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

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

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

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

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

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

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

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

Case No:

COUNTY OF LARIMER ) IN THE COMBINED COURT

 ) SS

STATE OF COLORADO )

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

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

 JUDGE / MAGISTRATE

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

**Snap Inc.**

 **Custodian of Records**

 **2772 Donald Douglas Loop North**

 **Santa Monica, CA 90405**

**Served via email: lawenforcement@snapchat.com**

The following records, data, or information for Snap User identified as ACCOUNT NAME **(hereinafter known as the “subject account”)** between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Snapchat passwords, Snapchat security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
2. Additional Snapchat accounts that were registered to the email address and/or phone number(s) utilized to establish the account;
3. All Accounts associated by device or cookie, to include User ID, subscriber name, cellphone number and email address.;
4. All devices(s) used and otherwise associated with the subscriber’s account, including ESN, ICCID, IMSI, IMEI, and MAC address numbers and activation dates;
5. All activity logs for the account and all other documents showing the user’s posts and other Snapchat activities;
6. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them and any associated metadata [camera make, model, capture date and time, capture latitude and longitude, etc.] and original sized image associated with those images and videos;
7. All profile information; news feed information; status updates; links to videos, photographs, articles, and other items; notes; wall postings; friend lists, including past and present friends along with the associated friends’ Snapchat user identification numbers; groups and networks of which the user is a member, including the groups’ Snapchat identification number(s) and Snapchat identification number(s) of all group or network members; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Snapchat applications;
8. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending “Friend” requests;
9. All “check ins” and any other location information, including location history data;
10. All Future and Past “events” the user responded to;
11. All IP logs and associated port IDs, including all records of the IP addresses that logged into the account;
12. All records of the account’s usage of the “Like” and “Follow” features, including all Snapchat posts and all non-Snapchat webpages and content that the user has “liked” and/or “followed”;
13. All records of the account’s usage of the “Share” feature, including all Snapchat posts and all non-Snapchat webpages and content that the user has “shared”;
14. All information about the Snapchat pages that the account is or was a “fan” of;
15. All records of Snap searches performed by the account;
16. All information about the user’s access and use of Snapchat Marketplace;
17. The types of service(s) utilized by the user, the length of service(s) (including start date), and the means and source of any payments associated with the service(s) (including any credit card or bank account number);
18. All privacy settings and other account settings, including privacy settings for individual Snapchat posts and activities, and all records showing which Snapchat users have been blocked by the account;
19. All records pertaining to communications between Snapchat and any person regarding the user or the user’s Snapchat account, including contacts with support services and records of actions taken.

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

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

**Electronic Definitions**

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

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

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

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

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

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

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

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

**Snapchat Definitions**

Snapchat is headquartered in Venice, California, and owns and operates a free access social networking website of the same name that can be accessed at http://www.snapchat.com. Snapchat is an application for sending and receiving “self-destructing” messages, pictures, and videos.

A “snap” is a picture or video message taken and shared with other Snapchat users in real time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed it is deleted from the company’s system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaves the Chat screen, messages viewed by both the sender and the receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and “snaps” constitute “electronic communications”. While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared. Snap’s servers are designed to automatically delete an unopened Snap sent directly to a recipient after 30 days and an unopened Snap in Group Chat after 24 hours.

Snapchat Chat: A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat app using the Chat feature. Snapchat servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user’s chat settings. Snap’s servers are designed to automatically delete unopened one-to-one chats in 30 days. Users can also chat in groups. Chats sent in groups are deleted after 24 hours whether they are opened or not. A user can save a message in Chat by pressing and holding the message. The user can unsave the message by pressing and holding it again. This will delete it from our servers. Users can also delete chats sent to a recipient before the recipient has opened the chat or after the recipient has saved the chat.

Snapchat Location Data: If a user has device-level location services turned on and has opted into location services on Snapchat, Snapchat will collect location data at various points during the user’s use of Snapchat, and retention periods for location data vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the app settings.

Snapchat Memories: Memories is Snapchat’s cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone’s photo gallery in Memories. Content saved in Memories is backed up by Snap and may remain in Memories until deleted by the user. Users may encrypt their content in Memories (called “My Eyes Only”), in which case the content is not accessible to Snap and cannot be decrypted by Snap.

Snapchat Stories: A user can add Snaps to their “Story”. A Story is a collection of Snaps displayed in chronological order. Users can manage their privacy settings so that their Story can be viewed by all Snapchat users, their friends, or a custom audience. A user can also submit their Snaps to our crowd-sourced service “Our Story”, which enables their Snaps to be viewed by all Snapchat users in Search and Snap Map. Snap’s servers are designed to automatically delete a Snap in a user’s Story 24 hours after the user posts the Snap, but the user may delete part or all of the Story earlier. Submissions to Our Story may be saved for longer periods of time.

**Child Pornography/Child Exploitation Definitions**

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

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

**Statements Regarding Current Investigation**

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

**Relevant Background Information of Child Pornography**

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

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

**Relevant Background Information of Technology**

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

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

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

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

**Description of Snapchat**

Snapchat is headquartered in Venice, California, and owns and operates a free access social networking website of the same name that can be accessed at http://www.snapchat.com. Snapchat is an application for sending and receiving “self-destructing” messages, pictures, and videos.

A “snap” is a picture or video message taken and shared with other Snapchat users in real time. The sender of a snap has the option of setting a timer for how long a snap can be viewed. Once a snap has been viewed it is deleted from the company’s system and is no longer visible to the recipient. Snapchat users can send text messages to others using the Chat feature. Once a user leaves the Chat screen, messages viewed by both the sender and the receiver will no longer be visible. The application notifies other users when they are online so they can begin messaging each other. In addition, Snapchat users can send pictures to other users by utilizing the camera on their device. Pictures can also be sent from the saved pictures in the photo gallery of the device. Accessing a Snapchat account and “snaps” constitute “electronic communications”.

A user can also type messages, send photos, videos, audio notes, and video notes to friends within the Snapchat app using the Chat feature. A user sends a Chat message to a friend, and once it is viewed by both parties – and both parties swipe away from the Chat screen – the message will be cleared. Within the Snapchat app itself, a user can opt to save part of the Chat by tapping on the message that he or she wants to keep. The user can clear the message by tapping it again.

“Our Stories” is a collection of user-submitted “snaps” from different locations and events. A Snapchat user, with the location services of their device turned on, can contribute to a collection of snaps regarding the event. For example, multiple different Snapchat users at a rave could all contribute to the same “Our Stories” collection by sharing their snaps, even if they do not know each other. Users can also view “Our Stories” events if they are not actually present at the event by subscribing to the story. In addition to “Our Stories,” a Snapchat user can keep a sort of photo/video diary using the “Story” feature. Each snap in a “Story” documents the user’s experience. Based on the user’s privacy settings, the photos and videos added to a “Story” can be viewed either by everyone on Snapchat or just the user’s friend. Stories are visible to other users for up to 24 hours.

In addition to photos, videos, “snaps” and stories, “Snapcash” is an online money transfer service offered by Snapchat. The actual business platform is run by “SquareUp,” the distributor of a mobile credit card reader and application Square Register. Snapcash can be used to transfer money between Snapchat users using a linked, U.S.-issued Visa or MasterCard debit card only; using credit cards is not permitted. Snapcash can only be sent to other users who have a linked debit card. Snapcash has a $250 weekly limit but can be upgraded to a $2,500 weekly limit. Users who upgrade have to provide their full name, date of birth, and Social Security number.

While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

Snapchat asks users to provide basic contact and personal identifying information to include date of birth. When a user creates an account they make a unique Snapchat username. This is the name visible to other Snapchat users. An email address is required to register a Snapchat account, and a new user must also provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code which must be entered before proceeding with the registration step. However, a user may elect to bypass entering a phone number so one may not always be present in the user’s account. Snapchat also retains the account creation date.

Snapchat stores device information such as the model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. Snapchat also collects unique device identifiers such as the Media Access Control (MAC) address and the International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event the Snapchat user’s application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.

Snapchat has a “Group Stories” feature allowing multiple users to contribute photos and videos to the same “Story,” a collection of posts that stay viewable for a limited amount of time. Snapchatters can name their group story and invite other users and “friends” by username to add content. The group Stories will disappear if 24 hours pass without a user adding a new photo or video.

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

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

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

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

***Further requests:***

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

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

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

AFFIANT

This affidavit was sworn to and subscribed in my presence this DATE day of MONTH 2020 at \_\_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

 ) SS

STATE OF COLORADO )

# SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS

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

 Judge / Magistrate

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

**Snap Inc.**

**Custodian of Records**

**2772 Donald Douglas Loop North**

**Santa Monica, CA 90405**

**Served via email: lawenforcement@snapchat.com**

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

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

The following records, data, or information for Snapchat User identified as ACCOUNT NAME **(hereinafter known as the “subject account”)** between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Snapchat passwords, Snapchat security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
2. Additional Snapchat accounts that were registered to the email address and/or phone number(s) utilized to establish the account;
3. All Accounts associated by device or cookie, to include User ID, subscriber name, cellphone number and email address.;
4. All devices(s) used and otherwise associated with the subscriber’s account, including ESN, ICCID, IMSI, IMEI, and MAC address numbers and activation dates;
5. All activity logs for the account and all other documents showing the user’s posts and other Snapchat activities;
6. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them and any associated metadata [camera make, model, capture date and time, capture latitude and longitude, etc.] and original sized image associated with those images and videos;
7. All profile information; news feed information; status updates; links to videos, photographs, articles, and other items; notes; wall postings; friend lists, including past and present friends along with the associated friends’ Snapchat user identification numbers; groups and networks of which the user is a member, including the groups’ Snapchat identification number(s) and Snapchat identification number(s) of all group or network members; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Snapchat applications;
8. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending “Friend” requests;
9. All “check ins” and any other location information, including location history data;
10. All Future and Past “events” the user responded to;
11. All IP logs and associated port IDs, including all records of the IP addresses that logged into the account;
12. All records of the account’s usage of the “Like” and “Follow” features, including all Snapchat posts and all non-Snapchat webpages and content that the user has “liked” and/or “followed”;
13. All records of the account’s usage of the “Share” feature, including all Snapchat posts and all non-Snapchat webpages and content that the user has “shared”;
14. All information about the Snapchat pages that the account is or was a “fan” of;
15. All records of Snap searches performed by the account;
16. All information about the user’s access and use of Snapchat Marketplace;
17. The types of service(s) utilized by the user, the length of service(s) (including start date), and the means and source of any payments associated with the service(s) (including any credit card or bank account number);
18. All privacy settings and other account settings, including privacy settings for individual Snapchat posts and activities, and all records showing which Snapchat users have been blocked by the account;
19. All records pertaining to communications between Snapchat and any person regarding the user or the user’s Snapchat account, including contacts with support services and records of actions taken.

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

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

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

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

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

IT IS FURTHER ORDERED:

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

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

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

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

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

JUDGE / MAGISTRATE

1. [↑](#footnote-ref-1)