

SEARCH WARRANT

DATE FILED: December 17, 2018

IN THE (DISTRICT) (COUNTY) COURT, TELLER COUNTY, STATE OF COLORADO
CRIMINAL ACTION NUMBER 18-119

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 COURT
OF TELLER COUNTY, COLORADO

DEC 18 2018

SHEILA GRIFFIN
CLERK OF COURT

USER ACCOUNT: mrs.lee10210@gmail.com or 208-731-6679 between the dates of November 21, 2018 – December 17, 2018.

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.

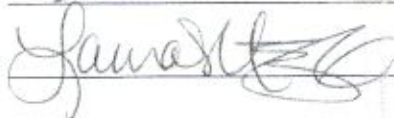
Further, a return shall be promptly made to this Court upon the execution of this Search Warrant along with an inventory of any property taken. The property seized shall be held in some safe place until the Court shall further order.

STATEMENT OF NON DISCLOSURE

The Court also orders Google, Inc not to disclose the existence of this search warrant to any person, including the subscriber, other than its personnel essential for compliance with the execution of this warrant. The Court further orders Google, Inc to continue to maintain the account of mrs.lee10210@gmail.com in an open and active status so as not to disrupt this ongoing investigation.

Done by the Court this 17 day of December, 2015.

Judge:



(DISTRICT) (COUNTY) COURT, TELLER COUNTY, STATE OF COLORADO
CRIMINAL ACTION NUMBER 18-119

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: mrs.lee10210@gmail.com or 208-731-6679

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 17 day of December 2018.

Judge: 

ATTACHMENT "A"

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. I have participated in other law enforcement investigations, and I have relied on other investigators with more training and experience than I have in electronic records.

This affidavit is being submitted in support of a search warrant to be issued for the Google account believed to be utilized by Krystal Lee ("Lee"). Based on the fact below, your Affiant submits that probable cause exists to believe the Google Account mrs.lee10210@gmail.com, also possibly referenced by cellular telephone 208-731-6679 more fully described in the respective Attachment B, contains evidence, fruits, and instrumentalities of a crime. Therefore, your Affiant requests the requested search warrants be issued.

The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officials, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

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

Facts in support of probable cause *Background of those mentioned in this affidavit*

Patrick Frazee, date of birth 04/18/1986, is a Colorado resident, and is the last known person to see Kelsey Berreth alive. Frazee works as a rancher and is involved in the ferrying of horses. Your affiant was unable to locate any prior felony criminal history for Frazee.

Krystal Jean Kenney Lee, date of birth 04/04/1986, is an Idaho resident who lives at 3551 E 3200 North, Kimberly, Idaho and appears to be a Registered Nurse (RN). Your affiant was unable to locate any prior felony criminal history for Lee. Investigators believe Lee has known Patrick Frazee for over twelve years, and has traveled to Colorado in the past, other than as it relates to this investigation.

Summary of a Missing Person Investigation in Colorado

On December 2, 2018 Cheryl Berreth reported to the Woodland Park Police Department (WPPD) that she had not been able to communicate with her daughter Kelsey Berreth, date of birth 09/15/1989, in over a week and requested WPPD conduct a welfare check at her residence. Officers responded to Kelsey's residence in Woodland Park, Colorado and were unable to locate Kelsey. Berreth's family reported that it would be highly unusual for Berreth to leave without informing any of her friends or family.

Officers later contacted the father of Kelsey's 14 month old child, Patrick Frazee, who claimed that he met Kelsey on November 22nd, 2018 when the two exchanged custody of their child. Frazee reported he had not seen her since then. Ultimately, Frazee is the last person investigators have found that saw Berreth alive. Frazee told officers that his relationship with Kelsey was over and during the custody exchange he returned items that belonged to her, including a handgun, residence keys, and other personal belongings.

Patrick reported that he was in cell phone communication with Berreth through November 25th, 2018. Investigators applied for, and were granted search warrants related to Frazee's and Berreth's historical call detail records, and historical cell site information. Indeed, investigators located messages between Berreth's phone and Frazee's phone between November 22nd and November 25th, 2018. A further analysis of those records revealed that Berreth's cellular telephone likely traveled from Colorado to Idaho via I-70 during the evening of November 24th and/or the morning of November 25, 2018. The last activity for Berreth's phone was on November 25, 2018 at 1713hrs approximately 6.38 W/SW from a cell phone tower in Gooding, Idaho. Based on the last location of Berreth's cell phone, members of the Gooding County Sheriff's Office were requested to search this area for her cell phone with negative results. These details will be further discussed below.

Investigators searched the residence of Berreth several times. During one of the lawful searches, crime scene analysts from the Colorado Bureau of Investigation (CBI) found traces of blood based on Blue Star Forensic latent blood stain reagent tests for the presence of blood in the bathroom of the residence. In summary, blood was located on the base of the toilet, bathtub, towel rack, door handle, ceiling, and other areas of the bathroom. A DNA profile was developed, and investigators learned that the blood matched the profile for Berreth, and additionally one unknown male profile and one unknown female profile were also developed from various areas of the bathroom. It is unlikely the male profile is Frazee's based on lab reports.

During the search of Berreth's residence, investigators were unable to find Berreth's wallet, identification card, car keys, cell phone, or her purse. Both of her known vehicles were parked outside of her residence, and were seized by investigators. Her toiletries, clothing, and other personal items were still inside the apartment. On or about December 13, 2018, investigators applied for, and were granted a search warrant for the residence of Frazee. That warrant was executed, and although some items of evidentiary value were collected, the body of Berreth was not found. Frazee has obtained legal counsel, and has not interviewed with investigators at this time.

Development of information related to Krystal Lee

Based on call detail analysis from Frazee's cell phone, investigators learned that Frazee was communicating with 208-731-6679 during the dates surrounding Berreth's suspicious disappearance. Open source and other information, including a recorded phone interview conducted by FBI Agents on December 14th, 2018, with Lee, revealed that the 6679 phone number belonged to Lee. In short, Lee provided materially false and misleading information.

During the interview, Lee was asked when the last time she communicated with Frazee was, and responded by saying she wasn't sure, and would have to look at her phone. When pressed by the interviewing Agents, she responded "within a month, month and a half". She then stated that she was actually at Frazee's residence in Colorado on Saturday, November 24th, 2018 from approximately 9am-5pm to look at a horse, and arrived back home in Utah on Sunday, November 25, 2018 around 10:30am or 11:00am after driving during the night. Lee stated she took this trip by herself.

Lee stated she had never met Berreth, and had "no idea" who she was until she saw the online new articles about her disappearance. Lee did know that Frazee had an infant daughter, and it is unusual she would not know who the mother of the child was.

As mentioned above, there are call records between Frazee and Lee (who used 208-731-6679) on the 24th of November of 2018 around 7:23am, 10:47am, 11:39am, 1:06pm, 5:21pm when Lee said she was at Frazee's residence. Your Affiant submits that it would be unlikely for Lee to be talking with Frazee if they were

together at his residence, as people tend to communicate in person and not telephone when they are with each other.

On her return trip, she stated she drove on I-70 through Salt Lake City to return home. Lee borrowed a black vehicle from a friend, but could not remember the make or model of the car. Lee stated Frazee did not ask her to take Berreth's phone and dispose of it.

Investigators applied for, and were granted a search warrant for the call detail records and historical cell site information related to Lee's cell phone. In summary, a review of the information revealed that Lee's phone was connected to not only a cell phone tower, but a sector of that tower that would service Berreth's residence. The tower is some distance from Frazee's residence, and likely would not service his residence. This fact tends to lead investigators that Lee was not at Frazee's residence like she stated, and lied during her interview. Additionally, investigators learned that Lee's phone traveled back to Idaho on the 24th and 25th of November. Coincidentally, Lee's phone was connected to the exact same tower and sector in a remote area of the Colorado/Utah border on the morning of November 25th, 2018.

Specifically, Lee's phone was connected to the tower at approximately 4:13am, 4:17am, and 4:23am. Berreth's phone was connected to the tower at approximately 4:11am, and 4:16am. It is reasonable to assume, based on this information, that Lee was likely in possession of Berreth's cellular telephone.

Also during the return trip to Idaho, Lee appeared to be in communication with Frazee, including shortly after the last activity of Berreth's cellular telephone.

Also on the 4th of December, investigators seized the cell phone belonging to Frazee. Also on the 4th of December, Lee obtained a new cellular telephone according to her phone records. The acquisition of Lee's new phone will be discussed below in more detail.

I know from training and experience that when people make road trips, they sometimes tend to keep documents such as receipts for fuel, meals, and other items that could provide inculpatory or exculpatory information related to this investigation. Usually these items are kept inside a vehicle, or inside a residence.

Interview of Chad Lee, Krystal Lee's ex-husband

Chad Lee, an Idaho resident, was married to Krystal Lee for the last approximately 8 years, but was recently divorced in the summer of 2018. Chad and Krystal still share a home in Idaho, and they raise two children together.

Lee lied to Chad about her whereabouts during November 24th and 25th of 2018. Initially, she told Chad she was going to a birthday party at a friend's house in Idaho, then told Chad she was going to help her friend Megan move, also in Idaho. Investigators ultimately learned that Lee drove Megan's 2012 Black Volkswagen Jetta to Colorado on or about these dates.

After Lee was interviewed on the phone around December 14th, 2018 by FBI Agents, Chad stated she was very nervous when she talked to him about the phone call, and finally told Chad she had actually gone to Colorado to see a horse she and Patrick own together around Thanksgiving. Lee also stated that she thought someone "set her up". Based on the facts Lee concealed her whereabouts to Chad, combined with lying to FBI Agents, it is reasonable to believe Lee's statements are unreliable at best.

Chad also stated that Krystal and Patrick dated in college, and that they were involved in a sexual relationship during at least 2016, and possibly into 2017. Chad did not want any of the details of the affair, and did not

have further information regarding their relationship to provide. Lee did not mention her sexual and romantic relationship with Patrick to investigators, and based on the circumstances, investigators consider this information to be both material and relevant, and that Lee purposely concealed this information.

On or about December 4, 2018, Lee told Chad she could not find her cell phone, and asked Chad to take her into town to purchase a new one, which ultimately was a replacement Samsung device. Based on phone records obtained from Verizon Wireless, investigators knew Lee had a Samsung device during the time period of Berreth's disappearance. Again, the timing of her new phone acquisition in Idaho is approximately the same as when Patrick's phone was taken by law enforcement in Colorado.

Chad knows the Lee has an email account, and had her account information was stored in Chad's phone contacts under "Krystal Lee" as "mrs.lee10210@gmail.com". Your affiant knows from training and experience that Samsung phones utilize an Android operating system, which was created by Google. Most Android phones use a version that is mostly provided by Google and utilizes Google services.

Conclusion

In summary, Lee's trip to Colorado was coincidental with the disappearance of Berreth. Lee's false statement to investigators, Lee's cell phone information, and cell phone travel pattern further increases suspicion of her involvement in the disappearance of Berreth. Additionally, Lee's historical cell site information places her phone in the vicinity of Berreth's residence on the morning of the 24th of November. An unknown female DNA profile was obtained from Berreth's bathroom. It also appears, based on the phone records of Berreth and Lee, that their cell phones traveled back to Idaho at roughly the same time. Lee stated she did not know Berreth, and has never met her.

Lee has likely lied to FBI investigators, and her ex-husband that she currently lives with, about her whereabouts and purpose of her trip to Colorado.

Your Affiants knows from training and experience that 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, previous map/directions requests, provide historical location services, and internet search history. Your affiant also knows that people tend to communicate electronically, including email, and that sometimes receipts from purchases are sent via email. Such receipts, or other email messages, might further shed light on the purpose of Lee's trip to Colorado.

Historical Google Account Record Background

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

Samsung Device utilizing cellular phone number 208-731-6679, and the account user identifier which this affidavit seeks a search warrant for, commonly have an associated account with Google, Inc., which is believed to be **mrs.lee10210@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 suspect, 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 suspect'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;

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 suspect, 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 suspect's mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing 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 suspect's search history would reveal information relevant to the ongoing investigation by revealing what information the suspect 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, 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 **associated to a Samsung Device utilizing cellular phone number (208)-731-6679, IMEI 35445506827378 and account user identifier mrs.lee10210@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;
- 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.

STATEMENT OF NON DISCLOSURE


The Court also orders Google, Inc not to disclose the existence of this search warrant to any person, including the subscriber, other than its personnel essential for compliance with the execution of this warrant. The Court further orders Google, Inc to continue to maintain the account of mrs.lee10210@gmail.com in an open and active status so as not to disrupt this ongoing investigation.

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: mrs.lee10210@gmail.com or 208-731-6679

AFFIANT: 
 Commander Christopher Adams #1220
 Woodland Park Police Department

JUDGE: 

DATE: 12/17/12 TIME: 2:27pm

ATTACHMENT "B"

The following items, specific to the dates of November 21, 2018 – December 17, 2018, if located during the search will be recovered as evidence:

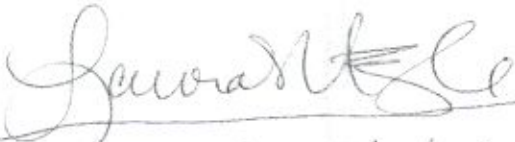
- 1) All subscriber records or other information regarding the identification of the account subscriber(s) and/or user(s), to include but not limited to:
 - a) Full name;
 - b) Physical address;
 - c) Telephone numbers;
 - d) Device identifiers to include but not limited to:
 - i) MAC addresses;
 - ii) 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.

STATEMENT OF NON DISCLOSURE

The Court also orders Google, Inc not to disclose the existence of this search warrant to any person, including the subscriber, other than its personnel essential for compliance with the execution of this warrant. The Court further orders Google, Inc to continue to maintain the account of mrs.lee10210@gmail.com in an open and active status so as not to disrupt this ongoing investigation.


County Court Judge 12/17/11