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

-This search warrant mask is specifically for the search of a Cybertip received from the internet crimes against children (ICAC) task force and obtain subscriber data for related IP addresses.

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

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

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

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

*United States v.* *Ackerman*, 831 F.3d 1292 (10th Cir. 2016) states that if NCMEC is a government agency. So, if NCMEC views an image without the electronic service provider first viewing the image then the government has illegally searched the suspects files under the Fourth Amendment. This warrant will cure that illegal search in that we can argue inevitable discovery.

There is a circuit split on whether the electronic service provider can have a computer identify the image (via hash value, PhotoDNA, Google’s hashing program, etc.) or if a person must view the image. Our circuit has not made a determination on whether hash value identification is good enough or not so in the abundance of caution, if a human with the electronic service provider has NOT reviewed the image then we need to get a court order to open the image. See *United States v. Ringland*, 966 F.3d 731 (8th Cir. 2020); *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018). *But See, United States v. Wilson,* 13 F.4th 961 (9th Cir. 2021).

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

Case No:

COUNTY OF LARIMER ) IN THE COMBINED COURT

 ) SS

STATE OF COLORADO )

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

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 thing to be searched, described as:

**ICAC/NCMEC CYBERTIPS(S)**

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

The following data is relevant to the criminal activity described in the affidavit, which is incorporated by reference:

1. Any Child Exploitative Material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j);
2. All other information reported in the cybertip, including:
3. Subscriber Information for any associated account, including any name, username, screen name, account number or identifier, address, phone number, or email address.
4. Any other account or service settings, preferences, or profile information included within the Cybertip.
5. Information relating to all dates and times on which the associated account accessed the reporting party’s network.
6. Any IP address from which the associated account accessed the reporting party’s network.
7. All content transmitted to and/or stored on the reporting party’s network, including:
8. Communications, including addressing and transmission data, contents, and attached files.
9. Stored files and data.
10. Published files and data.

**SUBSCRIBER DATA FOR RELATED INTERNET PROTOCOL ADDRESS**

INTERNET SERVICE PROVIDER

ADDRESS

SERVICE VIA

For the INTERNET SERVICE PROVIDER User identified as

* IP ADDRESS on DATE
* IP ADDRESS on DATE
* IP ADDRESS on DATE
* IP ADDRESS on DATE

The following records:

* Physical location of the IP address(es)
* IP address(es) Assignment Type
* Subscriber’s name
* Subscriber’s service and billing address
* Subscriber’s email account names
* Length of service including start date
* Types of Services Provided and Account Status
* Account Number
* Subscriber’s telephone number(s)
* Subscriber’s account number
* Subscriber’s account balance and payment information
* Instrument number or other subscriber number or identity, including a temporarily assigned network address
* Unique Device Identification Information related to any device associated with these IP address(es) at the date and times listed above, such as ESN, ICCID, IMSI, IMEI, MAC address numbers and activation dates.
* IP Address Access Logs

For which a search warrant may be issued upon one or more of the grounds set forth in Crim. P. 41 and CRS § 16-3-301, namely that this property has been used as a means of committing a criminal offense, the possession of which is illegal, and/or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court.

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.

**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 ICAC Cybertips**

The Internet Crimes Against Children (ICAC) Task Force is a nationwide task force tasked with investigating instances of child sexual exploitation and is overseen by the National Center for Missing and Exploited Children (NCMEC). The types of crimes investigated by ICAC can include, but are not limited to, the possession, distribution, and manufacturing of child sexual abuse material (CSAM); suspects traveling for the purposes of sexually assaulting a child; child prostitution and human trafficking; child luring or enticement; and any other crime (both state and federal) that involves the sexual exploitation of children and intertwines with technology. The national ICAC Task Force is broken down into regions with Colorado law enforcement agencies falling under the Colorado Regional ICAC Task Force. The headquarters for the Colorado Region is located within the Colorado Springs Police Department.

When an internet service provider (ISP) or electronic service provider (ESP) has information related to possible child exploitation, a report is made to the NCMEC. NCMEC processes the information - which in each case can vary from just a single IP address and one image to voluminous account-related data and gigabytes of files - and generates a Cybertip report. In some cases, the reporting party or a NCMEC analyst will conduct basic analysis (such as open-source searches) of some of the information to assist law enforcement in deconfliction or for determining if the incidents are related to other Cybertips. NCMEC next estimates the jurisdiction or nexus of the investigation based upon the suspect’s or the victim’s electronic or geographic identifiers as provided in the Cybertip. The Cybertip and associated files are then forwarded to the appropriate regional ICAC Task Force who assigns it to the local police agency to investigate.

How CSAM files are detected by service providers can vary. If CSAM files are discovered by an employee of the service provider or if CSAM is reported to them by a member of the public, the suspected images are typically reviewed by an employee and then reported to NCMEC as required by Federal mandate. However, based on my experience as an ICAC investigator, which includes attending meetings and trainings where representatives from some service providers have given presentations, I believe due to the increasing incidents of internet child sexual exploitation activity and the severity of the material involved, some service providers are opting to automate the process of identifying suspected CSAM using proprietary software technology.

In practice, this means that instead of an employee of the service provider actually inspecting the suspected CSAM material included in a Cybertip, a software program flags and reports the suspected CSAM. But the software only “knows” to flag a particular file as suspected CSAM because in the past a human actually viewed a copy of that file and classified it as CSAM or otherwise as reportable suspected child exploitation material to NCMEC.

This brings us to the concept of hash matching, which is essential to understand, as it explains the overall reliability and accuracy of Cybertip reporting to NCMEC:

On many NCMEC Cybertip reports, the cover page states, *"NCMEC Incident Type is based on NCMEC's review of the information or uploaded files in this report OR a 'Hash Match' of one or more uploaded files"*. Therefore, I am aware that many Cybertips NCMEC receives from internet service providers involve suspected CSAM files identified by hash value matching technologies.

A hash value is a unique numerical value assigned to a file. A hash value for a particular file is the equivalent of its DNA. Several different algorithms are commonly used to hash-identify files, including Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1). Hash values are a very reliable method of authenticating files. It can be concluded with an extremely high degree of certainty that two files sharing the same hash value also share identical content. Based on my training and experience, I know it is more likely that two humans would share the same biological DNA than for two files to share the same hash value. If even one bit (the smallest measure of data in a file) of a file is changed, the entire hash value of that file changes completely.

From experience, I know both government and private entities have created MD5 and SHA-1 hash value libraries representing confirmed CSAM image and video files. The MD5 and SHA-1 values contained in these libraries have been viewed and confirmed as CSAM or child sexual exploitation material by law enforcement or private service provider employees. To my knowledge, these libraries are used by many service providers to automatically flag suspected CSAM to prevent their illegal dissemination and to protect the privacy of child victims. When a photo or video is uploaded to a service provider’s server, the hash value of the content is compared to the lists of known CSAM hashes. A positive match will flag the content for reporting to NCMEC. The actual suspected content may or may not be reviewed by an employee of the company prior to reporting to NCMEC as this process can be automated without human interaction. It bears mentioning that there are hundreds or thousands of different service providers. Each service provider has its own process for complying with the federal CSAM reporting mandate, and a service provider may change that process from time to time. I have not researched the processes the different service providers use, and I cannot say what hash value libraries various providers use or how they were developed.

ESPs do not merely report hash values of suspected CSAM to NCMEC, they also report a limited amount of content analysis to NCMEC. This includes reporting on whether any victim who appears in a suspect file is prepubescent or pubescent and whether the suspected abuse depicted in the file involves a sexual act or a lewd display. The fact that some ESPs routinely make these content determinations when they report suspected CSAM to NCMEC is an indicator that the reported image has at some point in time been viewed by a person and determined to constitute CSAM.

After an incident is reported to NCMEC and disseminated to the appropriate regional task force and agencies, the Cybertip report – and the suspected CSAM files – can be accessed via a secure online portal called the ICAC Database System (IDS). There, ICAC investigators who have been vetted are able to download the Cybertip reports and files locally for use in their investigation.

**Statements Regarding Current Investigation**

On INSERT DATE, NCMEC (National Center for Missing and Exploited Children) transmitted the following ICAC/NCMEC CYBERTIP #(s), which include file(s) of sexually exploitative material, to AGENCY NAME via the ICAC (Internet Crimes Against Children) online portal:

ICAC/NCMEC CYBERTIP # originating from ELECTRONIC SERVICE PROVIDER

 ICAC/NCMEC CYBERTIP # originating from ELECTRONIC SERVICE PROVIDER

 ICAC/NCMEC CYBERTIP # originating from ELECTRONIC SERVICE PROVIDER

 ICAC/NCMEC CYBERTIP # originating from ELECTRONIC SERVICE PROVIDER

I reviewed the ICAC/NCMEC CYBERTIP(s) and associated records provided by ICAC, but did not review the associated CSAM file(s). Although these ICAC/NCMEC CYBERTIP(s) involve CSAM file(s) that were not viewed by ELECTRONIC SERVICE PROVIDER prior to reporting to NCMEC, the CSAM file(s) were identified as such by ELECTRONIC SERVICE PROVIDER because they possess hash values that match databased hash values of files that were previously viewed and identified by either law enforcement or private entities as being CSAM. Therefore, I have probable cause to believe the CSAM file(s) included in these ICAC/NCMEC CYBERTIP(s) constitute sexually exploitative material, and as such I am seeking authorization to open the file(s) and view their contents for the purpose of pursuing a criminal investigation into this matter.

These ICAC/NCMEC CYBERTIP(s) involve CSAM file(s) that were identified as such through either the viewing of said CSAM file(s) by ELECTRONIC SERVICE PROVIDER, or because they possess hash values that match databased hash values of files that were previously viewed and identified by either law enforcement or private entities as being CSAM. Therefore, I have probable cause to believe the CSAM file(s) included in these ICAC/NCMEC CYBERTIP(s) constitute sexually exploitative material.

According to the above identified ICAC/NCMEC CYBERTIP(s), ELECTRONIC SERVICE PROVIDER identified the following Internet Protocol (IP) Address(es) as associated with the account used to transmit or possess the CSAM files:

* ELECTRONIC SERVICE PROVIDER identified the IP Address IP ADDRESS on DATE at TIME
* ELECTRONIC SERVICE PROVIDER identified the IP Address IP ADDRESS on DATE at TIME
* ELECTRONIC SERVICE PROVIDER identified the IP Address IP ADDRESS on DATE at TIME
* ELECTRONIC SERVICE PROVIDER identified the IP Address IP ADDRESS on DATE at TIME

IP addresses are assigned by ISPs (Internet Service Providers) to account users and devices, and in doing so ISPs record geolocation information associated with those IP address assignments, typically to include country, state, and city. ISPs make this IP address assignment and geolocation information available to databases such as ARIN (American Registry for Internet Numbers), which is one of the major global entities responsible for the management and distribution of IP addresses. Many reliable open-source databases exist that collect said IP address assignment and geolocation information from ISPs, ARIN, and other sources and provide it online.

The above identified ICAC/NCMEC CYBERTIP(s) provided information for IP ADDRESS showing it was assigned by INTERNET SERVICE PROVIDER with geolocation information associated to Fort Collins, Colorado. This information was derived by ICAC/NCMEC from reliable open-source database information. Using a reliable open-source database, I confirmed this IP address assignment and geolocation information through an online search.

I believe the records, data, or information requested herein will further this investigation by providing identifying information for the account holder associated with the IP address that was identified in the ICAC/NCMEC CYBERTIP(s) as being associated with the transmission or possession of CSAM file(s).

***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 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 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 INTERNET SERVICE PROVIDER 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 INTERNET SERVICE PROVIDER 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.

The executing law enforcement officer(s) may enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imaging, and analysis of any and all of the information described.

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 by telephone this DATE day of MONTH 20\*\* at \_\_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

 ) SS

STATE OF COLORADO )

**SEARCH WARRANT**

**ICAC/NCMEC CYBERTIPS(S)**

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

 JUDGE / MAGISTRATE

TO: ANY PEACE OFFICER AUTHORIZED BY LAW TO EXECUTE SEARCH WARRANTS IN THE STATE OF COLORADO.

The Court, upon review of a sworn affidavit filed by YOUR NAME HERE, a commissioned law enforcement officer, in support of the issuance of this search warrant, hereby commands you to search the following described property, namely:

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

ICAC/NCMEC CYBERTIP #: INSERT ICAC/NCMEC REPORT #

The following data is relevant to the criminal activity described in the affidavit, which is incorporated by reference:

1. Any Child Exploitative Material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j);
2. All other information reported in the cybertip, including:
3. Subscriber Information for any associated account, including any name, username, screen name, account number or identifier, address, phone number, or email address.
4. Any other account or service settings, preferences, or profile information included within the Cybertip.
5. Information relating to all dates and times on which the associated account accessed the reporting party’s network.
6. Any IP address from which the associated account accessed the reporting party’s network.
7. All content transmitted to and/or stored on the reporting party’s network, including:
8. Communications, including addressing and transmission data, contents, and attached files.
9. Stored files and data.
10. Published files and data.

For which a search warrant may be issued upon one or more of the grounds set forth in Crim. P. 41 and CRS § 16-3-301, namely that this property has been used as a means of committing a criminal offense, the possession of which is illegal, and/or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court.

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. You are therefore authorized to execute this Search Warrant according to these terms and as otherwise permitted by law.

Therefore, any member of law enforcement agency or a designee, and/or a computer forensic lab, are commanded to:

* Access the aforementioned Cybertip(s) and view, copy and maintain the above described data contained therein;
* The ability to use whatever means necessary to override any encryption or secure files encountered during the forensic examination of the phone, which may be destructive to the equipment. This could include having the item transferred to specialized forensic laboratories outside of the jurisdiction and/or the State of Colorado, if necessary.
* The ability to enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imagining, and analysis of any and all of the information described.

IT IS FURTHER ORDERED:

1. That this Search Warrant and Order and application be **SEALED** until the filing of charges based on this law enforcement criminal investigation, that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Order to be served on any service provider or other person. After charges are filed, disclosure of this Search Warrant and Order and application is governed by Crim. P. 55.1.

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. 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

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

 ) SS

STATE OF COLORADO )

**SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS**

**SUBSCRIBER DATA FOR RELATED INTERNET PROTOCOL ADDRESS**

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:

INTERNET SERVICE PROVIDER

ADDRESS

SERVICE VIA

This Court also finds that there is probable cause to issue this search warrant and court order for production of the following described records or information pursuant to the provisions of 18 U.S.C. §2703, the Colorado Rules of Criminal Procedure, CRS §16-3-301, §16-3-301.1, and §19-2-504, namely that this property has been used as a means of committing a criminal offense, the possession of which is illegal, and/or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court.

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

For the INTERNET SERVICE PROVIDER User identified as

* IP ADDRESS on DATE
* IP ADDRESS on DATE
* IP ADDRESS on DATE
* IP ADDRESS on DATE

The following records:

* Physical location of the IP address(es)
* IP address(es) Assignment Type
* Subscriber’s name
* Subscriber’s service and billing address
* Subscriber’s email account names
* Length of service including start date
* Types of Services Provided and Account Status
* Account Number
* Subscriber’s telephone number(s)
* Subscriber’s account number
* Subscriber’s account balance and payment information
* Instrument number or other subscriber number or identity, including a temporarily assigned network address
* Unique Device Identification Information related to any device associated with these IP address(es) at the date and times listed above, such as ESN, ICCID, IMSI, IMEI, MAC address numbers and activation dates.
* IP Address Access Logs

This warrant and court order for the production of records shall be served upon the business entity to whom it is directed within fourteen days after being signed by the court.

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 filing of charges based on this law enforcement criminal investigation, that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Order to be served on any service provider or other person. After charges are filed, disclosure of this Search Warrant and Order and application is governed by Crim. P. 55.1.
2. That INTERNET SERVICE PROVIDER 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 INTERNET SERVICE PROVIDER **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 and C.R.S. 16-3-301, 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. 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