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

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

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

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

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

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

COMES NOW, Bryan C. Kohberger, by and through his attorneys of record, and submits the following Reply to the State's objection to his Motion to Suppress and Memorandum in Support Re: Google Warrants Dated 1-3-23, 1-24-23, and 2-24-23.

The words "proof upon oath" are not synonymous with "the affidavit for search warrant is here by incorporated". A non-particularized general affidavit in support of a search warrant held in the hands of law enforcement, which never accompanied the electronically served warrant, cannot be relied upon to validate a warrant. The warrants never directed law enforcement to exclude any legal information obtained, in support of particularity. All contents of the Google Warrant returns must be suppressed.

I. The Warrants were General and the Affidavit was Not Incorporated into the Three Warrants or Served with the Warrants.

The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Article I, Section 17 of the Idaho Constitution is virtually identical to the Fourth Amendment, except that "oath or affirmation" is termed "affidavit."

The Supreme Court has acknowledged "that a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Groh v. Ramirez*, 540 U.S. 551, 557–58, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004). In *SDI Future*, the Ninth Circuit held that a statement on the face of the warrant noting "the supporting affidavit(s)" was sufficient as a suitable reference and incorporation. The warrants contained no language that the affidavit was incorporated. In misguided fashion, the State asserts that there is no requirement for specific language and relies on *Adamcik v. State*, which upheld a warrant where "the opening paragraph of the warrant unambiguously referenced the affidavit and sworn testimony of Detective Sellers as the basis for

the warrant." 163 Idaho 114, 125 (Idaho S. Ct. 2017). No such language exists in the Google Warrants. The word affidavit is not mentioned or incorporated into the warrants.

The Affidavit of Det. Brett Payne swears that Detective Mowery served the "warrant." *See* Exhibit D Google Memorandum. The email between Mowery and Google reference a "warrant." *See* Exhibit F Google Memorandum. No return documents reference the Affidavit in Support of Search Warrant as having accompanied any of the Google warrants when they were served. Nor does the State produce such records in its Objection. The process described by the State as meeting the criteria of *State v. Teal* simply does not exist. In its incorporated Objection to the Motion to Suppress Apple Warrant, the State indicates that the "investigators necessarily had copies of the affidavit in their possession when they executed the warrant by emailing it to Apple." *See* Apple Objection, p. 5. Further, the State offers that "[t]he effect of this is that the Affidavit for Search Warrant and appended Exhibit A cure any supposed deficiencies in the naked warrant." *See* Apple Objection, pp. 5-6. An officer sitting at a computer executing a search warrant by submitting it to Google through a law enforcement portal and having the affidavit for search warrant in his hand is different than an officer being physically present when executing a search warrant and having the affidavit for search warrant available for reference. Where a supporting affidavit does not accompany the search warrant at the time of execution, the detail set out in the affidavit does not cure any deficiencies. *U.S. v. Pilling*, 721 F.Supp. 3d 1113, 1126 (D. Idaho 2024) (warrant suppressed where supporting affidavit was not provided to Apple). An affidavit is considered "to be part of a warrant, and therefore potential curative of any defects, 'only if (1) the warrant expressly incorporated the affidavit by reference and (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search.'" *SDI Future Health Inc.,* at 699 (citing *United States v. Kow,* 58 F.3d 423, 429 n. 3 (9th Cir.1995)).

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

Courts consider three factors in analyzing the potential overbreadth of a warrant: (1) "whether probable cause existed to seize all items of a category described in the warrant," (2) "whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not," and (3) "whether the government could have described the items more particularly in light of the information available." *United States v. Flores*, 802 F.3d 1028, 1044 (9th Cir. 2015) (quoting *United States v. Lei Shi*, 525 F.3d 709, 731–32 (9th Cir. 2008)).

The Fourth Amendment requires particularity. "The particularity requirement's objective is that those searches deemed necessary based on a probable cause determination by a magistrate should be as limited as possible." *State v. Teal*, 145 Idaho 985, 991, 188 P.3d 927, 933 (2008). Even if the Affidavit of Search Warrant had been incorporated into the warrant, it could have described particularized items as opposed to the laundry list of items held by Google without designation of a duty to separate lawful items.

The particularity requirement means that a warrant must be "specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized." *U.S. v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). Once the warrant is specific enough, there must still be a search that provides guidelines to 'distinguish items used lawfully from those the government had probably cause to seize." *Id.* at 964. Not only did the state obtain the entirety of Mr. Kohberger's Google accounts, it has taken no action to sort through that which is lawful or applies to the charges. It has produced the warrant return data without any reports or analysis whatsoever.

The fact that the Google Accounts are sought because they may hold some of the objects of the proposed search does not automatically give the State authority to seize every piece of data

that ever touched the accounts between January 1, 2021 and December 30, 2022. Instead, the "balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures of electronic data must be determined on a case- by-case basis." *United States v. Schesso*, 730 F.3d 1040, 1050 (9th Cir. 2013).

The Google Search warrants were not supported by probable cause to support everything listed, there were absolutely no limiting standards included at all, and the state could have particularized the warrant to specific dates and items that would be evidence of the specific crimes. The Google Search Warrants did none of that.

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

In response to the State's arguments under "Defendant Has Not Demonstrated the Search Warrant Affidavits Contain Intentionally or Recklessly False Statements or Omissions," Defendant refers the Court to and hereby incorporates Defendant's Replies in Support of Defendant's pleadings in support of a *Franks* Hearing and suppression of Genetic Information.

CONCLUSION

Mr. Kohberger requests that this Court suppress all evidence obtained by police via the subpoenas and warrants that permitted them to search Mr. Kohberger's Google accounts.

DATED this _19_ day of December, 2024.

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

CERTIFICATE OF DELIVERY

I hereby certify that a true and correct copy of the foregoing was personally served as indicated below on the ___19____ day of December, 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

721 F.Supp.3d 1113
United States District Court, D. Idaho.

UNITED STATES of America, Plaintiff,
v.
Brek PILLING, Defendant.

Case No. 4:22-cr-00282-BLW
|
Signed March 2, 2024

Synopsis

Background: Defendant, who was charged with violating the Clean Air Act (CAA) by causing the demolition of two buildings without following the Environmental Protection Agency's (EPA) National Emissions Standard for Hazardous Air Pollutants (NESHAP) work practice standards for handling and removal of asbestos, moved to suppress evidence obtained pursuant to two search warrants.

Holdings: The District Court, B. Lynn Winmill, J., held that:

search warrant directed to web-based email provider for two email accounts associated with defendant was not overbroad;

search warrant directed to web-based email provider was supported by probable cause;

search warrant directed to web-based email provider was sufficiently particular;

warrant authorizing search of defendant's entire cloud storage account for fruits, contraband, evidence, and instrumentalities of violations of five statutes lacked particularity required by Fourth Amendment;

doctrine of severance did not apply to warrant authorizing search of defendant's entire cloud storage account; and

government violated Fourth Amendment through its detailed, nine-month review of defendant's entire cloud storage account without removing unresponsive data.

Motion granted in part and denied in part.

Procedural Posture(s): Pre-Trial Hearing Motion.

Attorneys and Law Firms

***1117** Cassandra Barnum, DOJ-Enrd, Washington, DC, Francis Joseph Zebari, United States Attorney's office, Boise, ID, for Plaintiff.

David Z. Nevin, Nathan Pittman, Scott McKay, Nevin, Benjamin & McKay LLP, Boise, ID, for Defendant.

MEMORANDUM DECISION AND ORDER

B. Lynn Winmill, United States District Court Judge

INTRODUCTION

Before the Court is Defendant Brek Pilling's Motion to Suppress (Dkt. 37). The ***1118** defendant seeks to suppress evidence obtained pursuant to two search warrants. For the reasons explained below, the Court will grant the motion, in part, and deny it, in part.

BACKGROUND

The Clean Air Act (CAA) authorizes the Environmental Protection Agency (EPA) to establish standards for protecting the public from hazardous air pollutants. 42 U.S.C. § 7412(h)(1). The EPA exercised that authority by promulgating the National Emissions Standard for Hazardous Air Pollutants (NESHAP). Among other things, the NESHAP identifies asbestos as a hazardous air pollutant and establishes "work practice standards" that govern the handling and removal of asbestos. 40 C.F.R. § 61.140–157. The asbestos work practice standards apply to "owners" and "operators" of demolition and renovation activities. § 61.145(a). Under the CAA, failure to comply with the NESHAP is a crime. *See* 42 U.S.C. § 7413(c)(1).

In this case, the United States charges Defendant Brek Pilling with seven counts of violating the CAA. [1] Specifically, the Indictment (Dkt. 1) alleges that he caused the demolition of two buildings in Burley, Idaho, without following the NESHAP work practice standards. Each count of the Indictment corresponds to a separate work practice standard that the defendant allegedly violated. *See Indictment* ¶¶ 8–21, Dkt. 1.

[1] The Court dismissed Count One of the Indictment in a Memorandum Decision and Order entered February 27, 2024. Dkt. 78.

1. The Google Warrant

The government executed at least two search warrants in this case. The first ("the Google Warrant") was signed on November 2, 2021, and served on Google LLC the following day. It authorized a search of two email accounts associated with the defendant: brek66@gmail.com and brek@kodiakamerica.us. [2]

[2] The warrant also authorized a search of a third email account belonging to Brian Tibbets. The search of that account is not at issue here.

In a probable cause affidavit ("the Google Affidavit") attached to the warrant, Special Agent Bryan Byrd provided a basis for the search. First, Agent Byrd reported that two demolition bids had been emailed to brek66@gmail.com before the demolition of the buildings in Burley, Idaho. *Google Warrant*, Dkt. 38, ¶¶ 25–26. And second, after the demolition, the defendant reportedly sent an email from brek@kodiakamerica.us to Brian Tibbets regarding the discovery of asbestos at the demolition site. *Id.* ¶ 39.

Based upon those emails, Agent Byrd concluded that the email accounts likely "contain[ed] emails unknown to the Government regarding the Property, bids for the demolition, asbestos, and other relevant topics." *Id.* ¶ 41. He further explained that "information stored *in connection with an email account*" may show the "who, what, why, when, where, and how" of the alleged criminal conduct. *Id.* ¶ 46 (emphasis added). For example, "user attribution" evidence "may indicate who used or controlled the account at a relevant time." *Id.* Similarly, geographic location data revealing the "physical location associated with the logged IP addresses" may "inculpate or exculpate the account owner" by revealing who used the account on the relevant occasions. *Id.*

Based upon the Google Affidavit, the magistrate judge authorized a search of the defendant's accounts for "evidence, contraband, fruits, and/or instrumentalities of violations" of the Clean Air Act (CAA). *Id.*, Attach. B(II). The warrant only applied to "information from October 1, 2017, ***1119** to June 30, 2018." It also specified the categories of information and records that Google was required to produce, and identified the kinds of materials that the government was authorized to seize.

In December of 2021, Google produced, and the government downloaded, approximately 9.56 gigabytes of compressed data pursuant to the search warrant. The government segregated portions of the data that were presumably privileged and filtered the remaining documents using search terms designed to identify the materials that the government was specifically authorized to seize under Attachment B of the warrant.

2. The Apple Warrant

The government also served a warrant on Apple Inc. ("the Apple Warrant"). The warrant authorized a search of information associated with the defendant's Apple account, mobile phone number, and two Apple IDs (brek66@gmail.com and brek@kodiakamerica.us).

In his probable cause affidavit ("the Apple Affidavit"), Agent Byrd reported that the defendant's iCloud account likely contained evidence of "obstructive" conduct and information related to the defendant's ownership of the demolished buildings. *Apple Warrant* Dkt. 38-1. According to information that Agent Byrd obtained during a proffer session with the defendant's former business partner, Brian Tibbets, the defendant "made calls, sent text messages, or sent email to Tibbets and other relevant parties on or near the date of the first proffer session, as well as on or about June 2, 2018[.]" *Id.* ¶ 52. Mr. Tibbets also told Agent Byrd that he had transferred a recording of his first proffer session to the defendant via AirDrop. *Id.* ¶ 51.

Based upon the Apple Affidavit, the magistrate judge authorized a search of the defendant's Apple account. Attachment A of the warrant described the property to be searched, and Attachment B listed the things to be seized. Attachment B was divided into two subsections. Section I of Attachment B listed the information and records that Apple was required to disclose as to the defendant's accounts, including:

- All records and information "regarding the identification of the account;"
- All records and information about all devices ever associated with the account or used in connection with the account;
- The contents of all emails from October 1, 2017, to present, including drafts and deleted emails;

- The contents of all instant messages from October 1, 2017, to present, including drafts and deleted messages;
- The content of all files stored on the iCloud, including those related to email, photos, document drives, passwords, address books, contact lists, notes, reminders, calendars, images, videos, voicemails, device settings, and bookmarks;
- All activity, connection, and transactional records, including those related to FaceTime, messaging, email, iCloud, iTunes, the AppStore, and the Game Center;
- All records and information related to account access, device location, and services used;
- All records of communication with Apple regarding the account; and
- All files, keys, and information necessary to decrypt the disclosed data.

Section II of Attachment B listed the information and records that the government was authorized to seize, including:

- "All information described in Section I that constitutes fruits, contraband, ***1120** evidence, and instrumentalities of violations of 42 U.S.C. § 7413(c) (Clean Air Act), 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 1505 (obstruction of agency proceedings), and 18 U.S.C. § 1512 (witness tampering and destruction/alteration of evidence);"
- "[I]nformation pertaining to ... Clean Air Act violations, Conspiracy, False Statements, Obstruction, Witness Tampering, and Destruction/Alteration of Evidence;"
- "Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;"
- "Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;"
- "The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);" and
- "The identity of the person(s) who communicated with the user ID about matters relating to the aforementioned violations, including records that help reveal their whereabouts."

In November of 2022, Apple provided, and the government downloaded, approximately 118 gigabytes of data pursuant to the search warrant. In May of 2023, after filtering the data to exclude presumptively privileged results, the prosecution team began to search and review the files. On January 30, 2024, the government realized that it had inadvertently failed to purge the data of files that did not fall within the categories authorized for seizure under Section II of Attachment B. The government did so and was left with 156 responsive documents, nine of which it intends to offer at trial.

3. Motion to Suppress (Dkt. 37)

The defendant filed this motion on January 19, 2024, seeking to suppress all evidence seized pursuant to the Google Warrant and Apple Warrant. Dkt. 37. He argues that both warrants are overbroad and lack particularity in violation of the Fourth Amendment to the United States Constitution.

On February 1, 2024, the government informed the defendant that it had inadvertently failed to conduct the second step of the two-step electronic seizure process authorized by the Apple Warrant. *Def.'s Reply* at 2, Dkt. 54. The defendant addressed that failure in his Reply (Dkt. 54) and the Court allowed the government to file a Surreply (Dkt. 55-1) responding to the defendant's new arguments. *See* Dkt. 56.

The defendant's motion is now fully briefed and ripe for decision. The Court has determined that oral argument and an evidentiary would not aid the decisional process. An evidentiary hearing on a motion to suppress is required only if contested issues of fact going to the validity of the search are in issue. *See* *United States v. Howell*, 231 F.3d 615, 620–21 (9th Cir. 2000); *United States v. Babichenko*, Case No. 1:18-CR-00258-BLW, 2020 WL 4043143, at *1 (D. Idaho July 16, 2020). Here, the defendant challenges the validity of two search warrants on grounds that they are overbroad and lacking particularity. The Court need not resolve any disputed issue of fact to rule on the defendant's motion. Accordingly, an evidentiary hearing was not warranted.

*1121 LEGAL STANDARDS

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

Probable cause is the bedrock of every search warrant. It "means a fair probability that contraband or evidence of a crime will be found in a particular place, based on the totality of circumstances." *United States v. Diaz*, 491 F.3d 1074, 1078 (9th Cir. 2007) (internal quotation marks omitted). In addition to having a basis in probable cause, a warrant must be specific about the place to be searched and the things to seized. "Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." *United States v. Towne*, 997 F.2d 537, 544 (9th Cir. 1993) (internal quotation omitted).

A search warrant is sufficiently particular if it "enable[s] the person conducting the search reasonably to identify the things authorized to be seized." *United States v. Mann*, 389 F.3d 869, 877 (9th Cir. 2004). This principle keeps the government from "seiz[ing] the haystack to look for the needle." *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006). And in doing so, it protects against the "specific evil [of] the 'general warrant' abhorred by the colonists," and dissuades courts from authorizing "general, exploratory rummaging in a person's belongings[.]" *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971).

A search warrant is not overbroad if its scope is supported by probable cause. *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 703 (9th Cir. 2009) ("The search and seizure of large quantities of material is justified if the material is within the scope of the probable cause underlying the warrant.") (quoting *United States v. Hayes*, 794 F.2d 1348, 1355 (9th Cir. 1986)). In determining whether a warrant is overbroad, a court must consider (1) "whether probable cause existed to seize all items of a category described in the warrant," (2) "whether the warrant set forth objective standards by which executing officers could differentiate items subject to seizure from those which were not," and (3) "whether the government could have described the items more particularly in light of the information available." *United States v. Flores*, 802 F.3d 1028, 1044 (9th Cir. 2015) (quoting *United States v. Lei Shi*, 525 F.3d 709, 731–32 (9th Cir. 2008)).

Unique challenges arise when executing search warrants on electronically stored information. That is because "[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents[.]" *Flores*, 802 F.3d at 1044–45 (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176–77 (9th Cir. 2010) (hereinafter "*CDT*")). Given those challenges, the federal rules provide for a two-step process wherein "officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." FED. R. CRIM. P. 41(e)(2)(B) advisory committee note to 2009 amendment. The Ninth Circuit has embraced that two-step approached. *See Flores*, 802 F.3d at 1046; *United States v. Pelayo*, No. 21-30249, 2023 WL 4858147, at *2 n.2 (9th Cir. July 31, 2023); *United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013).

***1122** At the same time, courts have also recognized that the "nature of digital storage" creates "enormous" risks of authorizing "unbridled, exploratory search[es]" of electronically stored data. *United States v. Galpin*, 720 F.3d 436, 446–47 (2d Cir. 2013). Thus, while the Ninth Circuit has acknowledged that the "reality of over-seizing is an inherent part of the electronic search process," it has also emphasized the need for a "greater vigilance on the part of judicial officers" in balancing the needs of law enforcement and the privacy rights of the people. *CDT*, 621 F.3d at 1177; *see also Schesso*, 730 F.3d at 1042 ("[L]aw enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence.").

DISCUSSION

The defendant's motion will be denied to the extent that it challenges the Google Warrant. That warrant is not overbroad and sufficiently describes the place to be searched and the things to be seized. However, the defendant's motion will be granted as to the Apple Warrant, which lacks the degree of particularity required by the Fourth Amendment.

1. The Google Warrant

A. The Google Warrant was not overbroad.

The defendant first argues that the Google Warrant was overbroad. Based on the existence of a few emails, he explains, the government seized information "from every corner of [his] electronic life," including "volumes of other types of information that might be tangentially attached to a digital account[.]" *Def.'s Memo. in Supp.* at 8, Dkt. 37-1. The government responds by noting that the Google Warrant "imposed subject matter, categorical, and temporal limitations," that were reasonable under the circumstances. *Gov.'s Memo. in Opp.* at 10, Dkt. 42. Moreover, the government explains, the "unique challenges" of searching electronic records did not allow for the kind of specificity that the defendant suggests. *Id.* at 9.

In *United States v. Pelayo*, the Ninth Circuit rejected a broadness challenge under similar circumstances. 2023 WL 4858147 at *2.[3] There, as here, a warrant authorized a search of the defendant's iCloud account. *Id.* at *1. Although the warrant required Apple to produce "the entirety of [the defendant's] iCloud account" under step one, "the search and seizure of evidence was limited to the outlined crimes" and the warrant "specified twenty-one types of evidence that the government could seize." *Id.* at *1. Those limitations were adequate to prevent the warrant from becoming a "general warrant" that would "allow the executing officer to rummage through Pelayo's iCloud account without discretion." *Id.*

3 The Ninth Circuit's unpublished decision in *Pelayo* is not precedent. *See* 9th Cir. R. 36-3(a) (citation of unpublished opinions). It is, nevertheless, instructive.

The Google Warrant is similar to the search warrant upheld in *Pelayo*. At the outset, it lists broad categories of data to be disclosed by Google. It then narrows that list in several respects. First, it imposes a temporal limitation, only authorizing a search of information "from October 1, 2017, to June 30, 2018." That date range spans from the time the buildings were allegedly purchased until shortly after the defendant's alleged email communications regarding his engagement with the EPA. Based upon Agent Byrd's representations in the Google Affidavit, the Court concludes this nine-month window was reasonably rooted in the magistrate's probable cause finding. Next, the warrant limits the government to seizing information and records that "constitute[ ] fruits, contraband, ***1123** evidence, and instrumentalities" of violations of the Clean Air Act and 40 C.F.R. § 61.145(a). And finally, the warrant lists eight specific categories of evidence authorized to be seized.

Applying the three factors outlined by the Ninth Circuit in *Lei Shi*, the Court concludes that the Google Warrant was not overbroad. 525 F.3d at 731–32. First, the scope of the search warrant was supported by probable cause. Agent Byrd identified emails passing to and from the Google Accounts in which the defendant collected bids for the destruction of the buildings and communicated with his business partner about his dealings with the EPA. Two of those emails contained file attachments. Based on the defendant's alleged use of the email accounts to communicate about the building demolition and asbestos testing, the magistrate judge properly found probable cause to search the accounts for other emails related to the buildings and the presence of asbestos. Moreover, on that same basis, it was also reasonable to conclude that additional relevant evidence would likely be found within the files associated with the defendant's accounts. *See Google Warrant* ¶¶ 42–46, Dkt. 38. The warrant's scope did not exceed its probable cause foundation.

Second, as further explained below, the warrant established objective standards by which the executing officers could determine which items were subject to seizure. Attachment B tied each category of material to the suspected crime and delineated the kinds of evidence (*e.g.*, "emails or email attachments") authorized to be seized.

Finally, the government could not have been more specific in light of the information available. The defendant argues that the search should have been confined to email communications "between the parties identified by the government in its supporting affidavit." *Def.'s Memo. in Supp.* at 9, Dkt. 37-1. But such a limitation would have created a substantial risk of excluding relevant records; for example, demolition bids provided by other contractors, and communications between the defendant and other business associates about the presence of asbestos at the demolition site. The government limited the scope of the warrant to a

reasonable degree in light of the information upon which the warrant was based.

In sum, the Google Warrant was not overbroad. Its scope was supported by probable cause, described in sufficiently clear terms, and not reasonably susceptible to a greater degree of specificity.

B. The Google Warrant was sufficiently particular.

The Google Warrant was also sufficiently particular because it reasonably identified the place to be searched and the things to be seized. *See* *Mann*, 389 F.3d at 877.

To begin, the defendant argues that the Google Warrant did not "adequately describe the place to be searched." *Def.'s Memo. in Supp.* at 12, Dkt. 37-1. The relevant test is "(1) whether the warrant describes the place to be searched with 'sufficient particularity to enable law enforcement officers to locate and identify the premises with reasonable effort,' and (2) whether any reasonable probability exists that the officers may mistakenly search another premise." *Manriquez v. Ensley*, 46 F.4th 1124, 1129 (9th Cir. 2022) (quoting *United States v. Brobst*, 558 F.3d 982, 992 (9th Cir. 2009)).

The Google Warrant clearly identified the place to be searched:

> **PROPERTY TO BE SEARCHED.** This warrant applies to information from October 1, 2017, to June 30, 2018, associated with btibbets@gmail.com, brek66@gmail.com, and brek@kodiakamerica.us ***1124** that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Google Warrant, Attach. A, Dkt. 38.

That description enabled law enforcement officers to identify the place to be searched with "reasonable effort" and created little or no risk that the wrong place would be mistakenly searched. *Manriquez*, 46 F.4th at 1129; *see also Pelayo*, 2023 WL 4858147 at *2 (rejecting argument that an "iCloud account" was "too broad a place to be searched").

Next, the defendant argues that the Google Warrant lacked particularity because did not "specify how the items to be seized related to the designated crimes." *Def.'s Memo. in Supp.* at 12, Dkt. 37-1. As discussed above, the Google Warrant did describe the items to be seized with reasonable specificity. First, it only authorized the seizure of items that constituted "fruits, contraband, evidence, and instrumentalities of violations" of the Clean Air Act and/or 40 C.F.R. § 61.145(a). Second, it further limited what could be seized by listing eight specific categories of information and records. *See Pelayo*, 2023 WL 4858147 at *1 (rejecting particularity challenge because "the search and seizure of evidence was limited to the outlined crimes and specified twenty-one types of evidence that the government could seize"). Each category description specified how the items to be seized related to the alleged crime.[4] For example, the warrant authorized the seizure of any "emails or email attachments *related to the purchase or ownership of the property/buildings* located at 1222 and 1226 Overland Avenue in Burley, Idaho, including but not limited to contracts, deeds, tax records, and sales/purchase records." *Google Warrant*, Attach. B(II)(c), Dkt. 38 (emphasis added). That description is "reasonably specific" and "clearly state[s] what is sought." *Towne*, 997 F.2d at 544.

4 The one exception is found in paragraph (h) of Attachment B(II). That portion authorized the seizure of information related to the "identity of the person(s) who created or used the email account and associated ID, including records that help reveal the whereabouts of such person(s)." Although that paragraph did not specifically reference the alleged crime, it is nevertheless sufficiently clear as to the kind of data to be seized.

In sum, the Google Warrant was not overbroad and it contained sufficient particularity to satisfy the Fourth Amendment. The defendant's request to suppress evidence obtained pursuant to the Google Warrant will therefore be denied.

2. The Apple Warrant

The defendant next argues that the Apple Warrant was overbroad, lacked particularity, and was executed improperly.

The Court agrees that the warrant did not adequately describe the things authorized to be seized. Moreover, the government's failure to purge the data within a reasonable time violated the defendant's Fourth Amendment rights. Evidence obtained pursuant to the warrant will therefore be suppressed. [5]

5 The Court grants the defendant's motion based upon the warrant's lack of particularity and the government's delay in purging the data obtained from Apple. Accordingly, this Order does not address the defendant's additional argument related to overbroadness.

A. The Apple Warrant failed to particularly describe the things authorized to be seized.

The Apple Warrant authorized a search of the defendant's entire iCloud account for "fruits, contraband, evidence, and instrumentalities of violations" of five statutes. While the supporting affidavit ***1125** detailed the facts and circumstances underlying the magistrate's probable cause finding, it is unclear whether the affidavit accompanied or was incorporated into the warrant itself. [6] Consequently, the warrant provided almost no guidance as to what things the government was authorized to seize. In doing so, it violated the Fourth Amendment.

6 After carefully reviewing the warrant and probable cause affidavit, the warrant makes only a passing reference to the affidavit, and the Court has found no indication that the affidavit accompanied the warrant at the time of execution.

At its core, the particularity requirement of the Fourth Amendment means that a warrant must be "specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized." *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). Naturally, the degree of specificity required "varies depending on the circumstances of the case and the type of items involved." *Id.* Sometimes, it is simply impossible to use more than "generic descriptions" of the items likely to be found during a search. *Id.* Still, the Ninth Circuit has marked a cautious path when dealing with warrants that use generic descriptions and rely merely on references to the laws suspected of having been violated. *See* *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) ("As we noted before, 'limiting' the search to only records that are evidence of the violation of a certain statute is generally not enough.").

The Ninth Circuit considered a challenge to the particularity of a search warrant in *United States v. Spilotro*, 800 F.2d at 963. There, a search warrant was issued against individuals suspected of engaging in unlawful loan sharking and gambling activities. *Id.* at 961. The warrant authorized law enforcement to search the defendants' stores and seize "address books, notebooks, notes, documents, records, assets, photographs, and other items and paraphernalia evidencing violations of the multiple criminal statutes listed." *Id.* at 964. The warrant failed, however, to indicate the "precise identity, type, or contents of the records sought." *Id.* The court held that the warrant lacked sufficient particularity because it authorized the "wholesale seizure[ ] of entire categories of items" and "provide[d] no guidelines to distinguish items used lawfully from those the government had probable cause to seize." *Id.* The only limitation was the warrant's reference to the laws that the defendants were suspected of violating. But that reference alone did not provide sufficient guidance to satisfy the Fourth Amendment's standard of particularity.

The government urged the court to read the warrant "in light of the [supporting] affidavit," which "exhibit[ed] the required degree of specificity." *Id.* at 967. The court refused. "We are unable," it explained, "to rely on the affidavit to cure the generality of the warrants ... since it was not attached to and incorporated by reference in the warrants as required by this court's decision in *United States v. Hillyard*, 677 F.2d 1336, 1340 (9th Cir. 1982)." *Id.*

In another case, the Ninth Circuit distinguished *Spilotro* and rejected a defendant's particularity challenge. *United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006). There, a warrant authorized a search of the defendant, his vehicle, and his residence, for evidence of extortion. *Id.* at 1144. The warrant specified the kinds of things to be seized, including "records, documents and materials which reflect communications with" particular individuals, and "any and all evidence of travel, including hotel bills and receipts, gasoline receipts, ... or any other documents related to travel from January 8, 2004 to present." *Id.* The court

distinguished the warrant ***1126** from the one challenged in *Spilotro* and found that it contained "adequate specificity and sufficiently restricted the discretion of agents executing the warrant." *Id.* at 1148. Further, unlike in *Spilotro*, the "extensive 24–page supporting affidavit describ[ing] the extortion scheme in detail" was attached to the warrant. *Id.* at 1145. The warrant was sufficiently particular because it "provided a specific ... list of possible documents that fell within this category and temporally restricted the breadth of the search." *Id.* at 1148; *see also* *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003) (rejecting particularity challenge "[b]ecause the police were on notice that they could only search the computer for the items listed in the warrant, all of which were detailed and specific[.]"). "Moreover, the extensive statement of probable cause in the affidavit detailed the alleged crime and Adjani's unlawful scheme." *Id.* at 1149.

The Apple Warrant resembles the warrant invalidated in *Spilotro* in two important respects. First, the Apple Warrant itself did not provide any real guidance for the executing officer to determine what kinds of information and records may be seized. Instead, it broadly authorized a search of the defendant's entire iCloud account for information or records that "constitute[ ] fruits, contraband, evidence, and instrumentalities of violations" of five statutes. *Apple Warrant*, Attach. B, Dkt. 38-1. Unlike the warrant upheld in *Adjani*, the Apple Warrant did not state the identity and "nature of the items to be seized." *Adjani*, 452 F.3d at 1148. Nor did it describe, in *any* detail, "the items one commonly expects to find on premises used for the criminal activities in question." *Id.* at 1149. [7] There is ample case law in this circuit demonstrating that a search warrant's bare reference to 'evidence of a violation of' a certain statute is generally insufficient to satisfy the particularity requirement. *See* *United States v. Clark*, 31 F.3d 831, 836 (9th Cir. 1994) ("[T]he catchall phrase authorizing seizure of 'fruits and instrumentalities of [a] violation of' 21 U.S.C. § 841(a)(1) did not adequately describe the items to be seized."); *Cardwell*, 680 F.2d at 77–78 (finding insufficiently particular a warrant authorizing a search for "fruits and instrumentalities, of violations of Title 26, U.S.C. § 7201"); *see also* *United States v. Crozier*, 777 F.2d 1376, 1381 (9th Cir. 1985). [8]

7 To be clear, Section I of Attachment B did list many categories of information, such as emails and text message. But those were categories of data that Apple was required to disclose under step one of the two-step process. At step two, that data was to be searched for items falling within Section II of Attachment B.

8 "Other circuits agree that a warrant's 'reference to a broad federal statute is not a sufficient limitation on a search warrant.' " *United States v. Mokbel*, No. H-21-103-1, 2021 WL 4554660, at *4 (S.D. Tex. Oct. 5, 2021) (collecting cases)

Second, the supporting affidavit apparently did not accompany the Apple Warrant at the time of execution. Consequently, as in *Spilotro*, the significant detail set out by Agent Byrd cannot "cure the generality of the warrant[ ]." *Spilotro*, 800 F.2d at 967; *see also* *SDI*, 568 F.3d at 699 ("We consider an affidavit to be part of a warrant, and therefore potentially curative of any defects, only if (1) the warrant expressly incorporated the affidavit by reference and (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search.") (internal citations and quotations omitted). Viewed on its own, without the context provided in the affidavit, the Apple Warrant simply cannot satisfy the Fourth Amendment's particularity requirement. *See* ***1127** *Groh v. Ramirez*, 540 U.S. 551, 557, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004) ("The fact that the application adequately described the 'things to be seized' does not save the warrant from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents.").

The government claims it could not have provided more detailed descriptions of the items to be seized, given the unique challenges of searching electronically stored data. The Court disagrees. The warrant could have been more specific in several ways. First and foremost, the government could have incorporated the supporting affidavit and ensured that it accompanied the warrant at the time of execution. Doing so would have substantially increased the degree of guidance for the warrant's execution. The warrant also could have described the kinds of things authorized to be

seized, such as emails and text messages related to the buildings or the EPA. *Spilotro*, 800 F.2d at 964 ("[T]he government could have narrowed most of the descriptions in the warrants either by describing in greater detail the items one commonly expects to find on premises used for the criminal activities in question[.]"). Instead, the warrant simply punted to the executing officer, allowing that person to scour the defendant's entire iCloud account for "information pertaining" to the suspected criminal activity.

The warrant's reference to five criminal statutes did not add a sufficient dose of particularity to save the warrant. It is true that references to suspected crimes are relevant to —and sometimes sufficient to establish—particularity. *See id.* ("Reference to a specific illegal activity can, in appropriate cases, provide substantive guidance for the officer's exercise of discretion in executing the warrant."). But the Apple Warrant merely listed five broad statutes. [9] Beyond including parenthetical labels, the warrant provided no further guidance. Moreover, those criminal statutes were not specific enough to impose adequate "inherent guidelines," as is true when the suspected crime is highly specific. *See, e.g.*, *United States v. LeBron*, 729 F.2d 533, 538–39 (8th Cir. 1984) (noting that a reference to "specific illegal activity" like narcotic sales would provide a "particularized description and inherent guidelines"); *United States v. Hay*, 231 F.3d 630, 636–38 (9th Cir. 2000) (rejecting particularity challenge because limitation of the search to evidence of child pornography was "sufficiently specific"). Instead, the listed statutes were of "exceptional scope" and provided little guidance of their own. *Spilotro*, 800 F.2d at 965.

9 The warranted listed the following statutes: "42 U.S.C. § 7413(c) (Clean Air Act), 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 1505 (obstruction of agency proceedings), and 18 U.S.C. § 1512 (witness tampering and destruction/alteration of evidence)." *Apple Warrant*, Attach. B(II).

The outcome may have been different if Agent Byrd's affidavit had been incorporated into and accompanied the Apple Warrant. [10] That is, the warrant's instruction to search for evidence of violations of the five statutes would probably be sufficiently particular if *combined* with the information set forth in the affidavit. Without that information, however, the executing officer was left with no way of determining what constituted evidence of, say, "conspiracy to defraud the United States," or "obstruction of agency proceedings."

10 It is at least arguable that the language in the Apple Warrant was sufficient to establish incorporation by reference. *See United States v. Vesikuru*, 314 F.3d 1116, 1120 (9th Cir. 2002). But, even so, there is no indication that the affidavit accompanied the warrant at the time of execution.

***1128** In sum, the Apple Warrant authorized a search of vast swaths of data but failed to particularly identify the things to be seized. That gave the executing officer near total discretion to rummage through the defendant's iCloud account and seize anything that appeared to be "fruits, contraband, evidence, and instrumentalities" of the suspected crimes. The Fourth Amendment demands more.

B. The good faith exception does not apply.

In *United States v. Leon*, the United States Supreme Court held that "evidence obtained pursuant to a facially-valid search warrant later found to be invalid is admissible if the executing officers acted in good faith and in objectively reasonable reliance on the warrant." *Spilotro*, 800 F.2d at 968 (citing *United States v. Leon*, 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)). However, the Court noted that there may be instances where a warrant is "so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923, 104 S.Ct. 3405; *see also United States v. Crews*, 502 F.3d 1130, 1136 (9th Cir. 2007) ("[R]eliance is per se unreasonable ... where the warrant is facially deficient in detail as to the place to be searched or the things to be found that the officers could not reasonably presume it to be valid[.]").

The Ninth Circuit has applied the good faith exception where the government showed that an unattached, unincorporated probable cause affidavit actually limited the search. In *United States v. Luk*, the court affirmed a district court's application of the good faith exception to deny a suppression motion. 859 F.2d 667, 678 (9th Cir. 1988). The search

warrant there was "constitutionally defective for lack of particularity" because the "affidavit was not expressly incorporated into the warrant by reference." *Id.* at 676. As the court explained, however, that did "not preclude the use of the executing officers' reliance upon the affidavit as evidence of their reasonable reliance on the validity of the warrant or their good faith." *Id.* at 676–77. Indeed, the district court had found that "the agents specifically relied on the affidavit" and "acted in good faith by limiting their search to items ... described in the affidavit." *Id.* at 677.

To invoke the good faith exception in this context, the government must show that the individuals who executed the warrant "actually relied on the affidavit." *SDI*, 568 F.3d at 706; *see* *United States v. Kow*, 58 F.3d 423, 429 (9th Cir. 1995) (refusing to apply good faith exception absent evidence that the executing officers "actually relied on the information in the affidavit to limit the warrant's overbreadth"). Here, the government merely referenced the good faith exception in a footnote. Although the Court will not deem the argument waived, the government certainly has not carried its burden of showing that the exception applies in this case.

C. The doctrine of severance does not apply.

The Ninth Circuit has "embraced the doctrine of severance," which allows a court "to strike from a warrant those portions that are invalid and preserve those portions that satisfy the Fourth Amendment. Only those articles seized pursuant to the invalid portions need be suppressed." *Flores*, 802 F.3d at 1045 (quoting *United States v. Gomez–Soto*, 723 F.2d 649, 654 (9th Cir. 1984)).

In an exhibit attached to its Surreply, the government identified the nine items of evidence obtained pursuant to the Apple Warrant that it intends to offer at trial. Dkt. 55-2. To the extent the Court invalidates the Apple Warrant, the government ***1129** asks that the invalid portions of the warrant be severed from the valid portions and that the nine text messages be admitted under the doctrine of severance.

But the doctrine of severance cannot be applied to the Apple Warrant under the circumstances. Severance is only appropriate as to "identifiable portions of [a] warrant" where it is "feasible to excise" the problematic portions from the valid ones. *U.S. v. Sears*, 411 F.3d 1124, 1130 (9th Cir. 2005); *see also* *United States v. Barnes*, 749 F. Supp. 2d 1124, 1134–35 (D. Idaho 2010). Courts must also consider "the relative size of the valid and invalid portions of the warrant"—severance is not appropriate where only a "relatively insignificant" portion of the warrant is valid. *Sears*, 411 F.3d at 1131.

Here, the nine text messages sought to be introduced appear to have been obtained under the language of the warrant authorizing the seizure of "fruits, contraband, evidence, and instrumentalities" of violations of the suspected crimes. *Apple Warrant*, Attach. B(II), Dkt. 38-1. That is the same language the Court finds lacking in particularity. Moreover, even if the text-message portion of the warrant could be severed, that portion would be relatively insignificant compared with the vast scope of the warrant. In sum, severance does not apply here, and the evidence obtained pursuant to the Apple Warrant must be suppressed.

D. Suppression is also justified because the government did not filter unresponsive data before reviewing the defendant's entire iCloud account.

There is another, independent basis for suppressing the evidence obtained pursuant to the Apple Warrant. Namely, members of the prosecution team performed a months-long review of the defendant's entire iCloud account before excluding the information and records not authorized to be seized. The government insists that its failure to conduct this second step of the process outlined in the warrant was "inadvertent." *See* Dkt. 55-1. That may be. But, under the circumstances, the Court need not—and does not—make a factual finding to that effect. Even if the government did not intentionally violate the terms of the warrant, its detailed review of the defendant's entire iCloud account over the course of nearly nine months plainly violated the defendant's Fourth Amendment rights.

To be sure, Fourth Amendment violations do not always require application of the exclusionary rule. *See* *Hudson v. Michigan*, 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006). The judicially created exclusionary rule is "a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation." *Davis v. United States*, 564 U.S. 229, 236, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011). It is not, however, " 'a personal constitutional right,' nor is it designed to 'redress the injury'

occasioned by an unconstitutional search." *Id.* (quoting *Stone v. Powell*, 428 U.S. 465, 486, 96 S.Ct. 3037, 49 L.Ed.2d 1067 (1976)).

The government correctly notes that there is no "established upper limit as to when the government must review the seized electronic data[.]" *Gov.'s Surreply* at 4, Dkt. 55-1. But here, we are not dealing with a mere passage of time. The government engaged in a months-long review of the defendant's entire iCloud account before removing unresponsive data. During that process, at least one member of the prosecution team reviewed all 1,248 files that Apple had produced under step-one of the warrant, despite the fact that only 156 of those materials fell within the scope of the seizure authorized by the ***1130** warrant. If the government is to be given the latitude of the two-step process for seizing electronic data, it is absolutely essential that it performs the second step within a reasonable time, and in any case, before it reviews the data.

In sum, even if the warrant had not lacked particularity, the Court would likely suppress government's evidence on this independent ground.

ORDER

IT IS ORDERED that Defendant Brek Pilling's Motion to Suppress (Dkt. 37) is **GRANTED, in part, and DENIED, in part**, as follows:

1. The motion is **GRANTED** as to evidence obtained pursuant to the Apple Warrant; and

2. The motion is **DENIED** as to evidence obtained pursuant to the Google Warrant.

All Citations

721 F.Supp.3d 1113

End of Document