search otherwise conforms to constitutional standards. 3A Sarah N Welling, Federal Practice & Procedure Crim. (*Wright & Miller*) § 686 (4th ed) (June 2024 update). Rather, technical errors in warrants require suppression only if a defendant can show either prejudice or that there was evidence of “deliberate disregard of the rule.” *United States v. Manaku*, 36 F.4th 1186, 1190 (9th Cir. 2022) (citation omitted). With regard specifically to erroneous descriptions of the place to be searched, Idaho looks to whether the place “is described with sufficient particularity as to enable *the executing officer* to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.” *State v. Young*, 136 Idaho 711, 715, 39 P.3d 651, 655 (Ct. App. 2002) (citing *United States v. Gitcho*, 601 F.2d 369, 371 (8th Cir.1979)) (emphasis in original).

Defendant has not shown either prejudice or deliberate disregard of ICR 41(d). Further, as noted, the places to be searched are reasonably described so as to avoid any chance that a mistaken premises might be searched instead. Consequently, suppression is not warranted due to alleged problems with the search commands.

V. CONCLUSION

Based on the foregoing, the Court DENIES the following:

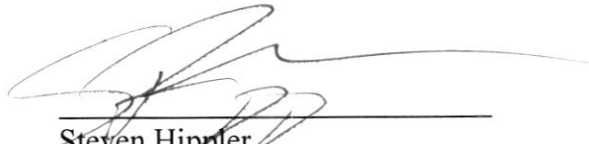
- Defendant’s Motion to Suppress Re: AT&T First Warrant (Nov. 14, 2024);
- Defendant’s Motion to Suppress Re: Pen Trap and Trace Device (Nov. 14, 2024);
- Defendant’s Motion to Suppress Re: re: Apple Account Federal Grand Jury Subpoena and Search Warrant Dated August 1, 2023 (Nov. 14, 2024);
- Defendant’s Motion to Suppress re: Amazon Account Federal Grand Jury Subpoena and Search Warrants Dated April 26, 2023 and May 8, 2023 (Nov. 14, 2024);

²⁰Rule 41(e) of the Federal Rules of Criminal Procedure is substantively the same as ICR 41(d) and, therefore, instructive.

- Defendant's Motion to Suppress re: Google Warrants Dated 1/3/23, 1/24/23, and 2/24/23 (Nov. 14, 2024), and;
- Defendant's Motion to Suppress re: Moscow Police Forensic Lab Warrant Dated January 9, 2023 (Nov. 14, 2024).

IT IS SO ORDERED.

DATED this 19th day of February, 2025.



Steven Hippler
District Judge

CERTIFICATE OF MAILING

I HEREBY CERTIFY that on this 19th day of February, 2025, I caused a true and correct copy of the above and foregoing instrument to be mailed, postage prepaid, or hand-delivered, to:

William W. Thompson, Jr.
Ashley Jennings
LATAH COUNTY PROSECUTING ATTORNEY
paservice@latahcountyid.gov

Jeffery Nye
DEPUTY ATTORNEY GENERAL
Jeff.nye@ag.idaho.gov

Anne Taylor
ATTORNEY FOR DEFENDANT
info@annetaylorlaw.com

Elisa C. Massoth
ATTORNEY FOR DEFENDANT
emassoth@kmrs.net

Jay Logsdon
KOOTENAI COUNTY PUBLIC DEFENDER
jay.logsdon@spd.idaho.gov

TRENT TRIPPLE
Clerk of the District Court

By: 
Deputy Court Clerk

