COUNTY OF LARIMER )

) SS IN THE COMBINED COURT

STATE OF COLORADO )

**AFFIDAVIT FOR SEARCH WARRANT**

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

Judge

Affiant, **OFFICER/DETECTIVE NAME**, a commissioned police officer, being duly sworn, deposes and says that I have probable cause to believe that in the premises, or is within the possession, custody, or control of described premises:

GOOGLE INC. is a corporation located at 1600 Amphitheatre Parkway, Mountain View, California 94043, United States. Google Inc. and is also a corporation doing business in Colorado and registered with the Colorado Secretary of State under registration number 20031277465.

There is now located within said premises or in actual or constructive control of said business, certain records which would be material evidence in a subsequent criminal prosecution in this state or another, namely:

**DETAILED DESCRIPTION OF WHAT ACCOUNT/PROFILE YOU WANT SEARCHED**

The below listed documents for **ACCOUNT NAME / EMAIL**

(eg. missmelaney@gmail.com) for the timeframe of **MONTH DAY, YEAR** through **MONTH DAY, YEAR:**

**(ADD/DELETE THE BELOW BASED ON CASE FACTS)**

1. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, telephone numbers and other personal identifiers;
2. All past and current usernames, account passwords, and names associated with the account;
3. Any telephone numbers which have been registered with Google for the purposes of sending and receiving messages and for accessing Google+ through mobile applications.
4. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
5. All IP logs and other documents showing the IP address, date, and time of each login to the account;
6. All IP logs and other documents showing the IP address and/or telephone number, date, and time of each message send to and from to the account;
7. All data and information associated with the profile page, including photographs, videos, “bios,” and profile backgrounds and themes;
8. All Stream Postings and Private Messages sent, received, or archived by the account, and all photographs, images or videos included in those Stream Updates and Private Messages;
9. All photographs, videos and images in the user profile for the account;
10. All location data associated with the account, including all information collected by Google+ for use with Google+ Local and other associated location based services;
11. All data and information that has been deleted by the user;
12. A list of all of the people that the user maintains in Circles and all people who maintain the user in their Circles;
    1. A list of all users that the account has blocked;
    2. All privacy and account settings;
13. All records of Google searches performed by the account within Sparks, including all past searches saved by the account;
14. All information about connections between the account and third-party websites and applications;
15. All records pertaining to communications between Google and any person regarding the user or the user’s Google+ account, including contacts with support services, and all records of actions taken, including suspensions of the account.
16. Any and all location data and information from the use of GoogleMapsTimeline, including but not limited to routes taken, check in data, points of interest selected, map searches, and any information related to places, timeline, traffic, and settings.

Further, I have probable cause to believe that the requested items constitutes property which has been stolen or embezzled, or which are designed or intended for use as a means of committing a criminal offense, or which are or have 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.

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

**STATE PROBABLE CAUSE HERE IN PARAGRAPH FORM – NOT IN BOLD**

**IT IS YOUR RESPONSIBILITY TO KNOW THE FOLLOWING INFORMATION, WHAT IT MEANS, AND BE ABLE TO EXPLAIN IT IN BASIC TERMS IF CALLED UP BY THE COURT TO DO SO. ALSO, YOU MUST READ THROUGH THE INFORMATION AND MAKE SURE IT APPLIES.**

The Internet is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even where the two computers are located in the same state.

Internet Service Providers (“ISPs”): Most individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers (“ISPs”). Comcast, AOL, and Time Warner are examples of some of the larger and better-known ISPs. Other ISPs include private entities such as corporations, universities, and government agencies. Among other services, ISPs provide their customers with access to the Internet using telephone, cable, Digital Subscriber Line (“DSL”), or other types of telecommunications lines.

Internet Protocol Address (“IP address”): An Internet Protocol (“IP”) address is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots (e.g., 149.101.10.40). Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet service providers (“ISPs”) assign IP addresses to their customers’ computers. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection (so-called “dynamic IP addressing”), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called “static IP addressing”). Either way, the IP address used by a computer attached to the Internet must be unique for the duration of a particular session; that is, from connection to disconnection. ISPs typically log their customers’ connections, which means that the ISP can identify which of their customers was assigned a specific IP address during a particular session.

Uniform Resource Locator or (URL) is the global address of documents and other resources including videos on the World Wide Web.

Uploading is the sending of data from a local system to a remote system such as a server or another client with the intent that the remote system should store a copy of the data being transferred, or the initiation of such a process.

Webcast is a media presentation distributed over the Internet using streaming media technology to distribute a single content source to many simultaneous listeners/viewers. A webcast may either be distributed live or on demand. Essentially, webcasting is “broadcasting” over the Internet.

This affiant knows that Google is an online content website that was launched on the internet in 1998. Since their debut Google currently maintains a variety of online content products and services and they are ranked as one of the most frequently visited web sites in the United States.

In 2011 Google introduced the social media web site Google+. Google+ offers many of the same popular features as other social media web sites and currently has millions of user profiles. Google+ shares many of the same account management features of Google including account management, access logs, data retained and information collected.

This affiant knows that Google+ allows an individual to create an account with his or her own page called a profile. Google+ profiles can include a short biography, photos of themselves and location information. Google+ also allows their users to send and receive messages, upload and link video and interact with other users through video conferencing. These features are described in more detail below:

A Google+ user can interact with other Google+ users in many ways. To send messages to users, post information, comment on hosted videos or upload videos to the site an individual must register for an account within the web site. To create a user account for Google+ an individual is transferred to Google.com and must create a user account within the Google network. Once an individual creates an account with Google the individual may also change this username, password, and name without having to open a new Google account.

Google asks individuals to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user’s full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user account, Google may retain information about the date and time at which the user’s profile was created, the date and time at which the account was created, and the Internet Protocol (“IP”) address at the time of sign-up. 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 a given Google account.

An individual with a Google+ account can post a personal photograph or image (also known as an “avatar”) to his or her profile, and can also change the profile background or cover photo for his or her account page. In addition, Google+ users can post “bios” and other information to their profile pages.

Google also keeps IP logs for each user of the Google+ web site. These logs contain information about the user’s logins to Google+ including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

Google+ users can post text, images, videos and links to external web sites within their profile for others to view in an area called their “Stream”.

Google+ users can use their user accounts to post messages to their profiles for others to view. Individuals can also use their Google+ accounts to send messages to their “Circles”. A Google+ “Circle” is a distribution list that a user maintains and organizes. A user can add, remove or censor a member of a particular “Circle” or several “Circles”. Within a “Circle” a user can send and receive messages with other users, post photographs, videos and links to external web sites.

Google+ users can initiate a “Hangout” which is an area to initiate video conferencing with several other Google+ users. Within a “Hangout” a Google+ user is able to interact with other users in a live real-time format or they are able to create a webcast that is hosted by Google+. Webcasts created in Google+ can be stored in a Google+ user’s profile and can be retrieved, shared and rebroadcasted at anytime. Whenever a Google+ user initiates a “Hangout” session, Google+ generates a unique URL that can be shared with others so that they can view the session. Or the “Hangout” can be broadcasted and stored on YouTube.

A Google+ user is also able to search using the Google.com search engine within the web site in a feature called “Sparks”. “Sparks” is a front-end to Google Search, enabling users to identify topics they might be interested in sharing with others. "Featured interests" sparks are also available, based on topics others globally are finding interesting.Sparks helps to keep users informed of the latest updates on the topics of their interest.

An individual can also access the Google+ web site through mobile applications that allow an individual to use the aforementioned features of Google+ through a mobile device such as a smart phone, and cellular telephone. An individual using a mobile device can communicate with other users through an application called “Messenger”. “Messenger” facilitates communication and the sharing of media between users through a smart phone application or through standard short messaging service (SMS) messaging.

A Google+ user can also use their mobile device to broadcast location data to the Google+ web site to use Google+ Local. Google+ Local users broadcast location data submitted to the web site to reveal trending information, restaurants, popular businesses and items of interest based on information stored on a user’s particular profile.

Google+ offers a wide variety of privacy settings that allow a user to expand or restrict the amount of information that is visible on their profile to friends or the general public. Regardless of the privacy settings selected by the User, the User’s information is shared with Google.com and Google.com’s marketing affiliates.

If a Google+ user does not want to interact with another user on Google+, the first user can “block” the second user from following his or her account.

Google+ users can connect their Google+ accounts to third-party websites and applications, which may grant these websites and applications access to the users’ public Google+ profiles.

Google users have the ability to store location data information about where users have been, trips users have taken, searches users have run in the Google Maps application under GoogleMapsTimeline. This data is being stored unless the user actively disables location history on the device and in the timeline application. If the service is enabled, it is actively connecting to GPS satellites in order to provide instant location data for a user. This data may be recoverable for a period of years through the user profile information stored with Google.

In some cases, Google+ users may communicate directly with Google and Google+ about issues relating to their account, such as technical problems or complaints. Social-networking providers like Google+ 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.

Therefore, the computers of Google are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Google+, such as account access information, transaction information, and other account information.

This affiant knows that individuals involved in the commission of criminal acts often utilize technology such as cellular telephones, smart phones, personal data assistants, laptop computers, personal media players, handheld radios, radio broadcast scanners and social media websites such as Google+ in order to: plan and discuss criminal activities, coordinate the movement of persons involved or property utilized or taken from a location and to relay information about law enforcement officials during the commission of a criminal act.

People who commit criminal offenses together often communicate prior to or following that crime. It is common for people to communicate via Google+ postings, emails and private messages. Individuals who have committed crimes or who are closely associated with such people often communicate about the details of what occurred (the crime itself), the stress/angst relating to the event, the quality and quantity of evidence possessed by the authorities, and fears about being apprehended.

Google.com is a provider of electronic communication service 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.com for compliance with the SCA, to serve this warrant via fax and/or email at the number and/or email address provided by the Google.com – Security Department

Due to the above-mentioned facts I believe that the records and documents held by GOOGLE Inc. for the email address of **ACCOUNT NAME / EMAIL**

(eg. missmelaney@gmail.com) would be of material aid in this investigation. I would now ask the Court to grant the warrant requested. I also request the Court ask that GOOGLE Inc. and/or its subsidiaries **not** disclose/notify the user/subscriber of the issuance of this search warrant. Disclosure to the user/subscriber could impede an investigation or obstruct justice.

***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 filing of charges based on this 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 Fort Collins Police Department records, conversations with fellow officers, personal observations and interviews. I am a sworn police officer with the Fort Collins Police Department. I have been trained at the state, and local levels with regard to my duties. I am authorized by law to execute search and arrest warrants in the State of Colorado.

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

Affiant

Dated this \_\_\_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_ at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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

Judge

COUNTY OF LARIMER )

) SS IN THE\_\_\_\_\_\_\_\_\_\_\_\_\_COURT

STATE OF COLORADO )

**SEARCH WARRANT**

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

Judge

The court, upon review of a sworn affidavit filed by **OFFICER/DETECTIVE NAME,** a commissioned police officer, 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 your actual or constructive possession or control:

GOOGLE INC. is a corporation located at 1600 Amphitheatre Parkway, Mountain View, California 94043, United States. Google Inc. and is also a corporation doing business in Colorado and registered with the Colorado Secretary of State under registration number 20031277465.

**DETAILED DESCRIPTION OF WHAT ACCOUNT/PROFILE YOU WANT SEARCHED**

The below listed documents for **ACCOUNT NAME / EMAIL**

(eg. missmelaney@gmail.com) for the timeframe of **MONTH DAY, YEAR** through **MONTH DAY, YEAR:**

**(ADD/DELETE THE BELOW BASED ON CASE FACTS)**

1. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, telephone numbers and other personal identifiers;
2. All past and current usernames, account passwords, and names associated with the account;
3. Any telephone numbers which have been registered with Google for the purposes of sending and receiving messages and for accessing Google+ through mobile applications.
4. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
5. All IP logs and other documents showing the IP address, date, and time of each login to the account;
6. All IP logs and other documents showing the IP address and/or telephone number, date, and time of each message send to and from to the account;
7. All data and information associated with the profile page, including photographs, videos, “bios,” and profile backgrounds and themes;
8. All Stream Postings and Private Messages sent, received, or archived by the account, and all photographs, images or videos included in those Stream Updates and Private Messages;
9. All photographs, videos and images in the user profile for the account;
10. All location data associated with the account, including all information collected by Google+ for use with Google+ Local and other associated location based services;
11. All data and information that has been deleted by the user;
12. A list of all of the people that the user maintains in Circles and all people who maintain the user in their Circles;
    1. A list of all users that the account has blocked;
    2. All privacy and account settings;
13. All records of Google searches performed by the account within Sparks, including all past searches saved by the account;
14. All information about connections between the account and third-party websites and applications;
15. All records pertaining to communications between Google and any person regarding the user or the user’s Google+ account, including contacts with support services, and all records of actions taken, including suspensions of the account.
16. Any and all location data and information from the use of GoogleMapsTimeline, including but not limited to routes taken, check in data, points of interest selected, map searches, and any information related to places, timeline, traffic, and settings.

The court also hereby finds probable cause to believe that the requested items constitutes property which are or have 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.

The grounds for this search warrant are set forth in the accompanying Affidavit for search warrant, a true and correct copy of which is attached hereto and is incorporated herein by reference. The court being satisfied that the grounds for the issuance of this search warrant exist and that there is probable cause to believe that they exist:

IT IS FURTHER ORDERED:

1. That this Search Warrant and Order and application be **SEALED** until the filing of charges based on this 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. After charges are filed, disclosure of this Search Warrant and Order and application is governed by Crim. P. 55.1.
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.

Therefore, you are commanded to execute and serve this warrant at any time within fourteen days from the date hereof pursuant to Stored Communication Act Google, Inc. is ordered comply with the requirements of this search warrant upon receiving a copy. An inventory and return shall be provided to the undersigned judge upon receipt of the records by the investigating officer named herein.

Dated this \_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_ at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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

Judge