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

-This search warrant mask is specifically for the search of a residence for digital devices and the subsequent search of the devices.

-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.

-There is ORANGE text below that explains and seek authorization to conduct onsite triage of digital devices. This section should not be used if examination of the devices is already in the warrant

-There is PURPLE text below which addresses at what time during the day a residential warrant may be served. By default, it must be served between 7AM and 7PM pursuant to C.R.S. 16-3-305(7)(a). Serving a warrant outside of that time period must be approved by the Court upon a showing of good cause.

- 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 FOR 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 in, on, or upon the address, together with the yard and curtilage thereof, described and identified as:

SPECIFICALLY DESCRIBE THE RESIDENCE

ADD PHOTO OF PHONE IF AVAILIABLE

There is now located within or upon said premises certain property that 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 that would be material evidence in a subsequent criminal prosecution in this state or another, namely:

ONLY INCLUDE THOSE ITEMS BELOW THAT ARE SUPPORTED IN THE PROBABLE CAUSE NARRRATIVE OF YOUR AFFIDAVIT

1. Documents and effects which tend to show possession, dominion and control over said premises, including but not limited to keys, mail envelopes, letters, rental/owner agreements and receipts, utility and telephone bills, photographs and film, prescription bottles, vehicle registration, insurance papers, address and telephone books, government notices and documents, papers bearing a person’s name, phone number or address;
2. Still and video photographs, and crime scene drawings.
3. Any electronic devices that are capable of analyzing, creating, displaying, converting, or transmitting electronic or magnetic computer impulses or data. These devices include, but are not limited to: desktop computers, laptop computers, personal data assistants, tablet devices, gaming consoles, personal digital assistant, or other stationary or portable devices capable of storing electronic data, such as USB storage devices, and memory cards.
4. Magnetic and optical storage devices capable of storing digital media include but not limited to discs, compact discs, DVDs, video cassettes, camera film and video film;
5. All telecommunications devices capable of sending and receiving telephone calls, SMS (text message) communications, or electronic communications, which include: wireless telephones, cellular phones, smart phones, iPhones, iPads, electronic tablets, etc.
6. Computer input and output devices.
7. Any written or printed material that provides instructions or examples concerning the operation of a computer system, computer software, and/or any related device. Any password, email address, account information, internet service provider (ISP) information, in the form of paper, documents or any other readable material, whether generated by handwriting, typewriter, computer, or any other device;
8. Photography equipment including but not limited to cameras, video cameras, and/or digital cameras, and storage media associated with such equipment including but not limited to undeveloped and/or unexposed film slides, negatives, videotapes, and/or magnetic/optical media used for storage of digital images.
9. Case specific items like cell phones, weapons, drugs, cash, bodily fluids or DNA, documents.
10. Other case specific items like cell phones, printers, scanners, email or electronic communication, documents, case related pictures, Internet data such as history, web sites visited, downloaded information.
11. Print media, photographs and printouts of child exploitative material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j).
12. Conduct a preview search of all located digital communications devices and digital storage media for sexual exploitation material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j), by use of manual or automated preview tools.
13. If computers or other digital devices are found, the investigator may acquire the contents of volatile memory related to computers and other digital communication devices that would tend to show the current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details necessary to preserve the true state of evidence.

The Affiant expressly requests that the search warrant authorize law enforcement to access, review and examine the devices seized pursuant to this warrant for data relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of CRIMINAL OFFENSE(S) perpetrated against NAME OF VICTIM OR LOCATION [IF APPLICABLE] (hereinafter “Subject Offense(s)”):

REVIEW THE LISTED CATEGORIES OF DATA, PLEASE REMOVE ANY CATAGORIES NOT SUPPORTED BY THE FACTS CONTAINED IN YOUR AFFIDAVIT

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. Evidence of software that may allow others to control a device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
5. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
6. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
7. Address books, contact lists, names, and lists of names and addresses of individuals who may have been contacted by use of the device or by other means for the purpose of committing violations of the Subject Offense(s);
8. Records, documents, invoices and materials that concern any accounts with an Internet Service Provider pertaining to Subject Offense(s);
9. Records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to Subject Offense(s);
10. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses pertaining to Offense(s) or that show who used, owned, possessed, or controlled the device;
11. Voicemail messages, text messages, MMS messages, Emails whether stored, received, or deleted as they pertain to pertaining to Offense(s), including username(s) and account information;
12. Photographs or images stored, sent, received or deleted, or documents containing photographs or images pertaining to Subject Offense(s);
13. Videos stored, sent, received or deleted pertaining to Subject Offense(s);
14. Notes, documents, records, or correspondence, pertaining to Subject Offense(s);
15. Electronic files, data, videos, and communications, including related metadata and location data, stored, sent, received or deleted from social media applications such as Facebook, Snapchat, Instagram, Twitter and/or any other third party programs or applications located on the device pertaining to Offense(s);
16. Global position system (GPS) data and any other geolocation data pertaining to Subject Offense(s);
17. Records of internet activity, including internet protocol (IP) addresses and Port IDs, firewall logs, transactions with internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses that show who used, owned, possessed, or controlled the device(s) pertaining to Offense(s);
18. Any Child Exploitative Material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j).

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST.

\*\*NOTE: Descriptions of the data, information, functions or services listed above are contained in Attachment A, which is incorporated herein by reference.

For which a search warrant may be issued upon one or more of the grounds set forth in the Colorado Rules of Criminal Procedure and CRS § 16-3-301, 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:

BACKGROUND OF AFFIANT

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

Based on this training and experience and conversations with others in law enforcement, I know the following about the following topics regarding this investigation:

Wireless Phone Capabilities

A cellular telephone is a handheld wireless device used for, inter alia, voice and data communication. A wireless telephone usually contains a “call log” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities, including storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet including websites, social media sites, bulletin boards, file sharing, and other Internet sites. It also includes GPS technology for determining the location of the device.

Cellular telephones have the ability to store and utilize data from external memory devices. These external digital storage devices, ie. microSD and SD cards, provide the device with the ability to capture and store an increased amount of data. By their design, they are removable and portable, allowing the stored information to be transported separately from the cellular telephone and/or utilized by additional cellular telephones and other digital devices.

Based on knowledge, training, and experience, Your Affiant knows that digital storage devices can store information for long periods of time. This information can sometimes be recovered with forensic tools. In addition, examining data stored on digital storage devices can uncover, among other things, evidence that reveals or suggests who possessed or used the computer or digital storage devices.

Based on the technology available to Your Affiant, obtaining the above described data and information will necessarily require an initial extraction of all of the data from the phone. This data, in raw form, is unreadable without the use of specific software. The extraction of the data will involve processing the data through the software, and a report containing only the data listed in the warrant will be produced. As such, only the data listed in this Affidavit and in the Search Warrant will be viewed by Your Affiant and/or his or her designee.

Nexus between the target offense(s) and the locations within the phone to be searched:

Your Affiant respectfully requests that this Search Warrant be approved so that your Affiant or Designee may search the above described data associated with the cellular phone identified above. A search of the data associated with the cellular phone is necessary because such data may be relevant to the offenses being investigated.

Based on training, experience, and general knowledge of human behavior in today’s society, Your Affiant knows that most individuals own and possess a cellular telephone and retain their phones on their person or in their immediate possession. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (“While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.”); *Riley v. California*, 134 S.Ct. 2473, 2484 (2014) (“modern cell phones [] are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”).

Your Affiant also knows from training and experience that criminals frequently communicate with each other and/or other individuals before, during, and after criminal events. Your Affiant also knows from his/her training and experience that this type of communication usually occurs via cellular phones. Analysis of the data contained in a cellphone or other mobile/electronic device could assist Your Affiant with determining the general location of the device before, during, or after the target offense. This information, along with other information that can be obtained through an electronic device such as a cellphone, will assist Your Affiant with furthering the above-described criminal investigation.

For example, evidence relating to the above described offense(s) and/or related events or information is likely to be contained in the categories detailed above. Communications made and preserved through call history, contact information, voice messages, text and MMS messages, emails, and social media applications with communication capability (i.e., Facebook Messenger, Snapchat, and other similar applications) may include evidence of the target offenses. Communications made by the person who possessed and used the phone through any of these methods may also include comments made to others that relate to the target offenses described above, or may include information that can lead to the discovery of other evidence.

In addition to information or data contained in the phone relating to communications, photos and/or videos stored in the phone may depict individuals involved in or with knowledge of the crimes, may show connections between individuals involved in the target offense(s), and/or may lead investigators to others who can provide further relevant evidence. Based on training and experience, individuals often take and distribute/post photos and videos that include information about their criminal actions and post details and communicate with others about criminal activity and other information relating to criminal activity. Photos and videos depicting involved persons wearing similar clothing to that described by witnesses or observed in recordings can also be found in cellphones.

Geographical location information can be obtained from various areas in the phone, such as connected with phone calls, text or MMS messages, email messages, photos, videos, and social media application. This data is important to establish the location of the phone (and therefore, the person in possession of the phone) before, during, and after the target crimes. Geographical location information may also be helpful to lead investigators to other persons who may have been present at the time the offenses described above occurred or may lead to the location of other evidence.

Data relating to the internet activity on the phone can provide multiple types of relevant evidence. Web searches can show efforts to identify locations, people, or other information relevant to the planning and/or commission of the offense. Such searches can also show efforts to keep track of the crime and investigation through the internet, which can establish consciousness of guilt and/or knowledge of these crimes. Internet data can show communications with others, through chat rooms, forums, or other websites, and such communications can establish the suspect’s involvement in or knowledge of the crimes, as well as provide information relevant to motive and intent. Internet data can also contain location information, and can demonstrate the use of services, programs, or applications that can themselves contain evidence of the criminal activity and/or the parties’ involvement therein.

In the event that relevant and/or incriminating evidence is located in the phone, it will be critical to establish the individual in possession of the phone at or about the time the communications are made, the photos and/or videos are captured, or social media applications are used. Evidence attributing particular data items located in the device can come in the form of other communications made at or near the time of the incriminating event that can be tied to the suspect(s), call logs and contact information connecting the device and/or particular communication events to the suspect, and other data that can be found on the phone that can establish the identity of the person in possession of the phone at the time the incriminating data was captured by the device. Data relating to possession, dominion and control over the cellphone will assist in associating any communications or data to the person who made such communications or accessed/created/distributed such data.

Child Pornography and the Sexual Abuse of Children

Child pornographers can produce images using a wireless device such as a cell phone. Photos can also be made using cameras, then can be transferred onto another device either using wire or wireless technology. Images can also be uploaded to Internet-based storage commonly referred to as the “cloud.” Hard-copy images can also be scanned into a computer. Via the Internet, connection can be made to literally millions of computers around the world. Child pornography can be transferred quickly and easily via electronic mail or virtually countless other online platforms, communication services, storage services, and applications.

A computer's capability to store images in digital form makes it an ideal repository for child pornography and other files related to the sexual abuse and exploitation of children. The digital-storage capacity in devices and in the “cloud” has grown tremendously within the last several years. Thumb drives with a capacity of 32 gigabytes are not uncommon. Flash cards with a capacity of 32 gigabytes are not uncommon. Hard drives with the capacity of 500 gigabytes up to 3 terabytes are not uncommon. Phones with over 100 gigabytes in storage are not uncommon. Devices can store thousands of images and videos at very high resolution. These devices are often internet capable and can not only store, but can transmit images via the internet and can use the devices to store images and documents in internet or “cloud” storage spaces. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

With Internet access, a computer user can transport an image file from the Internet or from another user’s computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one’s own computer is called “downloading”. The user can then display the image file on his computer screen, and can choose to “save” the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer). Sometimes the only method to recreate the evidence trail of this behavior is with careful laboratory examination of the computer, modem, printer, and other electronic devices.

The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that is 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.

The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes, cars, garages, sheds, and other secure storage locations, such as in a digital or electronic format in a safe, secure, and private environment, including in cloud-based storage online or on their person.

The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

The majority of individuals who collect child pornography often collect, read, copy or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

An individual who possesses images and/or videos depicting child pornography on one digital storage devices and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that s/he possesses. Additionally, based on this training and experience, I understand that an individual who discusses the sexual abuse and/or exploitation of children on one digital storage device is likely to conduct those communications on additional digital storage devices that s/he possesses.

Onsite Processing of Devices

Computers are machines that are programmed to automatically carry out operations allowing them to carry out a wide range of tasks. A complete computer including the hardware, operating system and required peripheral equipment are commonly referred to as “computer systems”. The term “personal computer” refers to a computer that is designed for use by an end user as opposed to a developer or programmer. Most computers are programmed to operate most efficiently therefor are constantly storing data from a user’s active session into memory to expedite processing of this data at a later time. This important data is at risk of being permanently deleted once the computer is powered off.

Due to recent advancements in computer encryption technology, as well as the increase in the size of Random Access Memory (RAM), which is volatile and will be lost when power is removed, I also know, through my training and experience, that it is often necessary to immediately do a limited examination of a system if it is powered on at the time of the search. This examination can include the use of a thumb drive which is inserted into the computer and then used to gain access to the RAM, as well as to check for the use of any encryption programs. If encryption is in-place, then it could be necessary to create an image of the active system while on-site since the removal of power will often leave the data in an encrypted state that will then be unreadable without a password. Additionally, the brief on-site examination of devices can assist in determining what, if any, devices contain contraband and need to be seized for a more thorough laboratory examination. In situations involving multiple people or family members living in the same home this on-site preview can prevent the unnecessary seizure of items that do not contain contraband material.

Computer Processing

Due to the nature and vulnerability of magnetic or digital data, it is necessary to seize media capable of storing magnetic data, and the computer, or what is commonly referred to as the CPU, meaning the computer case which contains the hard drive, motherboard and related hardware. It is necessary to remove these items from the scene and transport them to a controlled environment so a complete search of the items may be accomplished in such a way that the data it is protected, and unaltered.

Your affiant is aware that the current technology available for the downloading of data from digital devices such as cell phones, computers, or other mobile devices, does not allow the download of information only for a specific date range. Your affiant is also aware that the current technology available may not allow the downloading of only specific types of data, (e.g. pictures, messages, contacts, application data, etc.) as this data, including dates, may be in raw form, making it humanly unreadable without the use of specific software.  In light of that, the data from the digital device must be downloaded as completely as technologically possible. Once that download is completed, and the downloaded data is processed with specific software, a search of the data for a specific date range or specific type of data content is possible.

Your affiant is also aware that many times, there is only one opportunity to download the information from a digital device. Without obtaining all of the downloadable data from the cell phone, computer, or other mobile device, if additional information is learned later in the investigation, either by law enforcement, the District Attorney’s Office, or defense counsel, the same data that existed at the time of the initial download may no longer be available.  The only way to ensure preservation of all the downloadable data that existed at the time of the original download is to initially obtain all the downloadable data from the cell phone, computer, or other mobile device, and then preserve that data for any future searches.

Your affiant is requesting to obtain all of the downloadable data from the digital device(s). That data will be saved to preserve it in case additional review of the data is warranted and authorized by the courts at a later time. If a future search of the downloaded data from the device is necessary at a later time, additional applications will be made to the courts. At this time, the review of the data extracted from the device(s) will be for the date range and data authorized in the warrant.

***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 filing of charges based on this 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. Pursuant to CRS § 16-3-305(7)(a), Your Affiant requests that this Court authorizes the execution of this search warrant outside of the time requirements of between the hours of 7 A.M. and 7 P.M. Your Affiant requests authorization to execute this warrant between the hours of [AM TIME] and [PM TIME]. As good cause, [STATEMENT OF GOOD CAUSE].

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

**ATTACHMENT A**

1. **Internet Service Providers (“ISPs”):** ISPs 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, e-mail, 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 “e-mail address,” an e-mail 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.
2. **Internet Protocol Address (“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 dial-up 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.
3. **Digital Camera** is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable digital storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media includes various types of flash memory cards and miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos such as texts, word processing documents, or web pages. If the camera is equipped with global positioning system (“GPS”) technology, that information may be recorded as metadata associated with the photographs and videos taken with that camera as well as other information such as the make and model of the camera and the date and time the image was created. Some cameras and removable storage media are now equipped with wireless capabilities, which allow for images and files to be uploaded from the camera or digital storage media directly to the Internet or to other digital storage devices or computers using a wired or wireless connection.
4. **Wireless telephone** (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet including websites, social media sites, bulletin boards, file sharing, and other Internet sites. Wireless telephones often have a subscriber identity module or subscriber identification module (“SIM”), which is an integrated circuit that securely stores the International Mobile Subscriber Identity (“IMSI”) and the related key used to identify and authenticate subscribers on mobile telephone devices. A SIM is embedded into a removable “SIM card,” which can be transferred between different mobile devices. A SIM card contains a unique serial number (“ICCID”), IMSI, security authentication and ciphering information, temporary information related to the local network, a list of the services to which the user has access, and certain passwords. Most SIM cards will also store certain usage data, such as call history, text (“SMS”) messages, and phone book contacts. Wireless telephones may also be “smartphones,” such that they operate as personal computers capable of accessing the Internet. They may also include GPS technology for determining the location of the device. Such telephones may also contain removable storage media, such as a flash card—such devices can store any digital data, and can have the capacity to store many gigabytes of data. Some cellular telephones also have software, giving them the same capabilities as personal computers including accessing and editing word processing documents, spreadsheets, and presentations. Some cellular telephones also operate as a “tablet,” or mobile computer, and can contain software programs called applications. Those programs can perform different functions and save data associated with those functions, including use associated with the Internet.
5. **Personal digital assistant**, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.
6. **Tablet device** is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
7. A hard disk drive (“HDD”), also known as a hard drive or hard disk, is a data storage device that consists of an external circuit board, external data, power connections, and internal glass, ceramic, or magnetically charged rotating metal platters that permanently store data even when powered off.  A solid-state drive (“SSD”), also known as a solid-state disk, is a data storage device that uses integrated circuit assemblies as memory to permanently store data instead of using rotating platters. Flash drives, flash cards, and thumb drives are digital storage devices that can connect to computers or other devices using the appropriate connection. CDs/DVDs are digital storage devices capable of storing large amounts of digital data—a user can store information onto a CD/DVD by “burning” digital data to the device using a computer CD/DVD drive. These devices are capable of storing any electronic information including images, videos, word processing documents, programs and software, and web pages.
8. **Computer Routers and Modems** are also used as instrumentalities of crimes involving computers both to operate the computer to commit criminal offenses involving the sexual exploitation of minors. Modems and routers can contain information about dates, IP addresses, MAC addresses, frequency, and computer(s) used to access the Internet, and some have separate digital storage capacity that allow them to connect to other devices and to store information similar to an external digital storage device like a flash card or thumb drive. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device or the computers and devices connected to it.
9. “**Computers**” or “**digital storage media**” or “**digital storage devices**” may be used interchangeably, and can 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.

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**SEARCH WARRANT**

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 police officer, in support of the issuance of this search warrant, hereby commands you to search **PREMISES/VEHICLE** and curtilage thereof, described and identified as:

SPECIFICALLY DESCRIBE THE RESIDENCE

ADD PHOTO OF PHONE IF AVAILIABLE

AND seize:

ONLY INCLUDE THOSE ITEMS BELOW THAT ARE SUPPORTED IN THE PROBABLE CAUSE NARRRATIVE OF YOUR AFFIDAVIT

1. Documents and effects which tend to show possession, dominion and control over said premises, including but not limited to keys, mail envelopes, letters, rental/owner agreements and receipts, utility and telephone bills, photographs and film, prescription bottles, vehicle registration, insurance papers, address and telephone books, government notices and documents, papers bearing a person’s name, phone number or address;
2. Still and video photographs, and crime scene drawings.
3. Any electronic devices that are capable of analyzing, creating, displaying, converting, or transmitting electronic or magnetic computer impulses or data. These devices include, but are not limited to: desktop computers, laptop computers, personal data assistants, tablet devices, gaming consoles, personal digital assistant, or other stationary or portable devices capable of storing electronic data, such as USB storage devices, and memory cards.
4. Magnetic and optical storage devices capable of storing digital media include but not limited to discs, compact discs, DVDs, video cassettes, camera film and video film;
5. All telecommunications devices capable of sending and receiving telephone calls, SMS (text message) communications, or electronic communications, which include: wireless telephones, cellular phones, smart phones, iPhones, iPads, electronic tablets, etc.
6. Computer input and output devices.
7. Any written or printed material that provides instructions or examples concerning the operation of a computer system, computer software, and/or any related device. Any password, email address, account information, internet service provider (ISP) information, in the form of paper, documents or any other readable material, whether generated by handwriting, typewriter, computer, or any other device;
8. Photography equipment including but not limited to cameras, video cameras, and/or digital cameras, and storage media associated with such equipment including but not limited to undeveloped and/or unexposed film slides, negatives, videotapes, and/or magnetic/optical media used for storage of digital images.
9. Case specific items like cell phones, weapons, drugs, cash, bodily fluids or DNA, documents.
10. Other case specific items like cell phones, printers, scanners, email or electronic communication, documents, case related pictures, Internet data such as history, web sites visited, downloaded information.
11. Print media, photographs and printouts of child exploitative material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j).
12. Conduct a preview search of all located digital communications devices and digital storage media for sexual exploitation material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j), by use of manual or automated preview tools.
13. If computers or other digital devices are found, the investigator may acquire the contents of volatile memory related to computers and other digital communication devices that would tend to show the current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details necessary to preserve the true state of evidence.

The search warrant authorizes law enforcement to access, review and examine the devices seized pursuant to this warrant for data relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of CRIMINAL OFFENSE(S) perpetrated against NAME OF VICTIM OR LOCATION [IF APPLICABLE] (hereinafter “Subject Offense(s)”):

REVIEW THE LISTED CATEGORIES OF DATA, PLEASE REMOVE ANY CATAGORIES NOT SUPPORTED BY THE FACTS CONTAINED IN YOUR AFFIDAVIT

1. Data which tends to show possession, dominion and control over said equipment, including device and system ownership information (telephone number, ESN number, serial number, IMEI, IMSI, CCID);
2. Evidence of software that may allow others to control a device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
5. Passwords, encryption keys, codes, and/or other devices or information that may be necessary to access the device and its contents;
6. Date/time, language, and other settings preferences to include wireless local area network setting(s), Bluetooth settings to include device name(s), hotspot SSID (name), and MAC address and connection dates and times to the device;
7. Address books, contact lists, names, and lists of names and addresses of individuals who may have been contacted by use of the device or by other means for the purpose of committing violations of the Subject Offense(s);
8. Records, documents, invoices and materials that concern any accounts with an Internet Service Provider pertaining to Subject Offense(s);
9. Records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to Subject Offense(s);
10. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses pertaining to Offense(s) or that show who used, owned, possessed, or controlled the device;
11. Voicemail messages, text messages, MMS messages, Emails whether stored, received, or deleted as they pertain to pertaining to Offense(s), including username(s) and account information;
12. Photographs or images stored, sent, received or deleted, or documents containing photographs or images pertaining to Subject Offense(s);
13. Videos stored, sent, received or deleted pertaining to Subject Offense(s);
14. Notes, documents, records, or correspondence, pertaining to Subject Offense(s);
15. Electronic files, data, videos, and communications, including related metadata and location data, stored, sent, received or deleted from social media applications such as Facebook, Snapchat, Instagram, Twitter and/or any other third party programs or applications located on the device pertaining to Offense(s);
16. Global position system (GPS) data and any other geolocation data pertaining to Subject Offense(s);
17. Records of internet activity, including internet protocol (IP) addresses and Port IDs, firewall logs, transactions with internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses that show who used, owned, possessed, or controlled the device(s) pertaining to Offense(s);
18. Any Child Exploitative Material as defined by Colorado Revised Statutes (C.R.S.) 18-6-403(2)(j).

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST.

For which a search warrant may be issued upon one or more of the grounds set forth in the Colorado Rules of Criminal Procedure and CRS § 16-3-301, 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.

Based upon the affidavit of the above-named affiant, which is incorporated by reference, I am satisfied that there is probable cause to believe that the property described is located at the place above described, and probable cause to seize the items described above pursuant to Crim. P. 41, and §16-3-301. YOU ARE THEREFORE AUTHORIZED to search the place described for the property described, and to make a return of this Warrant to the undersigned judge within fourteen days, and to deliver to the person from whom the property is taken, a copy of this Warrant together with a receipt for the property taken, or, to leave a copy of the Warrant and receipt at the place from which the property was taken.

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

* If not already in possession of the device, seize the aforementioned device within 14 days of the date this warrant is signed;
* Access the aforementioned device and view, copy and maintain the above described data contained therein;
* Use and employ such force as may reasonably be necessary in the performance of the duties described herein;
* The ability to use whatever means necessary to override any encryption or secure files encountered during the forensic examination of the phone. 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 repair the device, replace the screen, replace the chassis, reconnect wires, or replace a battery. I also understand that it may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions.
* Physically access the internal workings of the device to extract any and all potential data stored on the device.
* Employ all means necessary to prevent damage to the device. Any intentional damage or destruction will require additional judicial approval.
* 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.
* Deliver to the person from whom the property is taken a copy of this warrant together with a receipt for the property taken, or to leave a copy of the warrant and receipt at the place from which the property was taken;
* Make prompt return of this search warrant, accompanied by a written inventory describing the physical storage media that was seized or copied, to the undersigned judge.

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. Pursuant to CRS § 16-3-305(7)(a), this warrant must be executed between the times of 7 A.M. and 7 P.M. --- OR --- Pursuant to CRS § 16-3-305(7)(a), the Court finds good cause and authorizes the execution of this warrant between the hours of [AM TIME] and [PM TIME].

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