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

-This search warrant mask is specifically for the search of Google for the anonymized data of devices located within a search zone

-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.

- 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 use this type of warrant with caution. This warrant should only be used when you: (1) have the ability to analyze the data that Google will provide, (2) can identify a precise location and timeframe for the offense, and (3) the identity of the perpetrator is unknow. If you have not used this warrant before, please consult with someone that has before moving forward. \*\*\*

To request this information from Google, you need two pieces of information –

1. A general location. This is the “geofence” piece of the warrant. This is the geographical area that you want Google to search for the presence of a device that reported location information. The “geofence” can be defined to Google in one of two ways –
	1. MOST PREFERED: A polygon shape with the latitude and longitude of each point of the polygon. For example, if you drew a square over the area you wanted search, provide Google with the latitude and longitude of each corner of the square. Multiple locations can (and probably should) be used.
	2. A latitude and longitude point with a given radius. For this location, simply provide the latitude and longitude of your scene/location to be searched and then a radius (provided in meters), given latitude xx.xxxxxx, given longitude -xx.xxxxxxx, and a 50 meters radius.
2. A timeframe. While this is typically fovused on the time of the crime, it is important to request a Significant enough data set to be able to determine what devices are regularly seen in the area and “belong” there, to be used as a control sample. By identifying those devices, it is easier to isolate suspicious devices that may be related to the crime. For a single event, 18 – 24 hours of data works well. The time of the crime should be at the center of the timeframe. For 18 hours – 9 hours either side of the crime, for 24 hours – 12 hours either side of the crime).

It is critical to explain in the PC statement that you are only going to receive anonymized data with this warrant. In order to be able to associate that data to a person, you will have to request further information from Google, via another search warrant. Take some time to explain to the Judge that your goal is to see if devices that are suspicious in nature are in the immediate area of the crime scene at the time of the crime. Once a device is identified; through the “Device ID”; you will need to draft a second search warrant, with the additional probable cause, to request more data on the “Device ID(s)” with the intention of identifying the user/suspect.

Identifying the user. Once a device is identified through the initial data, a second warrant is necessary for all of the location related information for the device spanning a greater period of time (3 to 6 months is recommended). It can be useful to ask for any related account information, but there is no guarantee it will be available; as the user may have deleted it. However, there will still be location data associated with the Device ID, as that data is not deleted by Google. Once you have the larger data set, it can be mapped providing a detailed pattern of life of the user. Through an analysis of the pattern of life, the user/suspect identification may be made.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*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**

**Service via Google’s Law Enforcement Request System (LERS) on-line**

**Service may be via email at uslawenforcement@google.com**

The following Identifying information according to the “**Production Protocol**” described below for Google accounts that reported a GPS, cellular, WiFi or Bluetooth sourced location history data generated from devices that reported a location within the geographic region bounded by the following coordinates dates and times “**Initial Search Parameters.**”

**Initial Search Parameters**

======================================

**Target Location 1**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Target Location 2**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Target Location 3**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Target Location 4**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Production Protocol**

======================================

* 1. Google shall query location history data based on the **Initial Search Parameters** (as described above).
	2. For each location point recorded within the **Initial Search Parameters**, Google shall produce anonymized information specifying the corresponding unique Reverse Location Obfuscated IDs/Device IDs of all location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, Bluetooth beacons, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings (with captured time zone), data source and device type (platform), during the date and time period associated with specific device IDs; (the “**Anonymized List**”).
	3. Law enforcement shall review the **Anonymized List** to remove Reverse Location Obfuscated IDs/Device IDs that are not relevant to the investigation, for example, device’s that were not in the location for a relevant period of time, or device’s that remained at the location after law enforcement arrival. Law enforcement will also shortlist the Anonymized List by reviewing the time stamped location coordinates for each device and compare that against the known time and location information that is specific to this crime. Law enforcement will also compare the Anonymized List for each location and attempt to locate devices located at two or more identified locations.
	4. If additional location information for a given anonymized Reverse Location Obfuscated IDs/Device ID is needed in order to determine whether that anonymized Reverse Location Obfuscated IDs/Device ID is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that fall outside of the **Initial Search Parameters**. These contextual location coordinates may assist law enforcement in identifying anonymized Reverse Location Obfuscated IDs/Device IDs that were located outside the search locations, were not within the search locations for a long enough period of time, were moving through the search locations in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

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 is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state, or the seizure of which is expressly required, authorized or permitted by any statute of this state, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant is outstanding.

The facts tending to establish the grounds for issuance of a Search Warrant are as follows:

Affiant’s Experience:

BACKGROUND OF AFFIANT

Investigation:

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

#### Google Location History Data:

Based on my training and experience, I know most people in today’s society possess cellular phones and other connected devices (e.g. tablets, watches, laptops) used to communicate electronically. I know these devices are capable of sending and receiving communications in many different forms. I know most people carry cellular phones on their person and will carry them whenever they leave their place of residence. I know that cellular phones may include global positioning systems (GPS) and other technology for determining the location of the device.

I know a subject’s physical cellular phone often times does not retain all the data relevant to a specific crime. Portions of this data may only be on the Electronic Communications Service Provider’s server located in the subscriber’s account. Google services are often interconnected with a log-in to a Google account allowing access to many of the other Google services.

Google is also a company which provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the provider’s services can access his or her email account from any computer or smart phone/device connected to the Internet.

Google has developed an operating system for mobile devices, including cellular phones, watches and tablets known as Android, that has a proprietary operating system. 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 activate a new Android device.

I know nearly every Android powered device has an associated Google account. I also know that Apple iPhone’s supports several Google applications, such as Google Search, Gmail, Google Maps, and Google Drive, all of which require a Google account. I also know Google continuously tracks devices with an associated Google account.

Based on my training, experience and conversations I’ve had with other law enforcement officers and/or from reviewing documentation, I know that Google collects and retains location data on their servers (also known as the “Sensorvault” database) from Android enabled mobile devices, as well as devices supporting Google applications such as Google Search, Gmail, Google Maps, and Google Drive, so long as the location services of the phone are enabled. The location data gathered is stored forever, unless it is deleted by the user. 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, Bluetooth beacons, 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 not only 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 email access, but also when the user is not interacting with the device (e.g. applications running in the background).

Additionally, location information digitally integrated into images, videos, or other computer files sent via the cellular phone can further indicate the geographic location of the account’s user at a particular time. Digital cameras, including cameras built into a cellular phone, frequently store GPS coordinates in the metadata of image files, indicating where a photo was taken. These image files may be stored in the account user’s Google cloud storage.

Based on my training and experience, I know when a user activates a Google Account, Google will request an associated phone number for the user, to assist in password recovery if a password is forgotten or for security purposes.

Given that almost all cellular phones and connected devices are either supported by Google or support Google software and most people in today’s society carry a cellular phone or other connected device on their person at nearly all times, I believe it is likely the suspect(s) involved in this criminal investigation were in possession of at least one cellular phone/device, which was either powered by Android OS or had a cellular phone with a Google application.

Based on my training and experience, suspects involved in criminal activity will typically use cellular phones to communicate when multiple suspects are involved. I am also aware Android based cellular phones report detailed location information to Google, where the geo-location and electronic data is then stored on their servers.

The timeframe of the Google request identified in the **Initial Search Parameters** will allow investigators to see which Google device IDs were present in the geographic area prior to, during, and after the crime. The information provided by the extended timeframe and times when entering and exiting the geographical area will allow investigators to determine which Reverse Location Obfuscated IDs/Device IDs require further investigation and which ones do not. The initial Reverse Location Obfuscated IDs/Device IDs provided by Google do not include any subscriber information and is provided in an anonymized list.

I believe the information provided by Google will assist investigators in understanding a bigger geographic picture and timeline, which may tend to identify potential witnesses, as well as possibly inculpate or exculpate the account owners. I therefore believe that it is likely that a review of Google’s location history will help law enforcement in developing suspect(s) in the offense described above and provide possible witnesses to the crime.

As such, I am requesting a list of any Google anonymized Reverse Location Obfuscated IDs/Device IDs in a geographic area around the addresses identified in the **Initial Search Parameters** in particular, the geographical region(s) identified and the date(s) and time(s) specified. This Application seeks authority to collect certain location information related to Google Reverse Location Obfuscated IDs/Device IDs that were located within the Target Location(s) during the Date and Time Period (Anonymized List).

The information sought from Google regarding the Anonymized List will potentially identify which cellular phones/devices were near the location where the crime occurred and may assist law enforcement in determining which persons were present or involved in the crime under investigation.

Law enforcement shall review the Anonymized List to remove Reverse Location Obfuscated IDs/Device IDs that are not relevant to the investigation, such as devices that were not in the location for a sufficient period of time. If additional location information for a given Reverse Location Obfuscated IDs/Device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that fall outside of the target location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the target location, were not within the target location for a long enough period of time, were moving through the target location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

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 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.com 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 that has been filed with the court in this matter. 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, but those individuals are precluded from further dissemination prior to expiration of this order without an order of the court handling the case.
2. So as not to disrupt this ongoing investigation, Your Affiant also requests that this Court order Google 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 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 County of Larimer and 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**

**Service via Google’s Law Enforcement Request System (LERS) on-line**

**Service may be via email at uslawenforcement@google.com**

This Court also finds that there is probable cause to issue this Search Warrant pursuant to the provisions of 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1, §19-2-504, and Crim. P. 41, namely that this property is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state or federal court, or the seizure of which is expressly required, authorized or permitted by any statute of this state or the United States, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant is outstanding.

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

The following Identifying information according to the “**Production Protocol**” described below for Google accounts that reported a GPS, cellular, WiFi or Bluetooth sourced location history data generated from devices that reported a location within the geographic region bounded by the following coordinates dates and times “**Initial Search Parameters.**”

**Initial Search Parameters**

======================================

**Target Location 1**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Target Location 2**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Target Location 3**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Target Location 4**

**Date:** DATE

**Time Period (Mountain Standard Time):** TIMEthroughTIME

**Target Location:** ADDRESS

**Geographical area identified as:** Geographical area identified as a four sided polygon identified by at least three coordinates identified by following latitude/longitude points connected by straight lines:

Point 1: LATITUDE**,** LONGITUDE

Point 2: LATITUDE**,** LONGITUDE

Point 3: LATITUDE**,** LONGITUDE

Point 4: LATITUDE**,** LONGITUDE

GOOGLE MAP OF LOCATION [IF AVAILABLE]

**Production Protocol**

======================================

* 1. Google shall query location history data based on the **Initial Search Parameters** (as described above).
	2. For each location point recorded within the **Initial Search Parameters**, Google shall produce anonymized information specifying the corresponding unique Reverse Location Obfuscated IDs/Device IDs of all location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, Bluetooth beacons, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings (with captured time zone), data source and device type (platform), during the date and time period associated with specific device IDs; (the “**Anonymized List**”).
	3. Law enforcement shall review the **Anonymized List** to remove Reverse Location Obfuscated IDs/Device IDs that are not relevant to the investigation, for example, device’s that were not in the location for a relevant period of time, or device’s that remained at the location after law enforcement arrival. Law enforcement will also shortlist the Anonymized List by reviewing the time stamped location coordinates for each device and compare that against the known time and location information that is specific to this crime. Law enforcement will also compare the Anonymized List for each location and attempt to locate devices located at two or more identified locations.
	4. If additional location information for a given anonymized Reverse Location Obfuscated IDs/Device ID is needed in order to determine whether that anonymized Reverse Location Obfuscated IDs/Device ID is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that fall outside of the **Initial Search Parameters**. These contextual location coordinates may assist law enforcement in identifying anonymized Reverse Location Obfuscated IDs/Device IDs that were located outside the search locations, were not within the search locations for a long enough period of time, were moving through the search locations in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

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 otherwise ordered by the court, 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 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, **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