\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INSTRUCTIONS\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

- This search warrant mask is specifically for the search of Google for all data associated with the identified account name

-There is RED text below that needs to be changed based on the needs of your search warrant.

-There is BLUE text below which is provided for information to the reader about what is being requested and why. Make sure you read this information and understand it since you are putting it your search warrant. You may need to adjust some of the wording or content in these areas to the specifics of your case.

-There is GREEN text below that articulate facts specific to ICAC or sexual exploitation investigations. Include this language only if it applies. Make sure you read this information and understand it since you are putting it your search warrant. You may need to adjust some of the wording or content in these areas to the specifics of your case.

- After the warrant is finalized, highlight all of the text by selecting CTRL+A and then change all text to black

- It would be a good idea to delete this section before printing/sending your warrant to get signed.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*PLEASE DELETE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Case No:

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS**

## BEFORE THE HONORABLE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

JUDGE / MAGISTRATE

Affiant, YOUR NAME HERE, a commissioned law enforcement officer, being duly sworn, deposes and states that I have probable cause to believe that at the place or business entity known or described as:

**Google, LLC**

**Google Legal Investigations Support:**

**1600 Amphitheatre Parkway**

**Mountain View, CA 94043**

**Phone: 650-253-3425**

**Email: uslawenforcement@google.com**

There is now located within or upon said internet service/social media provider the following records, data, information and technical assistance:

* All records or other information regarding the personal identification of the subject account, to include full name, date of birth, gender, other contact email addresses, physical address, telephone numbers, and any other personal identifiers;
* The date on which the account was created, the length of service, the IP address with associated Port ID(s) used to register the account;
* Any other Gmail addresses associated with the account(s) listed above along with all personal identifiers related to those Gmail accounts;
* All Google/Gmail accounts associated to the above account(s) by device or cookie: to include User ID, subscriber name, cellphone number and email address for such associated accounts;
* All devices(s) used and otherwise associated with the subscriber’s account(s) – ESN, ICCID, IMSI, IMEI and MAC address numbers and activation dates;
* Google Cloud and/or Google One data collected in connection with any devices associated with the above user account;
* All data collected by Google from any Chromebook devices associated with the above user account;
* All log-in IP addresses with Port IDs associated with the account(s) identified above;
* Data relating to account activity, including “web and app” activity, voice and audio activity, YouTube search history, YouTube watch history, YouTube comments; YouTube stories;
* All location data collected, 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, Wi-Fi location, and all Google SensorVault data, including coordinates, timeline data, and dates and times of all locations where the account was accessed or used;
* Semantic Location History data including, but not limited to, activity, start and end location, latitude and longitude for each, duration (epoch time), distance, activity type, confidence level and probability, waypoints including latitude and longitude, places visited including latitude and longitude, place ID, address, name, source info, location confidence, duration, and other candidate locations.
* The contents of all e-mails sent from or received by the above account(s), including any attachments, whether such emails are deleted, stored, or preserved, along with any draft e-mails and associated attachments, the source and destination addresses associated with all such e-mails, the date and time at which each e-mail was sent or received, the size and length of each e-mail, and the true and accurate header information including the actual IP addresses with associated Port IDs of the sender and the recipient of these emails;
* Any photos or videos captured or stored in connection with the Google account(s) identified above, to include any metadata attached to such images or videos (camera make, model, capture date and time, capture latitude and longitude, etc.), and original sized images associated with those images and videos;
* The Google services utilized by the subject account(s), such as Google Maps, Google Duo, Google Hangouts, Google Plus, Google Chrome, Google Home, Google Drive, Google Nest, Google Play, Google Photos, Google Voice, YouTube, along with any third party applications or platforms associated with the Google account identified above, including records or data generated by those services or accounts that has been collected by Google;
* All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voice-mail messages sent by or from the Google Voice account associated with the target account/device;
* All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;
* All contacts stored by Google including name, all contact phone numbers, e-mails, social network links, and images;
* All Google documents including by way of example and not limitation, Docs (a web-based word processing application), Sheets (a web-based spreadsheet program), and Slides (a web-based presentation program.) Documents will include all files whether created, shared, or downloaded.
* All records pertaining to communications between Google and any person regarding the account(s), including contacts with support services and records of actions taken;
* All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to the provider;
* All privacy settings and account verification methods, including two factor authentication associated phone number(s);
* All means and source of payment (including any credit or bank account numbers) used and/or stored in connection with the Google account(s) identified above, purchase history, and subscriptions.
* All data associated with the subscriber account related to the “Tombstone” data archive.

**The above information is being requested in reference to the following** **account(s):**

**Gmail Account:** ACCOUNT NAME [IF KNOWN]

**Google ID(UID):** GOOGLE ID(UID) [IF KNOWN]

**Device ESN / IMEI / MEID:** ESN / IMEI / MEID [IF KNOWN]

**MAC ID:** MAC ID [IF KNOWN]

**The above information is being requested during the following time period:**

Between the dates of DATE OF INTEREST through DATE OF INTEREST

**The above information is being requested for evidence of:**

LIST CRIMINAL OFFENSE(S)

For which a search warrant and court order for production of records may be issued upon one or more of the grounds set forth in 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41, namely that this property has been stolen or embezzled, or which is designed or intended for use as a means of committing a criminal offense, or which is or had been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

The facts establishing grounds for issuance of a search warrant and showing probable cause to believe that they exist are as follows:

**Electronic Definitions**

“Internet” means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are physically located in the same state.

“Computers”, “digital media storage”, or “digital storage devices” may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

Internet Service Providers “ISP’s” or Electronic Service Providers “ESP’s” are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “email address,” an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password.

“Internet Protocol Address” or “IP address”: Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of numbers separated by periods; an example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP’s customers or subscribers. Most ISPs employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next customer. On the other hand, some ISPs, including most cable providers, employ static IP addressing, that is a customer or subscriber’s computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer. A modem is an electronic device that allows one computer to communicate with another.

Social Media: In general, social media may be defined as websites and applications that enable users to create and share content or to participate in social networking.

IMEI: IMEI (International Mobile Equipment Identity) is a unique identification number that identifies mobile devices.

IMSI: An international mobile subscriber identity (IMSI) is a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber.

Cookie: A cookie is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application. One purpose of a cookie is to save log in and password information for an account. It also serves the purpose of saving user preferences for a site, such as a search engine saving a search or a news website saving a certain font you prefer.

**Child Pornography/Child Exploitation Definitions**

NCMEC- The National Center for Missing and Exploited Children (“NCMEC”) is an organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip, also known as a CyberTipline Report. To make such a report, a company providing services on the internet (“ISP) can go to an online portal that NCMEC has set up for the submission of these tips. The ISP then can provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and incident time, the remainder of the information the ISP provides is voluntary and undertaken at the initiative of the reporting ISP. The ISP may also upload to NCMEC any files it collected in connection with the activity. The ISP may or may not independently view the content of the files it uploads. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ISP provides such as IP addresses. NCMEC then packages the information from the ISP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

“Sexually Exploitative Material” means any photograph, motion picture, video, recording, or broadcast of moving visual images, print, negative slide, or other mechanically, electronically, chemically, or digitally reproduced visual material that depicts a child engage in, participating in, observing, or being used for explicit sexual conduct.

**Statements Regarding Current Investigation**

BACKGROUND OF AFFIANT

STATEMENT OF PROBABLE CAUSE REGARDING CRIME BEING INVESTIGATED – OR IF FOR FUGITIVE PURPOSES, EXISTENCE OF OUTSTANDING WARRANT – AND PC TO BELIEVE THE ACCOUNT LISTED IS AN ACCOUNT THAT COULD LEAD TO MATERIAL EVIDENCE OR A FUGITIVE MIXED WITH THE BELOW PARAGRAPHS

**Background Information Relating to Google**

Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications, including retrieved and unretrieved email for Google subscribers, attachments, photos, videos, and other information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. Based on Your Affiant’s training and experience, such information may constitute direct evidence of the crimes under investigation or may lead to the identification of other evidence related to the below-described offenses.

In Your Affiant’s training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account numbers). Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Even if subscribers insert false information to conceal their identity, this information can still often provide clues to their identity, location or illicit activities.

Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (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. In addition, email providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular 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 computers or other devices were used to access the email account.

Information stored in connection with Google account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the prosecution to establish and prove each element or alternatively, to exclude the innocent from further suspicion. This evidence may be found in the various areas of the Google account that are specified above. In Your Affiant’s training and experience, the information stored in connection with a Google/gmail account can also indicate who has used or controlled the account. Further, information maintained by Google can show how, where, and when the account was accessed or used. Based on Your Affiant’s training and experience, Your Affiant has learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user’s Internet browser.

Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account and users are prompted to add a Google account when they first turn on a new Android device.

Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. The company uses this information for location-based advertising and location-based search results. This information is derived from sources including GPS data, cell site/cell tower information, and Wi-Fi access points. Your affiant has also learned that users running Google products on the Apple iPhone or other cellular telephone operating systems may also have their location data stored in a similar way as devices running Android operating systems.

Location data can assist investigators in understanding the chronological and geographic context of the account access and use relating to the crime(s) under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. 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 email).

Google does not verify the true identity of an account creator, account user or any other person who accesses a user’s account using login credentials. For these reason’s it is necessary to examine particularly unique identifying information that can be used to attribute the account data to a certain user. This is often accomplished by analyzing associated account data, usage, and activity through communication, connected devices, locations, associates, and other accounts. For these reasons it may be necessary to search and analyze data from when the Google account was initially created to the most current activity;

Google maintains information about their customers including primary e-mail addresses, secondary e-mail addresses for account password recovery, applications, websites, and services that are allowed to access the user’s Google account or use the user’s Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. This information will assist in the investigation by identifying previously unknown e-mail accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers;

Google stores information about mobile devices associated with the user’s Google account. This includes the make, model, and unique serial numbers of all linked devices. This information will identify any previously unknown cell phones or other mobile devices associated with the suspect’s account and/or known device(s);

Google offers a calendar feature that allows users to schedule events. This calendar function is the default option in the Android operating system and remains so unless the user adds a third-party application. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. This information will identify dates and appointments relevant to this investigation, as well as, identify previously unknown co-conspirators and/or witnesses, and any potential corroborative evidence;

Google offers their users access to free, web-based alternatives to existing word processing, spreadsheet, and presentation software. These documents are stored in the user’s account and are accessible from any device or platform as long as the user knows the password. These documents can include those created by the user, modified or edited by the user, or shared by the user and others. This information may contain notes, files, and spreadsheets containing information relevant to this investigation including recordation of sales, communications with unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation;

Google maintains a unified payment service, which combined Google Wallet and Android Pay into one service. Google Pay is an application that stores purchase and payment activity, along with individual credit card, debit card, and gift card information associated with the Google subscriber(s). Google Pay allows subscribers to send and receive money from a mobile device or computer at no cost to either the sender or receiver and facilitates e-purchases. Yhis the data contains information relevant to this investigation including records of purchases and payments, as well as money transfers and communications with unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation;

When user of an Android device first activates the device they are prompted to associate the device with a Google mail, commonly referred to as Gmail, account. The purpose of this account is to facilitate password recovery in the event the user forgets their password or pattern lock. If the user does not have an existing Gmail account, they are prompted to create one. The Gmail account may be used to send and receive electronic mail messages and chat histories. These messages include incoming mail, sent mail, and draft messages. Messages deleted from Gmail are not actually deleted. They are moved to a folder labelled Trash and are stored there until the user empties the Trash file. Additionally, users can send and receive files as attachments. These files may include documents, videos, and other media files. These messages would reveal motivations, plans and intentions, associates, and other co-conspirators;

When a user links the Android device to their Google account the names, addresses, phone numbers, e-mail addresses, notes, and pictures associated with the account are transferred to the phone and vice versa. This process is continuously updated so when a contact is added, deleted, or modified using either the Google account or the mobile device the other is simultaneously updated. This information is pertinent to the investigation, as it will assist with identifying previously unknown coconspirators and/or witnesses.

Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent from other users, or uploaded from the user’s mobile device. In many cases, an Android user may configure their device to automatically upload pictures taken with a mobile device to their Google account. A review of these images would provide evidence depicting the suspect, his/her associates and others performing incriminating acts, and victims These image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation;

Google collects and retains location data from Android enabled mobile devices. The company uses this information for location-based advertising and location-based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or e-mail access. This data will show the movements of the suspect’s mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation;

Google Location History includes a subset of data known as Semantic Location History. This subset consists of additional contextual information in addition to the date, time, latitude, longitude, uncertainty/display radius, and technology used found with Location History. The Semantic Location History includes the activity type (e.g. walking, riding in a vehicle), waypoints, a unique Place ID, physical or street address, location confidence, and other possible location candidates at the same place. I believe this data would assist in the ongoing investigation by providing additional contextual location data, as well as, route and method of travel.

Google operates an online marketplace whereby Google and other third-party vendors offer for sale applications such as games, productivity tools, and social media portals. Many of these applications can be used to communicate outside the cellular service of a mobile device by accessing the internet via Wi-Fi.

These various applications facilitate communication via voice using voice over internet protocol (VOIP) technology, short message system (SMS) text messages, multi-media message system (MMS) text messages, audio transmission of recorded messages, and recorded or live video messages. As these services operate independently of the cellular service network there is no corresponding information regarding communications from the cellular provider. Identifying communications applications purchased, downloaded, and/or installed on the mobile device would assist investigators by determining what application provider should be served with additional search warrants. Furthermore, identifying the user’s applications would assist investigators with determining banking and other financial institution information and social media sites used. Identifying the purchased or installed applications would assist locating those with potentially criminal implications such as applications that appear to the observer to be a calculator or other innocuous appearing program but in actuality are used to conceal pictures, videos, and other files. These concealment applications are commonly missed during manual and forensic examinations of mobile devices as existing technologies are not designed to detect and locate them and the information they conceal;

Google retains a user’s search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user-selected results. Furthermore, the specific type of search a user performed into categories differentiates these searches. These categories include a general web search and specialty searches where the results are focused in a particular group such as images, news, videos, and shopping. A review of the suspect’s search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he sought it;

Google offers users access to a free voice over internet protocol (VOIP) communications system called Google Voice or simply Voice. This system is layered on top of any existing cellular service. Users are provided with a phone number they select from a pool of available numbers. These numbers can be from whatever area code and prefix they desire and have no correlation with the user’s actual location when the number is selected. Google allows users to access this system to make and receive phone calls and text messages. The service also has a voice-mail feature where incoming phone calls are permitted to leave a message that is subsequently transcribed by Google and delivered by electronic mail and/or text message. Google maintains call detail records similar to those of a traditional cellular or wireline telephone company. Additionally, they also store the text message content of sent and received text messages, as well as, any saved voice-mail messages and the associated transcriptions;

Google subscribers have the ability to delete their Google account information and any associated data at any time. Google will store this data if the subscriber deleted their user profile and all associated data related to their Google account, to include all the above-mentioned technologies, in what Google refers to as the “Tombstone” data archive. I learned Google will retain this data after a subscriber-initiated deletion of the account data, however it is not known how long Google will retain it.

This “Tombstone” data archive may be pertinent to the case, as data that may have been deleted was done with deliberate intention, with the intent of concealing or destroying evidence. The data, if deleted by the user and recovered via the “Tombstone” archive, may hold valuable information related to the ongoing criminal investigation. Due to the transient nature of the “Tombstone” data archive, the fact it is perishable data and not recoverable by law enforcement after a given period of time from subscriber-initiated deletion, it becomes imperative this data is obtained in a timely manner.

Google users may communicate directly with Google about issues relating to their account, such as technical problems or complaints. Social-networking providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications. Google may also suspend a particular user for breaching Google’s terms of service, during which time the Google user will be prevented from using Google services.

**Relevant Background Information of Child Pornography**

Collectors and distributors of child pornography often use online resources to retrieve, share, and store child pornography. Non-pornographic, seemingly innocuous images of minors are often found in accounts that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images. Further, the online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. These online storage accounts are often free but can involve a charge. A subscriber assigned a free online storage account frequently can set up such accounts by providing limited identifying information. Any information provided is frequently fictitious in an attempt to preserve the anonymity of the user. Consequently, even if it is known that a collector or distributor of child pornography is a subscriber of a free online storage service, the service provider frequently will have no records in that subscriber’s name. Instead, the online service will only be able to identify files, including child pornography, that are associated with a “login,” or unique, user-created identity the subscriber uses to “log on” to the online service. Such an online storage account is particularly useful to a collector or distributor of child pornography. Such a subscriber can collect, store, view and distribute electronic images, including child pornography, directly from the online service. Consequently, the illegal files have minimal contact with the subscriber’s home computer. The subscriber can also manipulate the files on an online storage service from any computer connected to the Internet. Nonetheless, evidence of an online storage account is often found on a home computer of a user subscribing to such a service. Evidence of an online storage account may take the form of passwords located in encrypted, archived,[[1]](#footnote-1) or other files on the user’s home computer. Other evidence can also be found through unique software that may exist on a user’s home computer that has been developed by the online storage service. This unique software will frequently contain evidence not only of the existence of such accounts, but the login and password.

I know from training and experience that persons trading in, receiving, transporting, distributing, or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation.

**Relevant Background Information of Technology**

I know from training and experience that digital evidence is not limited to computers. I have been involved in cases where persons engaged in the type of crime under investigation can access the Internet, display images reflecting their interests or participation in the crime, and communicate with other individuals with the same interests using digital storage devices to include cellular telephones, email devices, and personal digital assistants. These devices are frequently found to contain chat communications in the form of short message service (SMS) messages as well as enabling Internet and digital cellular network access.

I know from training and experience that the complete contents of online accounts may be important to establishing the actual user who has dominion and control of an online account at a given time. Online accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. So, information stored in connection with an online account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation. This helps establish and prove each element of the crime or alternatively, may exclude the innocent from further suspicion. In my training and experience, an online user’s account activity, IP log, location information, search history, stored electronic communications, and other data retained by providers, can indicate who has used or controlled an online account or can provide context for the crime under investigation. This can include evidence of motive and intent to commit a crime (e.g., communications about planning crimes) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. Further, account activity, especially when paired with other evidence of the crime, can show how and when the account was accessed or used and may reflect a user’s motive or state of mind when doing so. For example, as described herein, Providers log the Internet Protocol (IP) addresses from which users access their accounts 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 account access and use relating to the crime under investigation. Especially when considered in context with other evidence, such information allows investigators to understand the geographic and chronological context of an account’s access, use, and events relating to the crime under investigation. Location data also helps with this. Providers allow users to “tag” their location in posts to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the account user or other suspects.

I know from training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”) or code words (which require entire strings or series of email conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren “:)” to convey a smile or agreement) to discuss matters. Keyword searches would not account for any of these possibilities, so actual review of the contents of an online account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit in order to prevent unnecessary invasion of privacy and overbroad searches. I advise it would be impractical and infeasible for the government to review records produced by a Service Provider and keep only such records as the government finds to be related to the offenses described herein during a single analysis. I have learned through practical experience that various emails often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review, and incorporation of evidence into a consolidated whole. Analysis is content relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually and not in sum. Due to the interrelation and correlation between communication threads and contents of accounts, and any respective attachments, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. Therefore, to obtain the full picture and meaning of the data from the information sought in this application, and to maintain its admissibility at trial, the government needs to maintain access to all of the resultant data. The completeness and potential of probative value of the online accounts and data must be assessed within the full scope of the investigation. As with all evidence, the government will maintain the contents of the account(s) in its custody and control, without alteration.

Based on these facts, Your Affiant believes there exists probable cause to believe that there is material evidence now located in the above described **Google** account that is crucial to the investigation of this case and the offenses described above, and a search warrant is requested pursuant to 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41.

C.R.S. 16-3-301.1(5)(a) permits a court order for the productions of records to be granted to a Colorado criminal investigator or peace officer whose affidavit supports the issuance of the order. The Colorado criminal investigator or peace officer granted the order need not have authorization to execute a search warrant in the jurisdiction in which the business entity is located. C.R.S. 16-3-301.1(5)(c) permits service of a court order to be made through any electronic or other means established and utilized by the business to receive service of process.

**Google, LLC** is a provider of electronic communication services subject to the Stored Communication Act (SCA), 18 U.S.C. §2703, et seq. The SCA permits a state court with jurisdiction over an offense to issue an extraterritorial warrant for production of electronic communication content and electronic communication records. 18 U.S.C. §2703(g) authorizes service of the warrant via methods other than in-person service by a law enforcement officer. It is the intent of this affiant, consistent with the SCA and the procedures established by **Google, LLC** for compliance with the SCA, to serve this warrant via fax and/or email or law enforcement portal.

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

***Further requests:***

1. Pursuant to Crim. P. 41 and §16-3-304(2), Your Affiant requests that this Court seal the affidavit and search warrant and court order for production of records until the completion of the law enforcement criminal investigation. The affidavit establishes grounds to believe that disclosure at this time of the affidavit and search warrant and court order for production of records would be contrary to the public interest. Such order for sealing does not apply to representatives of law enforcement agencies, and District Attorney’s Offices.
2. So as not to disrupt this ongoing investigation, Your Affiant also requests that this Court order **Google, LLC** NOT to take adverse action against the subject account, such as disabling or terminating the account, because of this warrant.
3. Pursuant to 18 U.S.C. §2705(b) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), Your Affiant requests that **Google, LLC** be ordered NOT to disclose the existence of this search warrant and court order to the subscriber for a period of one year from receipt of the requested documents, unless otherwise ordered by a court of competent jurisdiction. Based on the information set forth in this affidavit, notification of the warrant may have an adverse result, as defined in 18 USC §2705(b)(1)-(5), i.e., disclosure may endanger the life or physical safety of an individual; allow flight from prosecution; allow destruction of or tampering with evidence; allow intimidation of potential witnesses; and/or would otherwise seriously jeopardize an investigation or unduly delay a trial.

I believe the above facts to be true from official LAW ENFORCEMENT AGENGY records, conversations with fellow officers, personal observations and interviews. I am a YOUR TITLE with the LAW ENFORCEMENT AGENGY. I have been trained at the State, and local levels with regard to my duties. I am authorized by law to execute search warrants in the State of Colorado.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

AFFIANT

This affidavit was sworn to and subscribed in my presence this DATE day of MONTH 20\*\* at \_\_\_\_\_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

JUDGE / MAGISTRATE

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

# **SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS**

## Before the Honorable \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge / Magistrate

The Court, upon review of an affidavit filed by YOUR NAME HERE which is incorporated by reference, in support of the issuance of this order, hereby orders the production of the following records, for which there is probable cause to believe are in the actual or constructive possession or control of the business entity known or described as:

**Google, LLC**

**Google Legal Investigations Support:**

**1600 Amphitheatre Parkway**

**Mountain View, CA 94043**

**Phone: 650-253-3425**

**Email: uslawenforcement@google.com**

This Court also finds that there is probable cause to issue this Search Warrant and Court Order for Production of Records pursuant to the provisions of 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41, namely that this property has been stolen or embezzled, or which is designed or intended for use as a means of committing a criminal offense, or which is or had been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

IT IS ORDERED that the internet service/social media provider provide the following records, data, information and technical assistance:

There is now located within or upon said internet service/social media provider the following records, data, information and technical assistance:

* All records or other information regarding the personal identification of the subject account, to include full name, date of birth, gender, other contact email addresses, physical address, telephone numbers, and any other personal identifiers;
* The date on which the account was created, the length of service, the IP address with associated Port ID(s) used to register the account;
* Any other Gmail addresses associated with the account(s) listed above along with all personal identifiers related to those Gmail accounts;
* All Google/Gmail accounts associated to the above account(s) by device or cookie: to include User ID, subscriber name, cellphone number and email address for such associated accounts;
* All devices(s) used and otherwise associated with the subscriber’s account(s) – ESN, ICCID, IMSI, IMEI and MAC address numbers and activation dates;
* Google Cloud and/or Google One data collected in connection with any devices associated with the above user account;
* All data collected by Google from any Chromebook devices associated with the above user account;
* All log-in IP addresses with Port IDs associated with the account(s) identified above;
* Data relating to account activity, including “web and app” activity, voice and audio activity, YouTube search history, YouTube watch history, YouTube comments; YouTube stories;
* All location data collected, 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, Wi-Fi location, and all Google SensorVault data, including coordinates, timeline data, and dates and times of all locations where the account was accessed or used;
* Semantic Location History data including, but not limited to, activity, start and end location, latitude and longitude for each, duration (epoch time), distance, activity type, confidence level and probability, waypoints including latitude and longitude, places visited including latitude and longitude, place ID, address, name, source info, location confidence, duration, and other candidate locations.
* The contents of all e-mails sent from or received by the above account(s), including any attachments, whether such emails are deleted, stored, or preserved, along with any draft e-mails and associated attachments, the source and destination addresses associated with all such e-mails, the date and time at which each e-mail was sent or received, the size and length of each e-mail, and the true and accurate header information including the actual IP addresses with associated Port IDs of the sender and the recipient of these emails;
* Any photos or videos captured or stored in connection with the Google account(s) identified above, to include any metadata attached to such images or videos (camera make, model, capture date and time, capture latitude and longitude, etc.), and original sized images associated with those images and videos;
* The Google services utilized by the subject account(s), such as Google Maps, Google Duo, Google Hangouts, Google Plus, Google Chrome, Google Home, Google Drive, Google Nest, Google Play, Google Photos, Google Voice, YouTube, along with any third party applications or platforms associated with the Google account identified above, including records or data generated by those services or accounts that has been collected by Google;
* All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voice-mail messages sent by or from the Google Voice account associated with the target account/device;
* All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;
* All contacts stored by Google including name, all contact phone numbers, e-mails, social network links, and images;
* All Google documents including by way of example and not limitation, Docs (a web-based word processing application), Sheets (a web-based spreadsheet program), and Slides (a web-based presentation program.) Documents will include all files whether created, shared, or downloaded.
* All records pertaining to communications between Google and any person regarding the account(s), including contacts with support services and records of actions taken;
* All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to the provider;
* All privacy settings and account verification methods, including two factor authentication associated phone number(s);
* All means and source of payment (including any credit or bank account numbers) used and/or stored in connection with the Google account(s) identified above, purchase history, and subscriptions.
* All data associated with the subscriber account related to the “Tombstone” data archive.

**The above information is being requested in reference to the following account(s):**

**Gmail Account:** ACCOUNT NAME [IF KNOWN]

**Google ID(UID):** GOOGLE ID(UID) [IF KNOWN]

**Device ESN / IMEI / MEID:** ESN / IMEI / MEID [IF KNOWN]

**MAC ID:** MAC ID [IF KNOWN]

**The above information is being requested during the following time period:**

Between the dates of DATE OF INTEREST through DATE OF INTEREST

**The above information is being requested for evidence of:**

LIST CRIMINAL OFFENSE(S)

Pursuant to §16-3-301.1, C.R.S., a criminal investigator or peace officer is hereby authorized to serve this order during normal business hours of the above-named business entity, and to receive the records during normal business hours of the business entity. Service shall issue in the same manner as a summons in a civil action or by personal service on a manager or supervisor of the business entity or through any electronic or other means established and utilized by the business to receive service of process. This order must be served within 14 days after the date it is issued.

The business entity is ORDERED to produce the above described records to the affiant or his/her designee within thirty-five (35) days of service.

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

The business entity shall also provide a notarized attestation of accuracy that the records produced represent complete and accurate copies of all records identified in this order that are in the actual or constructive control of the business entity. If the business entity does not produce all records identified in this order, it shall identify the records not produced. Failure to comply with this order shall support a finding of contempt of court.

Upon receiving the records from the business entity, the peace officer named herein shall file a return and inventory with the court indicating the records that have been received and the date and time upon which the records were received. The peace officer named herein may also file the original of the attestation of accuracy with the court.

IT IS FURTHER ORDERED:

1. That this Search Warrant and Order and application be **SEALED** until the completion of the law enforcement criminal investigation, that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Order to be served on any service provider or other person.
2. That **Google, LLC** NOT take adverse action against the subject accounts, such as disabling or terminating the accounts, because of this warrant.
3. Pursuant to 18 U.S.C. §2705(b) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), that **Google, LLC**, **NOT disclose the existence of this search warrant and court order to the subscriber for a period of one year**, unless otherwise ordered by a court of competent jurisdiction, as notification of the warrant may have an adverse result, as defined in 18 USC §2705(b)(1)-(5), i.e., disclosure may endanger the life or physical safety of an individual; allow flight from prosecution; allow destruction of or tampering with evidence; allow intimidation of potential witnesses; and/or would otherwise seriously jeopardize an investigation or unduly delay a trial.

THE INFORMATION SO ORDERED is related to the active and ongoing criminal investigation by YOUR AGENCY and in accordance with 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41, the records and information requested are or have been used as a means of committing a criminal offense or would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court; the seizure of which is expressly required, authorized, or permitted by statute; or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

Based upon the affidavit of the above-named Affiant, which is incorporated by reference, I am satisfied that there is probable cause to believe there is a legal basis and also legal authority for the issuance of this Search Warrant and Court Order for Production of Records. You are therefore authorized to execute this Search Warrant according to these terms and as otherwise permitted by law.

Dated this **\_\_\_\_\_day of \_\_\_\_\_\_\_\_\_ 20\_\_**, at \_\_\_\_\_\_\_.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

JUDGE / MAGISTRATE

1. [↑](#footnote-ref-1)