

SEARCH WARRANT

DATE FILED: December 13, 2018

IN THE (DISTRICT) (COUNTY) COURT, TELLER COUNTY, STATE OF COLORADO

CRIMINAL ACTION NUMBER 18-115

Whereas Commander Christopher Adams #1220 has made an Application and Affidavit to the Court for the issuance of a Search Warrant, and;

Whereas the application is in proper form and probable cause is found for the issuance of a Search Warrant to search the person(s) and or premises specified in the application.

THEREFORE, the applicant, and any other peace officer into whose hands this Search Warrant shall come, is hereby ordered, with the necessary and proper assistance, to enter and search within the next ten (10) days the person, premises, location and any appurtenances thereto, description of which is:

Google, Inc.
Google Legal Investigations
Support
1600 Amphitheatre Parkway
Mountain View, CA 94043

FILED IN THE COMBINED COURTS
OF TELLER COUNTY, COLORADO

DEC 14 2018

USER ACCOUNT: berke857@gmail.com, (719) 660-6179

The following person(s), property or thing(s) will be searched for, and if found seized:

See Attachment "B"

as probable cause has been found to believe that it:

- Is stolen or embezzled, or
- Is designed or intended for use in committing a criminal offense, or
- Is or has been used as a means of committing a criminal offense, or
- Is illegal to possess, or
- Would be material evidence in a subsequent criminal prosecution, or required, authorized or permitted by a statute of the State of Colorado, or
- Is a person, property or thing the seizure of which is expressly required, authorized or permitted by a statute of the State of Colorado, or
- Is kept, stored, transported, sold, dispensed, or possessed in violation of a statute of the State of Colorado under circumstances involving a serious threat to the public safety, or order, or to the public health.

(Mark "X" according to fact)

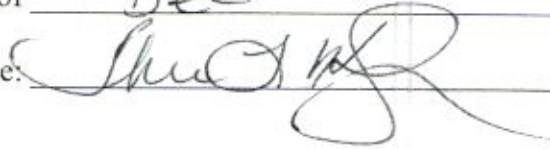
Furthermore, a copy of this warrant is to be left with the person whose premises or person is searched along with a list of any and all items seized at the time of its execution. If said person cannot be located or identified, a copy of the search Warrant and the list of property seized shall be left at the place from which the property was taken.

TK

Further, a return shall be promptly made to this Court upon the execution of this Search Warrant along with an inventory of any property taken. The property seized shall be held in some safe place until the Court shall further order.

Done by the Court this 13th day of Dec, 2018.

Judge:



APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

The undersigned, a peace officer as defined in 18-1-901 (3) (1), C.R.S. 1973 as amended, being first duly sworn on oath moves the Court to issue a Warrant to search those person(s) and/or premises known as:

Google, Inc.
Google Legal Investigations
Support
1600 Amphitheatre Parkway
Mountain View, CA 94043


USER ACCOUNT: berke857@gmail.com, (719) 660-6179

The undersigned states that there exists probable cause to believe that the following person, property or thing(s) to be searched for, and if found, seized will be found on the aforementioned person(s) and or premises and are described as follows:

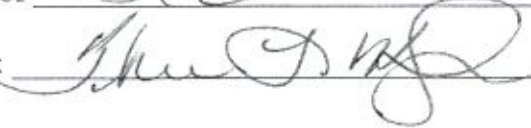
See Attachment "B"

The grounds for the seizure of said person(s), property or thing(s) are that probable cause exists to believe that it: () 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 (X) Is illegal to possess, or (X) would be material evidence in a subsequent criminal prosecution, or () Is a person, property or thing the seizure of which is expressly required, authorized, or permitted by a statute of the State of Colorado, or ()Is kept, stored, transported, sold, dispensed, or possessed in violation of the statute of the State of Colorado under circumstances involving a serious threat to the public safety, or order, or to the public health, (mark X according to the fact);

The facts submitted in support of this application are set for in the accompanying attachment designated as Attachment "A" which is attached hereto and made a part hereof.

Applicant: 
Law enforcement agency: Woodland Park Police Department
Position: Commander

Sworn and subscribed before me this 13th day of Dec 2018

Judge: 

TK

ATTACHMENT "A"

The following Affidavit is made in support of a request for a Search Warrant to be issued for the Google account for Kelsey Berreth.

Your Affiant is Commander Christopher Adams #1220, is a duly sworn and state certified police officer with the Woodland Park Police Department (WPPD) and has been employed as such since 2004 and is currently assigned to the Investigations Division.

All information contained in this affidavit can be found in Woodland Park Police Department Case Report No. 18-1530.

On 12-02-18, Corporal Currin was dispatched to 269 E. Lake Avenue in Woodland Park, Colorado for a welfare check. Cheryl Berreth called the Woodland Park Police Department reporting she has not heard from her daughter Kelsey Marie Berreth (DOB: 09/15/89). Cheryl stated this is highly unusual for Kelsey.

Cheryl told Cpl. Currin she has contacted her daughter's boyfriend Patrick Frazee and Patrick told her he has not heard from Kelsey since last Sunday 11/25/18. Cheryl told me Patrick and Kelsey have a one-year-old daughter together named . she is currently with Patrick. Cpl. Currin wrote in her report that Kelsey had no known planned vacations, two vehicles belonging to Kelsey were still parked at her residence, and there was a package at Kelsey's residence in the doorway along with a notice from Black Hills Energy.

Cpl. Currin called Patrick at 1315 hours at telephone number (719) 440-5759. This number was provided to Cpl. Currin by Cheryl as belonging to Patrick. Patrick told Cpl. Currin the last time he had any contact with Kelsey was a text message on the 25th. He told Cpl. Currin Kelsey was an employee at Doss Aviation in Pueblo, Colorado as a flight instructor. Patrick told Cpl. Currin that recently he returned all of Kelsey's belongings such as the spare key to her apartment, extra car key, a hand gun, and other personal belongings. He told Cpl. Currin they have grown apart and the extent of their relationship was their daughter. Cpl. Currin asked Patrick about depression and he denied Kelsie of having any.

At 1415 hours, Cpl. Currin, contacted Doss Aviation located at 1 William White Blvd. in Pueblo, Colorado (719) 423-8600. Cpl. Currin spoke to the security officer on duty, he advised he would return Cpl. Currin's call after he obtained any information. At approximately 1600 hours the security officer called and spoke with the dispatcher. The information obtained, Merle Merriak (719) 289-4514 is Kelsey's direct supervisor. He received a text message from Kelsey last Sunday 11/25/18 stating she was going out of state to check on grandma.

Cpl. Currin called Cheryl and she was not aware of her daughter traveling to see her grandmother. Cheryl told Cpl. Currin her mother has Parkinson's and Alzheimer's and is unable to communicate on the telephone. Cheryl told Cpl. Currin she was going to call her dad. Cheryl later told Cpl. Currin she contacted her father and he has not heard from Kelsey. Cheryl also told investigators Kelsey has never gone on a road trip to visit family without first notifying someone for her safety.

On 12-03-18, MPO Beth Huber conducted follow up related to this case. MPO Huber wrote in her report "On December 3, 2018 I, Officer B.Huber #3601 of Woodland Park Police Department, contacted Cheryl Berreth to see if she had heard from Kelsey. Cheryl informed me she had contacted Kelsey's direct supervisor this morning. Kelsey again did not show up to work. Kelsey's direct supervisor attempted to contact Kelsey with

no success. Cheryl said Patrick was attempting to work with Verizon to get text message transcripts in an attempt to determine if Kelsey was texting and to see if the texts would provide clues as to Kelsey's location.

I asked Cheryl if she would like to list Kelsey as missing. Cheryl said she would. Kelsey was entered into CCIC as a mission person, CIC: 124629897, NIC: M014878747 at 0944 hours.

I contacted Patrick to determine the last time he physically saw Kelsey. Patrick said the evening of 11/21 they spoke on the phone. Kelsey informed Patrick she wanted them to 'go their separate ways'. Kelsey said they had been growing apart. Patrick gave Kelsey all of her things back. Patrick said he and Kelsey talked about the custody of their daughter. Patrick said they both agreed they were both good parents and they would split custody 50/50. Patrick said Kelsey was not able to keep enough hours at work to maintain insurance for. Kelsey asked for Patrick to pick up on 11/22. Patrick went to Kelsey's residence to pick up. No one was home. Patrick ran some errands in town then returned to Kelsey's residence. Patrick saw Kelsey in the alley way leading to the residence. They spoke in the alley way where Kelsey gave to Patrick. Patrick said he and Kelsey talked on the phone on both Friday, Saturday, and Sunday. The last time Patrick talked with Kelsey she told him she was going to study. She did not tell Patrick where she was physically located that day. Patrick said on Sunday 11/25 Kelsey texted "Do you even love me?" to Patrick. Patrick texted her back telling her he did. Days later he received notice his reply did not go through. Patrick said if he had any further information regarding Kelsey. Patrick said she is a 7th Day Adventist and does attend church, but does not know where (maybe one in Colorado Springs). Patrick said Kelsey does have PO Box 811 in Florissant.

At approximately 1105 hours, I attempted to call Kelsey's phone number. It went straight to voice mail. Being concerned Kelsey may be suicidal due to the depression and rehabilitation mentioned by Patrick to Corporal Currin and the fact Patrick informed Corporal Currin he returned Kelsey's gun to her, I contacted Verizon in an attempt to determine Kelsey's last known location. I spoke with Jinny at Verizon. Kelsey's phone was last operational in Gooding, Idaho approximately 6.30 miles from the tower heading in a west/southwest direction on 11/25 at approximately 1713 hours. Dispatch contacted Gooding dispatch. Gooding dispatch said there has been no contact with Kelsey in Gooding or the surrounding four counties searching back to November 1, 2018."

Based on this information, I applied for a search warrant Kelsey's residence located at 269 E. Lake Ave, City of Woodland Park, County of Teller and State of Colorado. The warrant was signed by the Honorable Judge Kilgore. While searching the residence we recovered an iPad, Notebook with passwords and a Google email account for Kelsey Berreth berke857@gmail.com, and a Safeway receipt dated 11-22-18 at 1222 hrs. The Safeway purchase was for food items. There did not appear to be any signs of a struggle, altercations, or foul play. While searching the residence, I observed a 2006 Toyota Corolla and a red colored Chevrolet pick-up truck parked outside of the residence. The pick-up truck registered to Kelsey's mother and the Toyota registered to both Kelsey and Patrick.

On 12/04/18 the Colorado Bureau of Investigation (CBI) was requested to assist the WPPD due to the suspicious circumstances surrounding Kelsey's disappearance. CBI Agent's Gregg Slater and Kevin Torres responded to assist. CBI Agent Gregg Slater requested a second search of Kelsey's residence, curtilage, and vehicles. Agent Slater also arranged for a human decomposition K9 to respond to Kelsey's residence to assist with searching her residence and vehicles for the presence of human decomposition.

The two vehicles were towed from Kelsey's residence to the WPPD impound lot to be searched. A search warrant was obtained to search a 2006 Toyota Corolla belonging to Kelsey and Patrick. The Honorable Judge Billings-Vela signed the search warrant for the vehicle. A sock with a small amount of what appeared to be

blood was located on the front passenger seat. The K-9 indicated to the presence of human decomposition on the driver side rear bumper area.

A 2011 red colored Chevrolet Silverado pick-up truck parked at Kelsey's residence was searched at the WPPD after consent to search was obtained from Kelsey's mother (the registered owner). A Safeway receipt dated 11/22/18 at 1223 hrs. was located on the front passenger seat. The Safeway purchase was for flowers. A Wal-Mart receipt dated 11/22/18 at 0150 hrs. was located on the front passenger floor board. The Wal-Mart purchase was for Tum's Antacid and what appear to be over the counter stomach medicine.

Officer Huber requested an exigent cell phone ping for Kelsey's cell phone through Verizon. The ping revealed the following information:

- The last activity on Kelsey's phone was 11/25/18 at 17:13 hours located at 2037 S. 1800 E. Gooding, Gooding, ID. The ping was 6.38 miles west/southwest from the cell phone tower.
- On 11/25/18 at 17:11 hours there was an outgoing text message to 719-440-5759 (Patrick's Frazee's cell phone).

Gooding County Sheriff's Office Detective A. Boyer in Idaho was contacted regarding Kelsey's disappearance and cell phone ping. Detective Boyer and several law enforcement officers went to the location of the cell phone ping. Detective Boyer described the entire surrounding area of the cell phone ping to be a large steep gorge. Kelsey nor her cell phone were located.

On 12-04-18, Agent Kevin Torres of the Colorado Bureau of Investigation and Deputy Christopher Paulsen of the Teller County Sheriff's Office, currently assigned to the Federal Bureau of Investigation's Safe Street Team, met with Patrick to conduct a welfare check of the child. Patrick was asked if he would provide a formal statement regarding his knowledge, relationship, and details about his last interaction with Kelsey and her whereabouts. Patrick voluntarily agreed to provide a statement to Agent Torres but then changed his mind and requested an attorney before providing any information. Agent Torres asked Patrick if he knew what attorney he would consult so that a meeting could be arranged for him to provide a statement. Patrick stated he was going to meet with attorney Jeremy Lowe. Agent Torres impounded Patrick's cell phone which is described as a Moto M108D, Model Number XT1650-01.

On 12/04/18 CBI Agent Gregg Slater told me he spoke with Cheryl Berreth, Kelsey's mother. During that conversation Cheryl reported she last physically spoke with Kelsey on 11-22-18 at approximately 0900 at which time Kelsey stated that she (Kelsey, Patrick and) had gone out to check on a herd of cattle on 11-21-18. While driving back to Patrick's residence, Patrick became ill requiring Kelsey to drop him off at his residence, pick up some medication and take it back to Patrick. After doing so Kelsey and drove to Kelsey's home arriving at approximately 0400 on 11-22-18. Kelsey further reported She, baby and Patrick had plans to go out for thanksgiving dinner. The conversation quickly ended because ; diaper needed to be changed.

Chery told Agent Slater, on 11-22-18 at approximately 0915, she called Kelsey back and during that short conversation Kelsey spoke about Christmas gift lists and related items. Kelsey made no comments or statements to Cheryl regarding the dissolution of the relationship between Patrick and Kelsey. Kelsey provided no additional information and the conversation ended.

Cheryl told Agent Slater on 11/24/18 she (Cheryl) inadvertently dialed Kelsey's cell phone and hung up before anyone answered. A short time after the inadvertent call, Cheryl received a text message from Kelsey's phone stating, "I'm tied up, I'll call you later." Cheryl stated she never received a return phone call or text message from Kelsey.

Having not spoken to Kelsey since 11/22/18, Cheryl attempted to contact Kelsey on 12/02/18 via cell phone. Cheryl never received a response from Kelsey via text message or phone call, thus prompting Cheryl to text Patrick and inquire about Kelsey's whereabouts. Patrick called Cheryl from his cell phone (#719-440-5759) and said he and Kelsey had decided to end their relationship and go their separate ways, and said he and Kelsey were going to share custody of _____ 50/50. Patrick also stated he met with Kelsey on 11/22/18 at her residence and returned several items to her including a handgun, ammunition, keys to both vehicle (2006 Toyota Corolla & red Chevy pick-up truck), and keys to her residence. Patrick stated Kelsey also returned his personal property. Patrick said that was the last time he saw Kelsey, he did not know where she was, and he was going to give her some space.

Agent Slater asked Cheryl about Patrick and his behavior. Cheryl shared a story regarding the birth of _____ was born three weeks early and required some extra medical care. The special medical care prevented Kelsey from having _____ in her hospital room upon her birth. Patrick was very upset about this because he believed the first few hours of birth needed to be spent with mother and father for bonding purposes. Patrick became so upset and verbally abusive with the nursing staff that Social Services was notified. _____ was removed from the care of Patrick and Kelsey until a safety evaluation could be done to determine if Kelsey was being physically abused by Patrick. Cheryl stated Patrick later stated he should have "killed" the nurse that reported them and then again joked about the incident at _____ first birthday.

Cheryl told Agent Slater, Kelsey has never gone this long without contacting family, especially her. Kelsey does not have a history of disappearing, running away, or leaving without a trace. Cheryl stated she believes Kelsey is deceased. Cheryl also told Agent Slater she believed Patrick may have been using Kelsey's cell phone to communicate with her (Cheryl) because the text messages were fragmented. Cheryl stated Kelsey uses complete sentencing in her text messages and some of the last text messages she received from Kelsey were fragmented.

On 12/04/18 I received copies of bank records from Kelsie's credit union, ENT. The records contained transactions for Kelsey's bank account for the month of November and for the first four days of December. The last transaction on Kelsie's bank activity was on 11/22/18. This transaction was for the purchase of food items at Safeway previously described. No other physical financial transactions were made on Kelsey's ENT account since 11/22/18. It should be noted there are numerous transactions, both deposits and withdrawals, on Kelsie's bank records, but cease on 11/22/18.

Due to the fact that both modes of transportation for Kelsey were located at her residence it is unlikely she traveled anywhere far from her residence on her own will. No other vehicles belonging to Kelsey are known by family members or neighbors of Kelsey. No indication was observed in Kelsey's residence that indicate she had planned to be gone for any period of time.

After speaking with Agent Torres he told me Google keeps account records for its users and the data collected from Google users can be very beneficial to help determine a pattern of life, provide location services, and internet search history. Agent Torres directed me to look at Google privacy policies located at <https://policies.google.com/privacy>. I reviewed the privacy policies and learned the following information. It should be noted an email address for Kelsey Berreth was found in her password book during the search of her residence on 12/03/18 and is as follows; berke857@gmail.com

Historical Google Account Records

Based on my prior training and experience and after reviewing Google's privacy policy (<https://policies.google.com/privacy>), I am aware users of iOS operating system mobile devices, such as

TK 7

iPhone 6 containing cellular phone number (719)660-6179, IMEI 35445506827378 and account user identifier, which this affidavit seeks a search warrant for, commonly have an associated account with Google, Inc., which is believed to be berke857@gmail.com

When a user purchases and activates a mobile device one of the initial prompts during the set-up phase is to associate a Google Gmail e-mail account with the device. The purposes of this account are to facilitate a password reset in the event the consumer forgets their passcode, pattern unlock, or password. If the consumer does not have an existing Gmail account, the operating system prompts the user to create a new account. Whether the Gmail account is new or existing the association of the account with the device allows Google to collect and store information relevant to this criminal investigation. This information includes, by way of example and not limitation;

- 1. Account Information - User name, primary email address, secondary email addresses, connected applications and sites, and account activity including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;**

Google maintains information about their customers including primary email addresses, secondary email 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. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the victim, her mobile device, and/or computers;

- 2. Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device.**

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. I believe this information will identify any previously unknown cell phones or other mobile devices associated with the victims's account and/or known device(s);

- 3. User attribution data - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s);**

I know that Google may 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;

- 4. Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;**

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. I believe 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;

- 5. Contacts - All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;**

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

- 6. Documents - All user created documents stored by Google;**

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. I believe 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;

- 7. Gmail - All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;**

As noted previously, 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. I believe these messages would reveal motivations, plans and intentions, associates, and other co-conspirators;

TK 9

8. Google Photos - All images, graphic files, video files, and other media files stored in the Google Photos service;

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. I believe a review of these images would provide evidence depicting the victim, his/her associates and others providing information on who she might have been with that will help find her. I also believe these image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing investigation;

9. Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period 11/21/2018 to 12/04/2018;

Google collects and retains location data from Android and iOS 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 email access. I believe this data will show the movements of the victims'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 investigation;

10. Play Store - All applications downloaded, installed, and/or purchased by the associated account and/or device;

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;

11. Search History - All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;

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, these searches are differentiated by the specific type of search a user performed into categories. 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.

I believe a review of the victim's search history would reveal information relevant to the ongoing investigation by revealing what information the victim sought and when she sought it;

12. Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device;

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 voicemail 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 voicemail messages and the associated transcriptions;

13. Google Home (Smart Speaker & Home Assistant) - All information related to Google Home including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times;

Google Home is a brand of smart speaker developed by Google, Inc. Google Home Speakers have microphones that are always listening that enable users to speak voice commands to interact with services through Google's intelligent personal assistant called Google Assistant. A large number of services, both in-house and third-party, are integrated, allowing users to listen to music, control playback of videos and photos, and receive news updates entirely by voice. Google Home devices also have integrated support for home automation, letting users control smart home appliances with their voice. Multiple Google Home devices can be placed in different rooms in a home for synchronized connectivity. The data collected by Google Home devices are stored remotely on Google's servers. Users can access their Google Home account and associated data by way of a connected smart phone application or through their Google account. I believe the Google Home related data, including the archived audio recordings may be used to refute and corroborate statements, and may be important in identifying potential witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing a timeline and provide context and intent.

14. Android Auto - All information related to Android Auto including device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs and text messages, voice actions, and all location data;

Android Auto is a mobile device application developed by Google that allows enhanced use of an Android device within a vehicle equipped with a compatible head unit. Once the Android device is connected to the head unit, the system enables it to broadcast applications (apps) with a simple, driver-friendly user interface onto the vehicle's dash display, including GPS mapping/navigation, music playback, text messages (SMS), voice calls, and web search. The system supports both touchscreen and button-controlled head unit displays,

TLC 11

although hands-free operation through voice commands is encouraged. Once the user's Android device is connected to the vehicle, the Android mobile device will have access to several of the vehicle's sensors and inputs, such as GPS, steering-wheel mounted buttons, the sound system, directional microphones, wheel speed, compass, and other vehicle data.

I believe the Android Auto related data and the iOS related data, including the historical geo-location data (GPS, compass, speed, direction) may be important in establishing locations and activities of possible witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing the driver and occupants of a particular vehicle, refute and corroborate statements, and can be used to establish a timeline and provide context and intent.

For the reasons outlined above, I believe probable cause exists to seize and examine the specified records held by Google, Inc. associated with the account **iPhone 6 containing cellular phone number (719)660-6179, IMEI 35445506827378 and account user identifier berke857@gmail.com**. The records to be searched for and seized are more particularly described as;

- 1) All subscriber records or other information regarding the identification of the account subscriber(s) and/or user(s), to include but not limited to:
 - a) Full name;
 - b) Physical address;
 - c) Telephone numbers;
 - d) Device identifiers to include but not limited to:
 - i) MAC addresses;
 - ii) Electronic Serial Numbers ("ESN");
 - iii) Mobile Electronic Identity Numbers ("MEIN");
 - iv) Mobile Equipment Identifier ("MEID");
 - v) Mobile Identification Numbers ("MIN");
 - vi) Subscriber Identity Modules ("SIM");
 - vii) Mobile Station International Subscriber Directory Number ("MSISDN");
 - viii) International Mobile Subscriber Identifiers ("IMSI");
 - ix) International Mobile Station Equipment Identities ("IMEI");
 - e) Records of session times and durations;
 - f) The creation time and date of the account;
 - g) The IP address used to register the account;
 - h) The length of service of the account;
 - i) Login and usage IP addresses associated with session times and dates;
 - j) Account status;
 - k) Alternative email addresses;
 - l) Methods of connecting;
 - m) Log files;
 - n) Billing information to include, but not limited to, the means and source of payment (including any credit or bank account numbers);
- 2) All device information associated with the account;

- 3) Any passwords or other protective devices in place and associated with the Accounts, which would permit access to the content stored therein;
- 4) The types of service(s) utilized;
- 5) All search and browsing history associated with the account;
- 6) All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- 7) All communications delivered through the Google service known as Gmail including email communications and alternate or backup email addresses associated with the accounts;
- 8) All web search history, including, but not limited to, mobile and desktop browser searches;
- 9) All application (app) activity;
- 10) All voice and/or audio activity captured;
- 11) All Google map location history, saved and/or frequent locations, favorite and/or starred locations including, but not limited to, searches conducted using the Google maps service;
- 12) All incoming or outgoing phone calls, voicemails, including voicemail content in any and all incoming or outgoing text message history, together with the content thereof to include SMS, MMS, Chat logs, or any other form of text message communication to include, but not limited to, communication for the Google, Inc. service known as Google Voice;
- 13) All forms of communication including, but not limited to, audio, video text message and or chat delivered through the Google, Inc. service known as Google Hangouts;
- 14) All downloaded, installed, and or purchased applications through the Google, Inc. service known as Google Playstore;
- 15) All posts, status updates, and or other information including photographs and/or video for the Google, Inc. service known as Google Plus;
- 16) All photographs and/or videos that are contained and or were uploaded in the Google Inc. service known as Google Photos, Google Plus, or any other Google, Inc. service designed to store video, photographs, and/or data, including the metadata for each file;
- 17) All electronic files, folders, media, and or data uploaded and/or contained on the Google, Inc. service known as Google Drive;
- 18) Location history: all location data whether derived from global positioning system (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advanced or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings;

TK13

- 19) For all Google accounts that are linked to the Subject Email Account by cookies, recovery email address, or telephone number, provide:
- a) Names (including subscriber names, user names, and screen names);
 - b) Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
 - c) Local and long distance telephone connection records;
 - d) Records of session times and durations and IP history log;
 - e) Length of service (including start date) and types of service utilized;
 - f) Telephone number(s) or device identifiers to include but not limited to:
 - i) MAC addresses;
 - ii) Electronic Serial Numbers ("ESN");
 - iii) Mobile Electronic Identity Numbers ("MEIN");
 - iv) Mobile Equipment Identifier ("MEID");
 - v) Mobile Identification Numbers ("MIN");
 - vi) Subscriber Identity Modules ("SIM");
 - vii) Mobile Station International Subscriber Directory Number ("MSISDN");
 - viii) International Mobile Subscriber Identifiers ("IMSI");
 - ix) International Mobile Station Equipment Identities ("IMEI");
 - g) Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports));
 - h) Means and source of payment for such service (including any credit card or bank account number) and billing records.



ATTACHMENT "B"

The following items, if located during the search will be recovered as evidence.

- 1) All subscriber records or other information regarding the identification of the account subscriber(s) and/or user(s), to include but not limited to:
 - a) Full name;
 - b) Physical address;
 - c) Telephone numbers;
 - d) Device identifiers to include but not limited to:
 - i) MAC addresses;
 - ii) Electronic Serial Numbers ("ESN");
 - iii) Mobile Electronic Identity Numbers ("MEIN");
 - iv) Mobile Equipment Identifier ("MEID");
 - v) Mobile Identification Numbers ("MIN");
 - vi) Subscriber Identity Modules ("SIM");
 - vii) Mobile Station International Subscriber Directory Number ("MSISDN");
 - viii) International Mobile Subscriber Identifiers ("IMSI");
 - ix) International Mobile Station Equipment Identities ("IMEI");
 - e) Records of session times and durations;
 - f) The creation time and date of the account;
 - g) The IP address used to register the account;
 - h) The length of service of the account;
 - i) Login and usage IP addresses associated with session times and dates;
 - j) Account status;
 - k) Alternative email addresses;
 - l) Methods of connecting;
 - m) Log files;
 - n) Billing information to include, but not limited to, the means and source of payment (including any credit or bank account numbers);
- 2) All device information associated with the account;
- 3) Any passwords or other protective devices in place and associated with the Accounts, which would permit access to the content stored therein;
- 4) The types of service(s) utilized;
- 5) All search and browsing history associated with the account;
- 6) All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- 7) All communications delivered through the Google service known as Gmail including email communications and alternate or backup email addresses associated with the accounts;

- 8) All web search history, including, but not limited to, mobile and desktop browser searches;
- 9) All application (app) activity;
- 10) All voice and/or audio activity captured;
- 11) All Google map location history, saved and/or frequent locations, favorite and/or starred locations including, but not limited to, searches conducted using the Google maps service;
- 12) All incoming or outgoing phone calls, voicemails, including voicemail content in any and all incoming or outgoing text message history, together with the content thereof to include SMS, MMS, Chat logs, or any other form of text message communication to include, but not limited to, communication for the Google, Inc. service known as Google Voice;
- 13) All forms of communication including, but not limited to, audio, video text message and or chat delivered through the Google, Inc. service known as Google Hangouts;
- 14) All downloaded, installed, and or purchased applications through the Google, Inc. service known as Google Playstore;
- 15) All posts, status updates, and or other information including photographs and/or video for the Google, Inc. service known as Google Plus;
- 16) All photographs and/or videos that are contained and or were uploaded in the Google Inc. service known as Google Photos, Google Plus, or any other Google, Inc. service designed to store video, photographs, and/or data, including the metadata for each file;
- 17) All electronic files, folders, media, and or data uploaded and/or contained on the Google, Inc. service known as Google Drive;
- 18) Location history: all location data whether derived from global positioning system (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advanced or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings;
- 19) For all Google accounts that are linked to the Subject Email Account by cookies, recovery email address, or telephone number, provide:
 - a) Names (including subscriber names, user names, and screen names);
 - b) Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
 - c) Local and long distance telephone connection records;
 - d) Records of session times and durations and IP history log;
 - e) Length of service (including start date) and types of service utilized;
 - f) Telephone number(s) or device identifiers to include but not limited to:
 - i) MAC addresses;
 - ii) Electronic Serial Numbers ("ESN");

- iii) Mobile Electronic Identity Numbers ("MEIN");
- iv) Mobile Equipment Identifier ("MEID");
- v) Mobile Identification Numbers ("MIN");
- vi) Subscriber Identity Modules ("SIM");
- vii) Mobile Station International Subscriber Directory Number ("MSISDN");
- viii) International Mobile Subscriber Identifiers ("IMSI");
- ix) International Mobile Station Equipment Identities ("IMEI");
- g) Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports));
- h) Means and source of payment for such service (including any credit card or bank account number) and billing records.

Based on the aforementioned information, your Affiant respectfully requests that a Search Warrant be issued for

Google, Inc.
Google Legal Investigations
Support
1600 Amphitheatre Parkway
Mountain View, CA 94043

USER ACCOUNT: berke857@gmail.com, (719) 660-6179

AFFIANT: 

Commander Christopher Adams #1220
Woodland Park Police Department

JUDGE: 

DATE: 12/13/18 TIME: 7:00 p.m.