IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF ARKANSAS
[redacted] DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CASE NUMBER:** [redacted]
	)	
[redacted]	)	

DEFENDANT'S MOTION TO SUPPRESS AND BRIEF IN SUPPORT

Comes now the defendant, [redacted] by and through undersigned counsel, and, pursuant to Federal Rule of Criminal Procedure 12(b)(3)(C), respectfully requests the Court issue an order suppressing the contents of Google account associated with the email address "[redacted]@gmail.com" that was taken in violation of the Fourth Amendment to the United States Constitution, and for his motion states:

BACKGROUND

Mr. [redacted] is charged in a two-count indictment with transportation of child pornography in violation of 18 U.S.C. §§ 2252A(a)(1) and (b)(1), and possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). Trial in this matter is set for [redacted] 2023. Mr. [redacted] was arrested on [redacted] 2022, and has been detained since that time.

FACTS

On [redacted] 2021, special agent [redacted] sought a search warrant for the contents of Google account associated with the email address "[redacted]@gmail.com." This warrant sought to seize the entire Google account[1], despite the fact that special agent [redacted] only

[1] Although Google does offer products and services beyond those named in the warrant that can be connected to a Google account, Mr. [redacted] has either never activated or used any of those products or services. In fact, he has never activated or used many of the products the government sought to search in this case, including, for example: Google Pay, Google Wallet, Duo, Hangouts, or Meet.

provided probable cause to believe that evidence of a crime existed in the Google Drive and Google Photos portions of that account.

Google provides customers a vast array of services. These services include things like: email("Gmail"), an address book("Contacts"), appointment book("Calendar"), direct messaging services ("Duo" "Messages" "Hangouts" "Meet" and "Chat"), cloud storage ("Google Drive"), photo and video storage and editing ("Google Photo"), a payment system ("Google Pay") among a host of others.[2] *See also Affidavit in Support of An Application for a Search Warrant, IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT* [redacted]*@gmail.com' THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC, GOOGLEPAYMENT CORPORATION, AND/OR ANY PARENT OR SUBSIDIARY ENTITY THEREOF*, [redacted] ¶ 10-26, (filed [redacted]) (hereinafter "the Google Warrant Affidavit"). Google stores all the data from these services in a manner that allows users and law enforcement to access all or just a portion of the data.[3] In other words, if one wishes to obtain all of the account data or simply a portion (e.g., only Google Photos or only Google Drive) they may easily do so. *Id.*

To combat child sexual abuse material (hereinafter "CSAM") Google uses a proprietary technology called "CSAI match" to scan users accounts for hash values[4] of known CSAM.[5] Google

[2] *Google Products*, https://about.google/intl/ALL_us/products/ (last visited June 14, 2023).
[3] *How to Download Your Google Data*, https://support.google.com/accounts/answer/3024190?hl=en (last visited June 14, 2023); *see also*, https://www.youtube.com/watch?v=MeKKHxcJfh0 (last visited June 14, 2023).
[4] A hash value is unique digital signature. Susan Jasper, How we Detect Remove and Report Child Sexual Abuse Material, https://blog.google/technology/safety-security/how-we-detect-remove-and-report-child-sexual-abuse-material/ (last visited June 14, 2023).
[5] Kristie Canagallo, *Our Efforts to Fight Child Sexual Abuse Online*, https://blog.google/technology/safety-security/our-efforts-fight-child-sexual-abuse-online/ (last visited June 14, 2023); *see also Protect Your Content and Online Community From Child Exploitation Videos*, https://www.youtube.com/csai-match/ (last visited June 14, 2023).

also uses artificial intelligence to identify CSAM that has yet to be positively identified as CSAM.[6] Once the potential CSAM, or a portion of it, has been viewed by a human, Google reports the CSAM to the National Center for Missing and Exploited Children (hereinafter "NCMEC") through their CyberTipline. *See e.g. CyberTipline Report No.'s*, [redacted] These CyberTipline Reports indicate which portion of the Google account is storing the potential CSAM (i.e. Google Photos, Google Drive, Google Docs, Gmail, etc.). *See id.* at § A. It also provides filename and an MD5 hash value for each and every image it identifies as potential CSAM. *See id.*

Here, Google submitted Four CyberTipline Reports: [redacted] and [redacted] *Id.* Each report provided the hash values and filenames for each contraband item. In every report a section titled "Additional Information Submitted by the Reporting ESP" identified the place where the CSAM was located as either Google Photos infrastructure, Google Drive infrastructure, or both. *Id.* No CSAM was found in any other portions of the account (i.e. Gmail, Contacts, Calendar, Duo, Messages, Hangouts, Meet or Chat etc.) despite the fact that those services, if enabled, are subject to the same scanning for known and potential CSAM.

Even though the NCMEC Cybertips provided hash values for known CSAM and described the location of those images within the Google infrastructure, special agent [redacted] drafted a warrant seeking to seize the entire contents of the Google account. *See Search Warrant, IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT* [redacted]*@gmail.com' THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC, GOOGLEPAYMENT CORPORATION, AND/OR ANY PARENT OR*

[6] Nikola Todorovic, Abhi Chaudhuri, *Using AI to Help Organizations Detect and Report Child Sexual Abuse Material Online*, https://blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/ (last visited June 14, 2023); *see also Discovery Our Child Safety Toolkit*, https://protectingchildren.google/tools-for-partners/ (last visited June 14, 2023).

SUBSIDIARY ENTITY THEREOF, [redacted] *Attachment B*, at ¶ I ([redacted)

(hereinafter "the Google Warrant"). Specifically, the Google Warrant authorized a seizure of thirteen broad categories of information "from [redacted] 2021, though the present, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account(s), including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and duration, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or. instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and
8. Change history.

b. All device information associated with the Account(s), including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs;

d. The contents of all emails associated with the Account(s), including Stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;

e. Any records pertaining to the Account(s) contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;

f. Any records pertaining to the Account(s) calendar(s), including: Google Calendar

events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;

g. The contents of all text, audio, and video messages associated with the Account(s), including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history;

h. The contents of all records associated with the Account(s) in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

i. The contents of all media associated with the Account(s) in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the Account(s), including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs~ and IP addresses;

j. All maps data associated with the Account(s), including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

k. All Location History and Web & App Activity indicating the location at which the Account(s) was/were active including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and associated logs and user settings, including Timeline access logs and change and deletion history;

l. All payment and transaction data associated with the Account(s), such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time· stamp, location data, and change history; and

m. All Internet search and browsing history, and application usage history, for the Account(s), including Web & App Activity; browsing history, including· application usage; bookmarks passwords; autofill information; alerts, subscriptions, and other automated searches" including associated notifications

and creation dates; user settings; and all associated. logs and change history."
Id. at, ¶ I.

Furthermore, the warrant authorized a subsequent search and seizure of the following items:

"a. Evidence relating to the transportation, receipt, distribution, possession of, or access with intent to view, child pornography, as that term is defined in Title 18, United States Code, Section 2256(8), by any person;
b. Evidence indicating how and when the 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;
c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;
d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s)."
Id. at ¶ II.

Although the Google Warrant Affidavit mentions, in passing, that the contraband was found in Google Photos and Google Drive it completely omits that it was not found in any other location within the Google infrastructure. *See the Google Warrant Affidavit*, at ¶ 5, 9, 29. Furthermore, while it provides sixteen paragraphs regarding the various services within the Google infrastructure, nowhere does it mention that the government need not seize the entire account to access Google Drive, Google Photos, or even account subscriber information. *See the Google Warrant Affidavit*, at ¶ 10-26. Similarly, nowhere does the affidavit explain how hash values can be used to immediately and quickly search for and find previously identified contraband. Instead, the Google Warrant Affidavit intentionally obfuscates the manner in which Google retains data within its infrastructure and argues the entire account is necessary to prove "user attribution" demonstrate "state of mind" and because such a seizure "may lead to the discovery of additional evidence." *Id.* at 30-34.

LAW, ANALYSIS, & ARGUMENT

The Fourth Amendment's Warrants Clause provides that, "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. The clause was intended as a bulwark against "the 'general warrant' abhorred by the colonists" and protects against "a general, exploratory rummaging in a person's belongings." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Its overarching purpose is to ensure that "those searches deemed necessary should be as limited as possible." *Id*.

"To achieve its goal, the Warrants Clause requires particularity and forbids overbreadth. Particularity is the requirement that the warrant must clearly state what is sought." *United States v. Cioffi*, 668 F.Supp.2d 385, 390 (E.D.N.Y 2009) (citations and quotation marks omitted). The particularity requirement "prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). "Breadth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based. Thus… a warrant can violate the clause "either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries. *Cioffi*, 668 F.Supp.2d 390 (citations and quotation marks omitted).

In determining the standard of particularity required in a search warrant "[o]ne of the crucial factors to be considered is the information available to the government. 'generic classifications in a warrant are acceptable only when a more precise description is not possible.'" *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) (citations omitted). Put differently the government must describe the items to be seized "with as much specificity as the government's

knowledge and circumstances allow." *United States v. Riccardi*, 405 F.3d 852, 863 (10th Cir. 2005). The degree of precision concerning records requested in a warrant necessarily must vary with the type of items, the nature of the operation, and the circumstances of the case. *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988). When the government can describe the items they are searching for with greater particularity—they must do so. *See United States v. Bright*, 630 F2d 804 (5th Cir. 1980); *see also United States v. Galpin*, 720 F.3d 436 (2d Cir 2013) ("a failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspects privacy and property are no more than absolutely necessary.") *citing United States v. George*, 975 F.2d 72, 76 (2d Cir.1992); *c.f. United States v. Lacey*, 119 F.3d 742 (9th Cir. 1997) (where "no more specific description of the computer equipment sought was possible," because the agents, "did not know whether the images were stored on the hard drive or on one or more [of the defendant's] many computer disks.").

I. The Warrant Was Overbroad as to What the Government Could Seize from Google (Step One)

Here, despite knowing exactly what contraband they were looking for (images identified by NCMEC CyberTips) and where in the Google infrastructure they would be located (Google Drive and Google Photos), the government requested a form of "all data" warrant to seize 13 broad categories of data comprising everything related to the target Google account for government review. The warrant was therefore overbroad as to the evidence to be seized by the government from Google.

In the past, some courts have allowed two-tiered "all data" warrants allowing the initial seizure of all data related to an online account to be followed by an ostensibly more targeted search.

See e.g. United States v. Taylor, 764 F.Supp.2d 230, 232, 237 (D.Me.2011) (upholding search of "all information associated with an identified Microsoft hotmail account"); *United States v. Bowen*, 689 F.Supp.2d 675, 682 (S.D.N.Y.2010) (Fourth Amendment does not require authorities to "ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching"); *In re Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc*., 25 F. Supp. 3d 1, 6-7 (D. D.C. 2014), vacated, 13 F. Supp. 3d 157 (D. D. C. 2014). The reasoning in these cases is that only, "an agent steeped in the investigation could recognize the significance of particular language in emails…" while, "an employee of the email host would be incapable of doing so." *In the Matter of a Warrant for All Content and Other Info. Associated with the Email Account xxxxxxxgmail.com Maintained at Premises Controlled by Google, Inc.,* 33 F.Supp.3d 386 (S.D.N.Y. 2014). Similarly, these cases posit that "'over-seizing' is an accepted reality in electronic searching because '[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents.'" *Matter of Search of Information Associated With Four Redacted Gmail Accounts*, 371 F.Supp.3d 843, 845 (D. Oregon 2018) (*citing United States v. Flores*, 802 F.3d 1028, 1044-45 (9th Cir. 2015)).

However, courts now recognize that this "seize first, search later approach" should be limited to those situations where the third-party is incapable of providing a more targeted subset of data for the government to review. *See id.* (rejecting a warrant as overbroad because the "accepted reality" of over-seizing "has evolved"); *see also United States v. Blake*, 868 F.3d 960, 974 (11th Cir. 2017) (requiring breadth and particularity in the initial seizure from the internet service providers as well as the subsequent search and seizure of that data); *United States v. Mercery*, 591 F.Supp.3d 1369 (M.D. Ga. 2022) (same but finding the good faith doctrine

inapplicable in the wake of the *Blake* decision); *United States v. Shipp,* 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019); *State v. Hamilton*, No. 6:18-CR-57-REW-10, 2019 WL 4455997 (E.D. Ky. August 30, 2019) (where probable cause existed for Facebook messages a warrant information related to fifteen categories of Facebook data, many of which were broken down into additional categories was overbroad despite a temporal limitation); *United States v. Chavez,* 423 F.Supp.3d 194 (W.D.N.C. 2019).

In this case the government knew exactly what they were looking for and where it would be located. Google, through NCMEC, provided the government with a list of contraband images and associated hash values as well as a description of where in the Google infrastructure they were located (Google Drive and Google Photos). Furthermore, the government knew that because of the way Google's technology works, contraband was unlikely to be found in other locations within the account. Therefore, the government could have, and should have, described the known contraband images by the file names and the associated hash values in the actual warrant and restricted the initial seizure to those items. At a bare minimum the government should have restricted the scope of the seizure to Google Drive and Google Photos within the target account.

In *United States v. Blake*, the 11th Circuit examined the issue of "over-seizure" of data in relation to two warrants served on internet service providers in a child sex trafficking case—one for Facebook and another for Microsoft. *Blake*, 868 F.3d at 960. The court found that the Microsoft warrant was sufficiently particular and not overly broad because it "did not seek all emails in those two email accounts; instead, it was limited to certain categories of emails in them that were linked to the sex trafficking charges against [the two defendants]. For example, the warrant required Microsoft to turn over all '[e]mails, correspondence, and contact information for Backpage.com' and all '[e]mails and correspondence from online adult services websites' that were contained

within the two email accounts.'" *Id.* at 966. These provisions, "limited the emails to be turned over to the government, ensuring that only those that had the potential to contain incriminating evidence would be disclosed… and "prevented 'a general, exploratory rummaging' through [the defendant's] email correspondence." *Id.* at 973. On the other hand, the 11th Circuit found "[t]he Facebook warrants are another matter. They required disclosure to the government of virtually every kind of data that could be found in a social media account… And unnecessarily so. With respect to private instant messages, for example, the warrants could have limited the request to messages sent to or from persons suspected at that time of being prostitutes or customers. And the warrants should have requested data only from the period of time during which [the defendant] was suspected of taking part in the prostitution conspiracy." *Id.* at 974. The court also rejected the government's comparison of social media accounts to electronic device searches, explaining "[t]he means of hiding evidence on a hard drive—obscure folders, misnamed files, encrypted data—are not currently possible in the context of a Facebook account. Hard drive searches require time-consuming electronic forensic investigation with special equipment, and conducting that kind of search in the defendant's home would be impractical, if not impossible. By contrast, when it comes to Facebook account searches, the government need only send a request with the specific data sought and Facebook will respond with precisely that data." *Id.*

The same is true of the data stored by Google in this case. *See Four Redacted Gmail Accounts*, 371 F.Supp.3d at 845 (noting the "accepted reality" of over-seizing "has evolved"). Google was capable of quickly and easily limiting the data turned over to what the government had probable cause to seize—the contraband images located in Google Drive and Google Images. However, the government instead named 13 broad categories of data to be turned over by Google. Therefore, the warrant was overbroad as to what was to be seized from (or turned over by) Google.

Furthermore, the fact that the government included a "indicia of ownership" clause does not obviate the problems raised by *Blake* and the other cases holding over-seizure of data unconstitutional. *See infra* § II. B. This argument has already been rejected by multiple courts. *See id.* While the government may be "entitled to search for this information to a reasonable extent; for example, the registered user, email addresses, birth date, telephone number, physical address, and IP addresses associated with the account are likely to show ownership and control of the account… [t]he breadth of information the search warrant required [Google] to disclose… [in this case] amounted to "a general, exploratory rummaging" in [the defendant's] digital life that did not comport with the particularity requirement of the Fourth Amendment." *State v. Hamilton*, No. 6:18-CR-57-REW-10, 2019 WL 4455997 at *5 (E.D. Ky. August 30, 2019).

II. The Warrant Was Overbroad and Insufficiently Particular as to What the Government Could Search for and Seize (Step Two).

In addition to being overbroad as to the data to be seized from Google, the warrant was insufficiently particularized and overbroad as to what was to be searched for and seized by the government in their subsequent examination of that data. Again, the government had probable cause to believe that a known number of images would be found in Google Drive and Google Images. However, Attachment B allowed the government to search for any "evidence relating to… United States Code, Section 2256(8), by any person… [e]vidence indicating how and when the account was used… [e]vidence indicating the Account owner's state of mind…" and "[t]he identity of the person(s) who created or used the Account…" *The Google Warrant*, Attachment B § II a.-d. Not only does this language fail to restrict what the officers executing the search should seize, it explicitly authorizes a search for evidence they do not have probable cause to believe exists.

A. Paragraph a. Is Overbroad.

Paragraph a. allows the search for any "evidence of United States Code, Section 2256(8), by any person…." *The Google Warrant*, Attachment B § II a. However, the government only had probable cause to search for the CSAM that they named in their affidavit. Google scanned the entirety of the target account using its proprietary technology called "CSAI match" for hash values of known CSAM and using artificial intelligence to identify CSAM that had yet to be positively identified as such. Therefore, the government knew not only where the contraband was, but that no other contraband was likely to be found (because Google had already searched for it and recovered nothing). So, the warrant should have limited the search to the filenames and associated hash values of that contraband. Therefore, paragraph a. is overbroad.

B. Paragraphs .b Through .d Are Insufficiently Particular.

Paragraphs .b through .d are insufficiently particular because they do not identify what out of the vast account data indicates "how and when the Account was accessed or used" the account owner's "state of mind" or "identity" of the user or owner. *The Google Warrant*, Attachment B §§ II b.-d. Those categories are so broad and amorphas they allow a seizure of literally anything found in the target account.

Paragraph .b if read restrictively could mean that the account data can be searched for IP logs and location history data. However, if read permissively it could include every email photograph, private message, call log, calendar note, internet search, or keystroke. Each of these data points provides some "geographic and chronological context." The wording leaves it open to the discretion of the executing officer what data to search for or seize at this step. This is a fundamental violation of the particularity clause. *See Marron,* 275 U.S. at 196.

Paragraphs c. and d. are even more offensive to the particularity requirement than paragraph b. Warrants allowing for searches of "indicia of ownership" have already been rejected by courts across the country because they turn an otherwise valid warrant into a general warrant. *See State v. Bock*, 310 Or.App. 329 (Ct. Ap. Or. 2021); *People v. Coke*, 461 P.3d 508 (Colo. Sup. Ct. 2020); *Hamilton*, 2019 WL 4455997; *see also People v Herrera*, 357 P.3d 1227 (Colo. Sup. Ct. 2015) (rejecting the use of such clauses to justify broad searches); *United States v. Ford*, 184 F.3d 566, 586 (6th Cir. 1999) (rejecting the use of similar clauses that would potentially allow limitless seizures of financial information).

In *Bock*, the Oregon Court of Appeals suppressed evidence recovered from a cell phone in part because of a clause allowing the government to search for "[a]ny evidence identifying the owner/user of the device." *Bock*, 310 Or.App. at 332. The court held that "[r]egardless of whether the command to search for evidence of the owner or user of the device included a temporal limitation on the material subject to seizure… the search command violates the particularity requirement." *Id.* at 334. This is because "there is little information on the device that the state could not use to identify the defendant given the right circumstances and background information. Under such circumstances, the officer performing the search has the discretion to rummage freely throughout the device and seize nearly everything—the exact practice that the particularity requirement was adopted to prohibit." *Id.* at 335.

Similarly, in *Hamilton*, the District Court rejected the government's argument that broad warrants are lawful because, "anything and everything in the Facebook account could be used to prove identity of the Facebook user and control of the account…" *Hamilton*, 2019 WL 4455997 at *5. The court reasoned that "[t]aken to its logical conclusion, this argument nearly obviates the particularity requirement altogether; almost anything in someone's social media data can be used

to show they did (or did not) own and control that account." *Id.* The court elaborated, explaining that the government was "certainly entitled to search for this information to a reasonable extent; for example, the registered user, email addresses, birth date, telephone number, physical address, and IP addresses associated with the account are likely to show ownership and control of the account. The breadth of information the search warrant required Facebook to disclose, however, amounted to "a general, exploratory rummaging" in [the defendant's] digital life that did not comport with the particularity requirement of the Fourth Amendment." *Id.*

The same logic from *Bock* and *Hamilton* applies to, and invalidates, paragraph c. One can only begin to imagine what might constitute evidence of the account owner's "state of mind" when it comes to a crime. Evidence that they sought psychiatric help for depression could indicate they were in a fragile mental state that caused them to collect and view horrible images they would otherwise not have viewed. Internet searches for assistance with substance abuse could similarly prove their unstable state of mind. Evidence that an account holder committed other unrelated crimes could show their willingness to put their own interests before that of the rest of society. Calendar notes that someone was attending computer literacy classes could demonstrate that they had the technological sophistication to commit the charged offence. Indeed, even agent [redacted] struggled to define what data he might search for under this clause. *See Google Warrant Affidavit*, at ¶ 31.[7] Instead, he identified what he *might* search for in general categories like evidence of "motive and intent" or "consciousness of guilt." *Id.* The closest he came to defining what kind of evidence or data he might search for under such a clause was "deleted account information" but even this was merely by way of illustration. *Id.* Thus the boundaries of this clause are left only to

[7] Defense notes that the Google Warrant does not expressly incorporate the Google Warrant Affidavit. Therefore, the Google Warrant Affidavit may not be considered in determining the particularity and breadth of the Google Warrant. *Groh v. Ramirez*, 540 U.S. 551 (2004). However, the agent's affidavit illustrates that he understood the phrase to grant him just as much discretion as is apparent on its face.

the imagination of the executing officer as they come across previously unidentified evidence during their unrestrained search. This is "the exact practice that the particularity requirement was adopted to prohibit." *Bock*, 310 Or.App. at 335.

Therefore, paragraph a. is overbroad because it allows for seizure of contraband for which there is no probable cause, while paragraphs .b through .d violate the particularity requirement by allowing a search and seizure of any and all data that they believe could be used to show the account holder's state of mind, account usage, and indicia of ownership.

III. A Franks Hearing is Required Because Agent [redacted] Deceived the Magistrate as to the Nature of Google's Storage of the Contraband in This Case.

A *Franks* hearing is required because agent [redacted] intentionally deceived the magistrate through the use of intentional omissions and boilerplate language in an affidavit that was "artfully drafted" to mislead the magistrate as to the particular facts of this case. Specifically, the affidavit omitted facts about Google's CSAM scanning processes and the location of the contraband in this case in order to obtain the general warrant submitted here.

Search warrants enjoy a presumption of validity and therefore hearings are not generally granted where a warrant was issued. However, when a defendant can demonstrate that the warrant was obtained through false or misleading statements or omissions they are entitled to a hearing. *Franks v. Delaware*, 438 U.S. 154, 171 (1978).

Here a *Franks* hearing is warranted because agent [redacted] deceived the magistrate in several material respects. First, he did not fully explain that he was aware, through the NCMEC CyberTipline report, of the exact location of the contraband within the Google account (i.e. Google Drive and Google Images). Second, he did not state that Google can, and does, provide only the relevant portions of the entire target account at the request of the government, and therefore could

have simply provided the contents of the Google Drive and Google Photos. Third, he omitted an explanation that, because of Google's use of "CSAI match" and its proprietary artificial intelligence, it was unlikely that contraband images other than those identified in the CyberTipline report existed elsewhere in the Google account. Finally, he failed to explain that, through the use of the filenames and hash values in the NCMEC CyberTipline report, he could have specifically requested production of the contraband that was known to be within the account and that he therefore did not need to rummage through the whole of the Google Drive or Google Photo infrastructure to locate those items. As a result of these intentional omissions the judge was misled to believe that agent [redacted] had to target all the 13 broad categories of information to recover the reported contraband and that there may have been significantly more contraband in the account. In fact, the government could have easily limited the search for contraband to the Google Drive and Google Images portions of the account and used the filenames and hash values to identify the known and suspected contraband.

Instead of explaining these facts in a clear and coherent manner [redacted] spent sixteen paragraphs describing various irrelevant parts of the Google infrastructure, *see the Google Warrant Affidavit*, at ¶ at ¶ 10-26, and at the end stated "[b]ased on my training and experience; messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation." *Id.* at ¶ 29. While he mentioned, in passing, that the contraband identified in the CyberTipline Report was found in Google Photos and Google Drive, this fact had no significance given the omissions regarding Google's technology, capabilities, and infrastructure. This is the kind of "artfully drafted" affidavit that courts have found

violates the law because it is intended to mislead a judge. *See United States v. Ailemen*, 986 F. Supp. 1228, 1240 (N.D. Cal. 1997) (citing *United States v. Simpson*, 813 F.2d 1462, 1471 (9th Cir.1987) (quoting district court); *see also Groh*, 540 U.S. at 561 n.4 (where government agent did not alert the magistrate to the defect in the warrant that the agent had drafted, the Court could not be certain whether the magistrate was aware of the scope of the search he was authorizing). Had the magistrate been aware of all the omitted facts they would have restricted the search for contraband to either the specific items named in the CyberTipline reports or to Google Images and Google Drive. Therefore, the omissions were material, and a *Franks* hearing must be granted.

IV. The Good Faith Exception Does Not Apply Because Law Enforcement Deceived the Magistrate in Their Application in Order to Obtain a General Warrant.

The good faith doctrine does not apply in this case because Agent [redacted] obtained the Google Warrant by intentionally deceiving the magistrate. Furthermore, the good faith doctrine does not apply to general warrants especially where, as in this case, they closely mirror warrants previously found to be unconstitutional.

"Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996). Instead, it is a limited exception to the rules of the warrant requirement and does not shield "an officer who relies on a duly issued warrant in at least four circumstances: '(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient [i.e. failing to particularize the place to be search or the things to be seized] that reliance upon it is unreasonable.'" *United States v. Raymonda*, 780 F.3d 105, 118 (2d Cir. 2015) (quoting *United States v. Clark*, 638 F.3d 89, 100

(2d Cir. 2011)); *see also United States v. Leon*, 468 U.S. 897, 923 (1984). "The Supreme Court has since clarified that these limitations apply not merely in cases of deliberate police misconduct, but also in situations where an officer is "reckless" or "grossly negligent" in seeking or executing a warrant." *Raymonda*, 780 F.3d at 118 (citing *Herring v. United States*, 555 U.S. 135, 144 (2009); *Davis v. United States*, 564 U.S. 229, 237 (2011))

Here this general warrant was only granted because of agent [redacted]'s intentional omissions and an "artfully drafted" affidavit that was designed to mislead the magistrate judge. *See supra* § III. In *Franks*, the Supreme Court observed: "When the Fourth Amendment demands a factual showing sufficient to comprise 'probable cause,' the obvious assumption is that there will be a truthful showing." *Franks*, 438 U.S. at 164-65 (original citation omitted). Here the affidavit deceived the court as to multiple material facts regarding Google's technology, data storage, and the information available to [redacted] at the time he requested the warrant. *See supra* § III. Without those misrepresentations the magistrate surely would not have issued this general warrant. Therefore, the good faith rule from *Leon* does not apply. *See Leon*, 468 U.S. at 923.

Furthermore, this was a general warrant both in terms what the government could seize from Google at step one and what they could subsequently search for and seize at step two. *See supra* §§ I. & II. And an executing officer may not rely on a general warrant in good faith. *See Groh,* 540 U.S. at 558. To hold otherwise would invite the kind of "systematic error" and "reckless disregard of constitutional requirements" that the Supreme Court has cautioned against. *Herring*, 555 U.S. at 144; *see also United States v. Krueger*, 809 F.3d 1109, 1123 (10th Cir. 2015) (Gorsuch, J., concurring) (finding that when a warrant is void, "potential questions of 'harmlessness'" do not matter"); *United States v. Winn*¸ 79 F. Supp. 3d 904, 926 (S.D. Ill. 2015) ("Because the warrant is a general warrant, it has no valid portions."). While the good-faith exception is relatively new, the

prohibition on general warrants is not. General warrants were a catalyst for the American Revolution and the inspiration behind the Fourth Amendment. And as a result, the Constitution forbids them. Because *Leon* was not decided until 1984—nearly 200 years after the Fourth Amendment outlawed general warrants in this country, fewer courts have had occasion to consider whether the good-faith rule has any bearing on a general warrant. But consistently, courts have found that the good-faith exception is inapplicable to general warrants. *See, e.g., Groh*, 540 U.S. at 558 (finding that a warrant "so obviously deficient" in particularity must be regarded as "warrantless" within the meaning of our case law); *United States. v. Zemlyansky,* 945 F.Supp.2d 438 (2013) (finding an insufficiently particular warrant so clearly defective that suppression was warranted); *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents ($92,422.57),* 307 F.3d 137, 149 (3d Cir. 2002) (finding general warrants to be "so plainly in violation of the particularity requirement that the executing officers could not have reasonably trusted in its legality"); *United States v. George*, 975 F.2d 72, 77-78 (2d Cir. 1992); *United States v. Medlin*, 842 F.2d 1194, 1199 (10th Cir. 1988); *United States v. Crozier*, 777 F.2d 1376, 1381 (9th Cir. 1985); *see also United States v. Minnick*, No. TDC-14-055, 2016 WL 3461190, at *5 (D. Md. June 21, 2016) (considering the good-faith exception's applicability to suppression after rejecting the claim that what issued was a general warrant); *Winn*, 79 F. Supp. 3d at 926; *United States v. Fleet Mgmt. Ltd.,* 521 F. Supp. 2d 436, 445-46 (E.D. Pa. 2007) ("[W]e read Third Circuit precedent to prohibit the use of the good faith exception in connection with general warrants.") (citing *United States v. Christine*, 687 F.2d 749, 758 (3d Cir. 1982) ("It is beyond doubt that all evidence seized pursuant to a general warrant must be suppressed.")).

Additionally, courts all over the country have found these specific types of warrants to third party internet service providers violate the Fourth Amendment. First the warrant allowed the

government to seize 13 broad categories of information from Google despite having probable cause only to seize and search a small portion of the account (Google Images and Google Photos). *See supra* § I. Second, it employed an "indicia of ownership" clause and two similar clauses that stripped it of any particularity and gave complete discretion to agent [redacted] as to what he was to search for and seize. *See supra* § II. Third, the warrant and affidavit utilized boilerplate language from templates used in other cases where courts found the warrants unconstitutional. *Compare the Google Warrant Affidavit*, at ¶ 28 (This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation") *with United States v. Whitt*, No. 1:17CR060, 2018 WL 447586, at *3 (S.D. Ohio Jan. 17, 2018) (when the agent stated that a search of the Facebook account will allow it to determine the "'who, what, why, when, where, and how' of the criminal conduct under investigation."); *compare the Google Warrant*, Attachment B at § II. ¶ c & d ("Evidence indicating the Account owner's state of mind as it relates to the crime under investigation; d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s)."); *with Shipp*, 392 F.Supp.3d 300 ("(e) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation; (f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s)"). Finally, the Google Warrant Affidavit contained tacit admissions by agent [redacted] that the Google Warrant allowed a general search when it stated they hoped to find "[o]ther information connected to the use of a Google account [which] may lead to the discovery of additional evidence…" *See Google Warrant Affidavit*, at ¶ 32.

Therefore, the use of intentional deception to obtain a type of general warrant that has been previously held unconstitutional vitiate any claims by the government that agent [redacted] relied in good faith on the Google Warrant.

CONCLUSION

The Google Warrant was overbroad as to what the government was to seize from Google and overbroad and insufficiently particular as to what, from that initial over-seizure, the government was to further search for and seize. The good faith doctrine does not apply because agent [redacted] intentionally omitted facts in order to obtain a general warrant that was strikingly similar to warrants previously found unconstitutional by other courts around the country.

WHEREFORE, defendant [redacted] respectfully requests that his Motion to Suppress be granted and that the Court enter an order preventing the government from admitting the contents of Google account associated with the email address [redacted]@gmail.com" and any and all derivative evidence acquired as an indirect result of the unlawful search and seizure, or for a hearing on the matter, with the opportunity to file a post-hearing brief based on evidence that may be introduced at the hearing, and for all other relief to which he may be entitled.

Respectfully submitted,

[redacted]
FEDERAL PUBLIC DEFENDER
WESTERN DISTRICT OF ARKANSAS

By: [redacted]

Counsel for Defendant

CERTIFICATE OF SERVICE

I hereby certify that I have electronically filed the foregoing with the Clerk of the Court using the CM/ECF System which will send notification of such filing to Mr. [redacted]

Assistant United States Attorney and a copy of this pleading was mailed by the United States Postal Service to: none.

/s/ [redacted]
Assistant Federal Public Defender