

IN THE DISTRICT COURT OF LANCASTER COUNTY NEBRASKA

STATE OF NEBRASKA )  
 ) SS  
COUNTY OF LANCASTER )

CR24-1

RETURN AND INVENTORY  
NSP21013352

Investigator Justin Podany, being first duly sworn, deposes and says that, on December 20, 2023, he served the within warrant at Google Inc. 1600 Amphitheatre Parkway, Mountain View, CA 94043 through the Google Law Enforcement Portal and Inv. Podany made a diligent search for the property described therein at the place, or person, mentioned therein, and seized and am in possession of the following described property, to-wit:

8.57 GB of zipped files and data

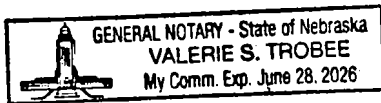
Said property returned to Inv. Podany on 1/12/24 and was inventoried in the presence of Google, Inc. and a copy of said Warrant and a receipt for said property was left with the Clerk of the Lancaster District Court.

Dated this 12 day of January, 2024.

*Inv. Podany #76*

Inv. Justin Podany, Nebraska State Patrol

SUBSCRIBED AND SWORN TO before me this 12<sup>th</sup> day of January, 2024.



Notary

*Valerie S. Trobee*

Warrant and inventory returned on this \_\_\_ day of \_\_\_\_\_, 20\_\_.

Lancaster County Clerk

LANCASTER COUNTY  
2024 JAN 16 PM 2:50  
CLERK OF THE  
DISTRICT COURT



002162738D02

5

IN THE DISTRICT COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA )
) ss. AFFIDAVIT IN SUPPORT
COUNTY OF LANCASTER ) FOR SEARCH WARRANT

THE COMPLAINT AND AFFIDAVIT of Justin Podany, Investigator, Nebraska State Patrol, on this 19th day of December 2023 who first being duly sworn, upon his oath says:

Your affiant is an Investigator with the Nebraska State Patrol, State of Nebraska and has been employed as a certified law enforcement officer since 2018. He has received specialized investigative training on a variety of topics including Conspiracy Investigations and Drug Investigations through the National White Collar Crime Center. Your affiant is assigned to investigate criminal complaints in approximately 14 counties in southeast Nebraska, to include misdemeanor and felony offenses.

Your affiant is presently assisting with the investigation of Conspiracy to Distribute a Controlled Substance. Investigators believe that this is a criminal matter likely involving one or more of the following offenses:, 83-417 : Unlawful acts by any person RE: inmate, 28-202-2A : Conspiracy to commit a class 2A felony, 28-416(1)(A)-F2A : Del/dsp/dst/man/pos cntrl subs-Sch 1,2,3, 28-416(10)(B) : Possess (meth)amphetamine 28-139 grams.

Your Affiant has just and reasonable grounds to believe, and does believe that there is secured or kept at Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, the following property, to-wit:

- 1. All information listed below is requested for the Google account identified as foxxycleo007@gmail.com for activity occurring between 4/20/2020 until 11/29/2023.
a. Account Information - User name, primary email address, secondary email addresses, connected applications and sites, and account activity from 4/20/2020 until 11/29/2023, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;
b. Device Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;
c. Evidence of user attribution - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).
d. Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, from 4/20/2020 until 11/29/2023, calendar entries, notes, alerts, invites, and invitees;

- e. **Contacts** - All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;
- f. **Documents** – All user created documents stored by Google;
- g. **Finance** - All records of securities, funds, and portfolios associated with the target Google account and/or target device from 4/20/2020 until 11/29/2023;
- h. **Gmail** - All email messages, whether stored in the account, previously stored in the account, preserved by Google on Google's servers, or otherwise stored, maintained, controlled, or preserved by Google from 4/20/2020 until 11/29/2023, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;
- i. **Google Photos** - All images, graphic files, video files, and other media files stored in the Google Photos service
- j. **Location History** - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period 4/20/2020 until 11/29/2023;
- k. **Play Store** - All applications downloaded, installed, and/or purchased by the associated account and/or device;
- l. **Search History** - All search history and queries from 4/20/2020 until 11/29/2023, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;
- m. **Voice** - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device from 4/20/2020 until 11/29/2023;
- n. **Google Drive** - All folders and/or files present in the user's Drive account, including, but not limited to, pictures, videos, documents, and metadata for each file.
- o. **Any and all files**, if applicable, from Google Chat, Google Hangouts, Google Groups, Google Docs, YouTube, or other Google services related to the user account.
- p. **Wallet/Checkout** - All information contained in the associated Google Wallet account including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers used for the transactions, and address book from 4/20/2020 until 11/29/2023.
- q. **Complaints** - If available, documentation of any criminal investigations or complaints made against the subscriber for inappropriate conduct while using services provided by Google, Inc.

Your Affiant submits this Affidavit and Application for Issuance of a Search Warrant pursuant to Neb.Rev.Stat. § 86-2,106 and § 86-2,108. Affiant further states that he may obtain a Search Warrant requiring the disclosure by a provider of electronic communication service of the contents of an electronic communication pursuant to Neb.Rev.Stat. § 86-2,106(1), and additionally may obtain an order commanding a provider of electronic communication service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order pursuant to Neb.Rev.Stat. § 86-2,108(2).

Based on his training and experience, your Affiant has developed probable cause to believe, and does believe that evidence relative to proving the crimes described herein is secured or is being kept at or within the following described place, or person, to-wit: Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043.

That said property is under the control or custody of Google, Inc., Custodian of Records, 1600 Amphitheatre Parkway, Mountain View, CA 94043.

That the following are grounds for issuance of a search warrant for said property and the reason for this belief, to-wit:

- On April 20, 2021, a package was received at the Reception and Treatment Center (formerly the Lincoln Correctional Center) located at 3216 W Van Dorn St in Lincoln, Nebraska. The parcel information read: The Next Millennium/ 402-393-1121/ The UPS Store #2220/ 505 Cornhusker Rd/ Bellevue NE 68005-7911. Tracking #1Z 84Y 07R 03 5657 2214. The shipping date was April 19, 2021.
- On April 27, 2021, the package was picked up by RTC Religious Coordinator Benjamin Salo. On April 21, 2021 Salo received an Inmate Interview Request form from inmate Troy Hess #37165 inquiring about the package, indicating that he knew about the parcel.
- RTC Front Entrance Corporal Jasmin Corona passed the parcel through the X-Ray scanner. Cpl. Corona determined that the contents of the package contained items that appeared unusual. Cpl. Corona removed the items, which included 7 large candles, 4 smaller candles, incense, and religious cloths. After Cpl. Corona sent each candle through the x-ray one at a time, she determined that the candles contained unknown items.
- Upon searching inmate Hess' cell, inmate Hess began flushing items down his toilet. The subsequent cell search found a paper containing a leafy substance.

- The candles were taken by RTC Captain Jonathan Kruse and passed through the x-ray again and photographed. Capt. Kruse then turned the evidence over to RTC evidence custodian Nicholas Bosak.
- On May 5, 2021, Inv. Podany traveled to RTC and took possession of the UPS package containing the candles, incense, and cloth. Inv. Podany transported it to the Nebraska State Patrol temporary evidence storage, sealed the evidence and secured it in storage. At a later date, Inv. Podany submitted a request to the Nebraska State Patrol Crime Laboratory to check the contents of the box as well as the items concealed within the candles for latent prints. During this time from being picked up from RTC to being transported to the State Patrol evidence storage and ultimately the State Patrol Crime Laboratory, the candles remained in their original form and were untampered. The items contained within the candles were not observed or removed from inside the candles until the Nebraska State Patrol Latent Fingerprint Lab received them.
- On June 1, 2021, Inv. Podany traveled to Omaha Nebraska to speak with Dmitri Kolesnikov and to view the video surveillance from UPS store #2220. Kolesnikov stated he utilized the shipment tracking information as well as the receipt to find the customer that sent that particular package to RTC (I.CC). Kolesnikov copied the relevant videos and provided them to Inv. Podany. The videos were submitted into evidence.
- On February 15, 2022, the Crime Laboratory sent their report to Inv. Podany. In the report, the Forensic Scientist that completed the report indicated that sixteen latent fingerprints were recovered from items inside the UPS box. Latent print L1 was recovered from item 1C, which is a white/grey pillar candle. L1 is a plastic impression in the outside surface of candle 1C. The plastic impression would have been deposited on the candle wax when the candle was soft and moldable. This latent print was searched through Nebraska AFIS which resulted in match with LeAnne Marie Strong DOB:05/30/1970.
- Latent print L9 was recovered from item 1D2, a plastic IKEA Ziplock bag. Latent print L10, L11, L12, L13 and L14 were taken from item 1F5A4A, a Walmart receipt. All latent impressions were found on record with the FBI's NGI bearing the name Dawnelle Marie Vaughn, DOB: 12/27/1984.
- Items containing drug evidence were then sent for Drug Analysis. On April 28, 2022, the State Lab confirmed the presence of multiple controlled substances. Items contained within the candles were as follows:
  - Lab confirmed 22.6 grams of synthetic cannabinoid
  - Lab confirmed 57.04 grams of methamphetamine
  - Multiple cell phones
  - Multiple AT&T sim cards

- Glass Pipes and rolling papers
  - Multiple Vape Pens
- 
- On December 9, 2021, Inv. Podany received inmate email correspondence between LeAnne Strong and inmate Corey Brooks #78533. In an email sent on April 2, 2021, LeAnne Strong sent Brooks a photo of herself from the email [foxxyclco007@gmail.com](mailto:foxxyclco007@gmail.com). In the photo she is wearing a brown jacket, a blue plaid shirt, blue jeans, and light brown boots. In the video from the UPS store #2220 in which the box of candles was sent, the female that brought the box into the store was wearing a blue plaid shirt and brown boots. In the video from the UPS surveillance cameras the clothing described closely matches the clothing in the photo sent by LeAnne Strong to inmate Brooks.
  - On September 6, 2023, Inv. Podany interviewed Shawna Wagner. Wagner, at the time of the offense, was roommates with LeAnne Strong. Wagner told Inv. Podany that she witnessed Strong and an unknown female crafting candles. Wagner stated that Strong had told her that she had made candles for the purpose of sending them into state prisons with concealed contraband inside on three to four occasions. Inv. Podany asked Wagner to describe the unknown female. Wagner advised the unknown female was approximately 5'5" and around 125 lbs. This closely matches the description of Dawnelle Vaughn.
  - On November 27 and 29, 2023, Inv. Podany monitored calls placed by Dawnelle Vaughn at the Lancaster County Detention Center. In a call placed by Vaughn on November 20, 2023, at approximately 20:19 hours to the number 531-225-9279, who is identified as Angela Short, Vaughn made multiple statements regarding her current charges. In this call she stated to Short that she was coerced to commit her current offenses due to her and her children being threatened. Vaughn told Short that these threats were documented in emails on her Gmail account. In a call placed by Vaughn on November 23, 2023, at approximately 10:52 hours to the number, 531-225-9279, who is identified as Angela Short, Vaughn stated (regarding her current charges) she didn't do it because she wanted to do it. Your Affiant believes this is in reference to Vaughn being coerced to commit the offenses. In a call placed on November 23, 2023, at approximately 16:39 hours to the number 531-225-9279, Vaughn and Short again are discussing her charges and Vaughn told Short that there are emails on her gmail account.
  - On December 12, 2023, Inv. Podany conducted a Proffer interview of Dawnelle Vaughn. During this interview, Vaughn stated that she trafficked multiple phones through an unknown correctional officer prior to the package of candles being sent. Vaughn believes that her, then boyfriend, Felix Alarcon, used one of those phones to email and call her to threaten her to engage in the conspiracy to send the contraband into the facility inside the candles. Also, during this interview, Vaughn stated that she believes that Strong had

engaged in the trafficking of contraband through candles prior to her being involved. Vaughn also stated that Strong assisted in preparing and sending the candles seized on April 20, 2021.

- Your Affiant believes that if Strong had engaged in this conspiracy prior to Vaughn's involvement, then there is likely communication on her email account from inmate Alarcon and other coconspirators discussing and planning the trafficking of contraband inside the candles as well as possible evidence to identify the unknown correctional officer.
1. Google provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. Google accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other Google services, such as instant messages and remote photo or file storage.
  2. Based on my training and experience, I know that Google allows subscribers to obtain accounts by registering on Google's website. During the registration process, Google asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases a means of payment. Google typically does not verify subscriber names. However, Google does verify the e-mail address or phone number provided.
  3. Once a subscriber has registered an account, Google provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Google subscribers can also use that same username or account in connection with other services provided by Google.
  4. Google Services may include: electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and storage), local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).
  5. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a Google account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on Google's servers for a certain period of time.

6. Thus, a subscriber's Google account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing, voice calls, video chats, SMS text messaging, and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on Google's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on Google's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Google's servers for a certain period of time. Furthermore, a Google subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on Google's servers. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within such computer files and other information created or stored by Google subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.
7. Based on my training and experience, I know that providers such as Google also collect and maintain information about their subscribers, including information about their use of Google services. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as Google also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Google typically collect and maintain location data related to subscriber's use of Google services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.
8. Based on my training and experience, I know that providers such as Google also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Google in order to track what devices are using Google's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Google accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Google account.
9. Based on my training and experience, I know that providers such as Google use cookies and similar technologies to track users visiting Google's webpages and using its products and



services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to Google. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as Google may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a Google account and determine the scope of criminal activity.

10. Based on my training and experience, I know that Google maintains records that can link different Google accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Google accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Google account.
11. Based on my training and experience, I know that subscribers can communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.
12. In summary, based on my training and experience in this context, I believe that the computers of Google are likely to contain user-generated content such as stored electronic communications (including retrieved and un-retrieved e-mail for Google subscribers), as well as Google generated information about its subscribers and their use of Google services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.
13. As explained above, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling law enforcement to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Google can show how and when the account was accessed or used. For example, providers such as Google typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological

and geographic context of the Google account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Google account may indicate its user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

Your Affiant believes that the above property is being concealed, kept, or used in violation of the laws of the State of Nebraska, or is being concealed or kept at the premises and constitutes evidence of, or evidence relevant to proving a violation of the laws of the State of Nebraska as previously described in this affidavit.

Based on the information set forth herein your Affiant requests that a search warrant be issued for the requested information related to Google user account, foxxycleo007@gmail.com.

Your Affiant notes the information being requested is being provided by the Google Custodian of Records and/or Google Payment Corporation. Your Affiant has no control over the amount of time they take to respond to the search warrant request which may take longer than the 10 days required to complete the search warrant return. As a result, your Affiant will complete the search warrant return upon the service of the requested search warrant, unless otherwise ordered by the Court.

Your Affiant further requests that Google, Inc. shall disclose responsive data by sending it to: Inv. Justin Podany #76, justin.podany@nebraska.gov, 4600 Innovation Dr. Lincoln, NE 68521.

FURTHER AFFIANT SAYETH NAUGHT.

WHEREFORE, he prays that a Search Warrant be issued according to law.

Inv. Podany #76 12/19/23  
Justin Podany, Investigator, Nebraska State Patrol

SWORN TO AND SUBSCRIBED before me this 19th day of December, 2023.

Ryan Post  
Judge

LANCASTER COUNTY

2024 JAN 16 PM 2:50

CLERK OF THE DISTRICT COURT

IN THE DISTRICT COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA )  
 ) SS.  
COUNTY OF LANCASTER )

SEARCH WARRANT

TO: Inv. Justin Podany, Nebraska State Patrol

WHEREAS, Inv. Justin Podany, Nebraska State Patrol has made a sworn affidavit before me, the undersigned Judge in and for the County of Lancaster, State of Nebraska, and

That the Court has jurisdiction of this matter pursuant to the sections 29-729 through 29-829, Nebraska Revised Statutes, 1943, as amended.

WHEREAS, I am satisfied that there is probable cause to believe that secured or kept on the premise at Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043 the following grounds exist for issuance of a search warrant, to wit:

1. All information listed below is requested for the Google account identified as foxxycleo007@gmail.com for activity occurring between 4/20/2020 until 11/29/2023.
  - a. **Account Information** - User name, primary email address, secondary email addresses, connected applications and sites, and account activity from 4/20/2020 until 11/29/2023, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;
  - b. **Device Information** - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;
  - c. **Evidence of user attribution** - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).
  - d. **Calendar** - All calendars, including shared calendars and the identities of those with whom they are shared, from 4/20/2020 until 11/29/2023, calendar entries, notes, alerts, invites, and invitees;
  - e. **Contacts** - All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;
  - f. **Documents** - All user created documents stored by Google;
  - g. **Finance** - All records of securities, funds, and portfolios associated with the target Google account and/or target device from 4/20/2020 until 11/29/2023;
  - h. **Gmail** - All email messages, whether stored in the account, previously stored in the account, preserved by Google on Google's servers, or otherwise stored, maintained,

- controlled, or preserved by Google from 4/20/2020 until 11/29/2023. including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;
- i. **Google Photos** - All images, graphic files, video files, and other media files stored in the Google Photos service
  - j. **Location History** - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period 4/20/2020 until 11/29/2023;
  - k. **Play Store** - All applications downloaded, installed, and/or purchased by the associated account and/or device;
  - l. **Search History** - All search history and queries from 4/20/2020 until 11/29/2023, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;
  - m. **Voice** - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device from 4/20/2020 until 11/29/2023;
  - n. **Google Drive** - All folders and/or files present in the user's Drive account, including, but not limited to, pictures, videos, documents, and metadata for each file.
  - o. **Any and all files**, if applicable, from Google Chat, Google Hangouts, Google Groups, Google Docs, YouTube, or other Google services related to the user account.
  - p. **Wallet/Checkout** - All information contained in the associated Google Wallet account including transactions, purchases, money transfers, payment methods, including the full credit card number and/or bank account numbers used for the transactions, and address book from 4/20/2020 until 11/29/2023.
  - q. **Complaints** - If available, documentation of any criminal investigations or complaints made against the subscriber for inappropriate conduct while using services provided by Google, Inc.

YOU ARE THEREFORE ORDERED, with the necessary and proper assistance, to search the above described premises, for the purposes of seizing the before described property, and if found, to seize and deal with the same as provided by law.

IT IS FURTHER ORDERED, notwithstanding 18 U.S.C. § 2252.2252A or any similar statute or code, Google, Inc. shall disclose responsive data by sending it to Inv. Justin Podany #76, [justin.podany@nebraska.gov](mailto:justin.podany@nebraska.gov), 4600 Innovation Dr. Lincoln, NE 68521.

IT IS FURTHER ORDERED, that the execution of the Search Warrant be forthwith during daylight hours.

IT IS FURTHER ORDERED, that Investigator Justin Podany, of The Nebraska State Patrol, or his designee, make return of this Search Warrant to me within ten days after the date hereof.

Given under my hand this 19th day of December 2023.

  
\_\_\_\_\_  
Judge

NSP21013352