IN THE CIRCUIT COURT OF THE EIGHTH JUDICIAL CIRCUIT

IN AND FOR ALACHUA COUNTY COUNTY, FLORIDA

STATE OF FLORIDA, AGENCY CR #: 00-00-000000

Plaintiff,

-vs-     

SUSPECT(S), **APPLICATION & AFFIDAVIT**

Defendant. **FOR SEARCH WARRANT**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

**APPLICATION FOR SEARCH WARRANT**

**BEFORE ME**, the undersigned Judge, State of Florida, came this sworn application and affidavit by YOUR RANK YOUR NAME, a law enforcement officer employed by the YOUR AGENCY, who was first duly sworn, deposes and says that HE/SHE (YOU) believes and has good reason to believe the laws of the State of Florida have been violated and are now being violated, and that the articles, property, electronic communications, and data described below are lawfully subject to seizure, and are now located at the location(s) set forth below:

**LOCATION OR PROPERTY TO BE SEARCHED AND/OR SEIZED**

North Florida Internet Crimes Against Children (ICAC) Task Force National Center for Missing and Exploited Children (NCMEC) CyberTipline Reports XXXXXXXXX which are in the virtual possession of investigators at the AGENCY.

All files contained in the CyberTipline Reports were forwarded to the AGENCY for investigation. AGENCY is an affiliate agency of the North Florida Internet Crimes Against Children (ICAC) Task Force. CyberTipline Reports and associated files are reported by Internet Service Providers (ISP) and Electronic Service Providers (ESP) to the National Center for Missing and Exploited Children (NCMEC). NCMEC then distributes the CyberTipline Reports to the appropriate regional task force. The Gainesville Police Department manages our region and disseminates the CyberTipline Reports to the various jurisdictions based on the approximate geographical location of the suspect.

The files are contained within each of the following CyberTipline Reports were reported by the ISP or ESP companies to NCMEC, sent to GPD and then forwarded by GPD to AGENCY (if not GPD) and are as follows:

|  |  |  |
| --- | --- | --- |
| **CyberTip Creation Date and Time** | **CyberTip Number** | **ESP / ISP** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

ALL OF WHICH are being kept and/or used and/or obtained in and/or is evidence of a felony violation of the laws of the State of Florida, to-wit:

Florida Statute 827.071- Sexual performance by a child; child pornography

THE BASIS for Your Affiant's belief is:

Your Affiant, YOUR RANK YOUR NAME (hereinafter referred to as YA), is a duly sworn law enforcement officer employed by the AGENCY and has been since HIRE DATE. YA successfully completed Basic Law Enforcement Training at ACADEMY YOU ATTENDED in CITY WHERE YOU ATTENDED, COUNTY WHERE YOU ATTENDED County, Florida. YA served as SUMMARIZE YOUR LEO WORK EXPERIENCE. YA has attended SUMMARIZE SPECIAL TRAINING & LEO CLASSES INCLUDING APPROXIMATE DATES OF COMPLETION. By HIS/HER training and experience, SUMMARIZE SPECIAL QUALIFICIATIONS BASED ON ABOVE TRAINING – IE, FAMILIARITY WITH CONTROLLED SUBSTANCES, KNOWLEDGE OF CHILD PORNGRAPHY, ETC. YA is currently assigned to CURRENT ASSIGNMENT, and has been assigned to investigate various criminal offenses to include, but not limited to, YOUR CASE LOAD since MONTH, YEAR YOUR CURRENT ASSIGNMENT BEGAN.

SUMMARIZE YOUR CASE HERE – YOUR NARRATIVE MUST SPECIFY HOW EACH OF THE OPTIONS SELECTED ABOVE IS RELEVANT TO YOUR FACTS.

**DEFINITIONS**

The following definitions apply to this affidavit:

* 1. “Chat,” as used herein, refers to any kind of text communication over the internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as internet forums and email.
  2. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in children but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.
  3. “Child pornography” means any material or items depicting a minor engaged in sexual conduct.
  4. For the purposes of this affidavit, a “minor” or “child” refers to any person less than eighteen years of age and for the purpose of this search warrant, “depictions of minors engaged in sexually explicit conduct” is defined in F.S.827.071, defined as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex or between humans and animals; penetration of the vagina or rectum by any object; masturbation; sadomasochistic abuse; defecation or urination for the purpose of sexual stimulation of the viewer; depiction of the genitals or unclothed pubic or rectal areas of any minor, or the unclothed breast of a female minor, for the purpose of sexual stimulation of the viewer and touching of a person's clothed or unclothed genitals, pubic area, buttocks, or breast area for the purpose of sexual stimulation of the viewer.
  5. “Cloud-based storage service,” as used herein, refers to a publicly accessible, online storage provider that collectors of depictions of minors engaged in sexually explicit conduct can use to store and trade depictions of minors engaged in sexually explicit conduct in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders or collectors of depictions of minors engaged in sexually explicit conduct in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.
  6. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device,” including smartphones and mobile devices.
  7. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
  8. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
  9. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse that process in order to restore it.
  10. “Data,” as used herein refers to the quantities, characters, or symbols on which operations are performed by a computer, being stored, and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.
  11. “Digital Devices” as used herein refers to any physical object that has a computer, microcomputer, or hardware that is capable of receiving, storing, possessing, or potentially sending data.
  12. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
  13. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations, community-owned, non-profit, or otherwise privately-owned companies 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.
  14. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.
  15. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
  16. “Remote Computing Service” (“RCS”), is the provision to the public of computer storage or processing services by means of an electronic communications system.
  17. “User Attributes,” as used herein refers to any tangible data, documents, settings, programs, or other information that provides information related to the identity of the specific user of the device, computer, application, program, or record.

**BACKGROUND**

Based on my training, experience, and collaboration with ICAC detectives, industry experts, academia and other law enforcement personnel, I know the following:

That adult persons with a sexual interest in minors are persons whose sexual targets are children. They receive sexual gratification and satisfaction from actual physical contact with children, fantasy involving the use of writings detailing physical contact with children, and/or from fantasy involving the use of pictures and/or videos of minors.

The development of the computer has changed the way child erotica and depictions of children engaged in sexually explicit conduct are distributed and children are victimized. The computer serves four functions in connection with depictions of children engaged in sexually explicit conduct. These four functions include: production, communications, distribution, and storage.

Pornographers produce both still and moving images, i.e.: photographs and video. These images can be transferred either directly from the camera into a computer, directly from a storage device such as a computer disk or flash drive to a computer, or the image can be transferred directly into the computer by use of a scanner.

E-mail consists of messages from one person to another that are electronically transmitted through a user's electronic device. As opposed to letters sent via the postal service, e-mail sends the messages instantaneously via the internet anywhere in the world. Due to that fact and the relatively low cost, emails have become a very popular form of communication. In fact, there are now more e-mail addresses than telephone numbers in the world. In addition to written messages which are generally sent in emails, pictures, graphs, and other text files can be attached to an email message and sent as well.

All that a computer user needs to do in order to use email is open up an email account with one of the myriads of companies that provide email service (e.g. America On-Line, Microsoft, Comcast, Yahoo etc.). Once the account is set up, the user can choose the "name" of his email address, which does not have to match (or even relate to) identifying information of the user. Thus, the email address name by itself does nothing to identify the owner of the email address or the composer of the email message. Nevertheless, often times the email messages themselves, contain information that either directly or indirectly identifies the composer of the email message. Based on my training and experience investigating depictions of minors engaged in sexually explicit conduct offenses, I know it is common for collectors of depictions of minors engaged in sexually explicit conduct to use multiple email accounts in order conceal their true identity and/or more easily categorize their collection according to the type of material or source.

Individuals involved in computer-related crimes often use e-mail accounts to conduct both criminal and non-criminal communications. Consequently, these emails can be a great source of information to help identify the sender and/or recipient of the message. The ability to view these e-mails by investigating law enforcement often provides further investigative leads to assist in identifying the person of interest.

I know that an Internet Protocol (IP) address is a numerical label assigned to devices communicating on the internet and that the Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally. An IP address provides the methodology for communication between devices on the internet. It is a number that uniquely identifies a device on a computer network and, using transport protocols, moves information on the internet. Every device directly connected to the internet must have a unique IP address.

An IP address is typically comprised of four (4) series of numbers separated by periods and is most commonly represented as a 32-bit number such as 71.227.252.216 (Internet Protocol Version 4) however, a newer version, IPv6, is currently being deployed as well and is represented as a 128-bit number such as 2001:db8:0:1234:0:567:8:1.

IP addresses are owned by the Internet Service Provider and leased to a subscriber/customer for a period of time. They are public and visible to others as you surf the internet. The lessee has no expectation of privacy due to the public nature of IP addresses.

When an Internet Service Provider’s customer logs onto the internet using a computer or another web-enabled device, they are assigned an Internet Protocol (IP) address.

There are two different types of Internet Protocol addresses. The first is a dynamic IP address, which means the user’s IP address may change each time they log on to the internet. The frequency in which this address changes is generally controlled by the Internet Service Provider and not the user. The other type of IP address is a static IP address, which means that a user is assigned a specific IP address that remains constant every time they log on to the internet.

IP addresses are similar to a license plate on a motor vehicle. They are the property of the issuer, and not the vehicle owner. Just as your license plate is visible as you cruise your city or town, your IP address is visible as you cruise the internet. Your IP address is visible to the administrators of websites you visit, attached emails you send, and broadcast during most internet file and information exchanges that occur on the internet.

I know based on my training and experience, that Electronic Service Providers (“ESP”) and/or Internet Service Providers (“ISP,” collectively ISP) typically monitor their services utilized by subscribers. To prevent their communication networks from serving as conduits for illicit activity and pursuant to the terms of user agreements, ISPs routinely and systematically attempt to identify suspected depictions of minors engaged in sexually explicit conduct that may be sent through its facilities. Commonly, customer complaints alert them that an image or video file being transmitted through their facilities likely contains suspected depictions of minors engaged in sexually explicit conduct.

When an ISP receives such a complaint or other notice of suspected depictions of minors engaged in sexually explicit conduct, they may employ a “graphic review analyst” or an equivalent employee to open and look at the image or video file to form an opinion as to whether what is depicted likely meets the federal criminal definition of depictions of minors engaged in sexually explicit conduct found in 18 USC § 2256, which is defined as any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. If the employee concludes that the file contains what appears to be depictions of minors engaged in sexually explicit conduct, a hash value of the file can be generated by operation of a mathematical algorithm. A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, results in a different hash value. Consequently, an unknown image can be determined to be identical to an original file if it has the same hash value as the original. The hash value is, in essence, the unique fingerprint of that file, and when a match of the “fingerprint” occurs, the file also matches.

ESPs typically maintain a database of hash values of files that they have determined to meet the federal definition of depictions of minors engaged in sexually explicit conduct found in 18 USC § 2256. The ISPs typically do not maintain the actual suspect files themselves; once a file is determined to contain suspected depictions of minors engaged in sexually explicit conduct, the file is deleted from their system.

The ESPs can then use Image Detection and Filtering Process (“IDFP”), Photo DNA (pDNA), or a similar technology which compares the hash values of files embedded in or attached to transmitted files against their database containing what is essentially a catalog of hash values of files that have previously been identified as containing suspected depictions of minors engaged in sexually explicit conduct.

When the ESP detects a file passing through its network that has the same hash value as an image or video file of suspected depictions of minors engaged in sexually explicit conduct contained in the database through a variety of methods, the ISP reports that fact to National Center for Missing and Exploited Children (NCMEC) via the latter’s CyberTipline. By statute, an ESP or ISP has a duty to report to NCMEC any apparent depictions of minors engaged in sexually explicit conduct it discovers “as soon as reasonably possible.” 18 U.S.C. § 2258A(a)(1). The CyberTip line report transmits the intercepted file to NCMEC. Often that occurs without an ISP employee opening or viewing the file because the files hash value, or “fingerprint,” has already been associated to a file of suspected depictions of minors engaged in sexually explicit conduct. The ISP’s decision to report a file to NCMEC is made solely on the basis of the match of the unique hash value of the suspected depictions of minors engaged in sexually explicit conduct to the identical hash value in the suspect transmission.

ESP’s also monitor which devices are used to access their platform by recording the advertising identification number. This number is a unique identifier assigned to hardware devices used by ESP’s to track users semi-anonymously and provide targeted advertisements. Because it is a unique identifier, this information can link specific devices owned by specific individuals with the criminal activity on a particular platform’s account.

Most Internet Service Providers keep subscriber records relating to the IP address they assign, and that information is available to investigators. Typically, an investigator has to submit legal process (e.g. subpoena or search warrant) requesting the subscriber information relating to a particular IP address at a specific date and time.

A variety of publicly available websites provide a public query/response [protocol](http://en.wikipedia.org/wiki/Protocol_(computing)) that is widely used for querying [databases](http://en.wikipedia.org/wiki/Database) in order to determine the registrant or assignee of [internet](http://en.wikipedia.org/wiki/Internet) resources, such as a [domain name](http://en.wikipedia.org/wiki/Domain_name) or an [IP address](http://en.wikipedia.org/wiki/IP_address) block. These include WHOIS, MaxMind, arin.net, and other common search tools.

The act of ‘downloading’ is commonly described in [computer networks](http://en.wikipedia.org/wiki/Computer_network) as a means to receive data to a local system from a remote system, or to initiate such a data transfer. Examples of a remote system from which a download might be performed include a [webserver](http://en.wikipedia.org/wiki/Webserver), [FTP server](http://en.wikipedia.org/wiki/File_Transfer_Protocol), [email](http://en.wikipedia.org/wiki/Email) server, or other similar systems. A download can mean either any file that is offered for downloading or that has been downloaded, or the process of receiving such a file. The inverse operation, ‘uploading’, can refer to the sending of data from a local system to a remote system such as a server or another client with the intent that the remote system should store a copy of the data being transferred, or the initiation of such a process.

The National Center for Missing and Exploited Children (NCMEC) is a private, [non-profit organization](http://en.wikipedia.org/wiki/Non-profit_organization) established in 1984 by the [United States Congress](http://en.wikipedia.org/wiki/United_States_Congress). Primarily funded by the [Justice Department](http://en.wikipedia.org/wiki/United_States_Department_of_Justice), the NCMEC acts as an information [clearinghouse](http://en.wikipedia.org/wiki/Clearinghouse) and resource for parents, children, law enforcement agencies, schools, and communities to assist in locating missing children and to raise public awareness about ways to prevent [child abduction](http://en.wikipedia.org/wiki/Child_abduction), [child sexual abuse](http://en.wikipedia.org/wiki/Child_sexual_abuse) and [depictions of minors engaged in sexually explicit conduct](http://en.wikipedia.org/wiki/Child_pornography).

The Center provides information to help locate children reported missing (by parental abduction, [child abduction](http://en.wikipedia.org/wiki/Child_abduction), or running away from home) and to assist physically and sexually abused children. In this resource capacity, the NCMEC distributes photographs of missing children and accepts tips and information from the public. It also coordinates these activities with numerous state and federal law enforcement agencies.

The CyberTipline offers a means of reporting incidents of child sexual exploitation including the possession, manufacture, and/or distribution of depictions of minors engaged in sexually explicit conduct; online enticement; child prostitution; child sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images.

Any incidents reported to the CyberTipline online or by telephone go through this three-step process: CyberTipline operators review and prioritize each lead; NCMEC’s Exploited Children Division analyzes tips and conducts additional research; The information is accessible to the FBI, ICE, and the USPIS via a secure Web connection. Information is also forwarded to the ICACs and pertinent international, state, and local authorities and, when appropriate, to the ESP.

Internet Crimes Against Children (ICAC) is a task-force started by the [United States Department of Justice](http://en.wikipedia.org/wiki/United_States_Department_of_Justice)’s Office of Juvenile Justice and Delinquency Prevention (OJJDP) in 1998. Its primary goals are to provide state and local law enforcement agencies the tools to prevent [internet crimes](http://en.wikipedia.org/wiki/Internet_crime) against children by encouraging multi-jurisdictional cooperation as well as educating both law enforcement agents and parents and teachers. The aims of ICAC task forces are to catch distributors of [depictions of minors engaged in sexually explicit conduct](http://en.wikipedia.org/wiki/Child_pornography) on the internet, whether delivered on-line or solicited on-line and distributed through other channels and to catch sexual predators who solicit victims on the internet through chat rooms, forums and other methods. Currently all fifty states participate in ICAC.

Based upon my knowledge, experience, and training in depictions of minors engaged in sexually explicit conduct investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in depictions of minors engaged in sexually explicit conduct:

1. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
2. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media.  Such individuals often times use these materials for their own sexual arousal and gratification.  Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.  These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.
3. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct often possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location.  These individuals typically retain these “hard copies” of child pornographic material for many years.
4. Likewise, those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area.  These collections are often maintained for several years and are kept close by, usually at the individual’s residence, to enable the collector to view the collection, which is valued highly.
5. Those who possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other depictions of minors engaged in sexually explicit conduct distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in depictions of minors engaged in sexually explicit conduct.
6. Those that possess, receive, and attempt to receive depictions of minors engaged in sexually explicit conduct prefer not to be without their depictions of minors engaged in sexually explicit conduct for any prolonged time period.  This behavior has been documented by law enforcement officers involved in the investigation of depictions of minors engaged in sexually explicit conduct throughout the world.
7. Based on my training and experience, collectors, and distributors of depictions of minors engaged in sexually explicit conduct also use online, remote, resources to retrieve and store depictions of minors engaged in sexually explicit conduct, including services offered by many companies for cloud-storage and digital communications. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of electronic files in any variety of formats. A user can set up, and access, an online storage account from any computer or digital device with access to the internet. Evidence of such online storage of depictions of minors engaged in sexually explicit conduct is often found on the user's computer or smart phone. Even in cases where online storage is used, however, evidence of depictions of minors engaged in sexually explicit conduct can be found on a user’s digital device if that device is used to access the internet. Cloud storage allows the offender ready access to the material from any device that has an internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender’s device. Evidence located in cloud storage may be deleted from any device capable of reaching the website of the cloud hosting company. Once the individual user credentials, often a username and password are entered, the data in the cloud storage may be accessed, modified, shared, or deleted. Unlike deleting data from a local hard drive, once data is deleted from cloud storage, it is wiped from the cloud hosting company’s servers and is unrecoverable.
8. In addition to the traditional collector, law enforcement has encountered offenders who obtain depictions of minors engaged in sexually explicit conduct from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a ‘seek and delete’ offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification.
9. Additionally, offenders may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender’s device.
10. Based on my training and experience and my consultation with computer forensic detectives and agents who are familiar with searches of computers and smartphones, I have learned that offenders will try and obfuscate data containing images and videos of minors engaged in sexual activity. One potential manner of trying to hide the contraband may be by changing file extensions. For example, an image file may often have a file extension of “.jpg” of “.jpeg” signifying that it is an image or photograph. An offender may change that file extension by selecting the “save as” format on a computer or digital device and select “.doc” or “.docx” to make it appear that instead of a contraband image or photograph, it is a word document. The same process may be used to attempt to hide a video file as well. Based on these, and other attempts to hide potential contraband is necessary for forensic examiners to examine all potential data on a digital device.
11. I know that, regardless of whether a person discards or collects depictions of minors engaged in sexually explicit conduct he accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related devices, including storage media, used by the person.  This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of depictions of minors engaged in sexually explicit conduct, backup files, and other electronic artifacts that may be forensically recoverable.

**GOOGLE**

Google is an online search engine, content platform, service provider, and information amalgamator. Since their debut Google currently maintains a variety of online content products and services and they are ranked as one of the most frequently visited web sites in the United States. The following information was gleaned from Google’s website, privacy policy and other on-line resources. Google offers a large number of products including Gmail, Chrome Web Browser, Waze, YouTube, Chromecast, Google Home, Android, Google Auto, Google Maps, Gmail, the Google+ social media site, photo hosting platforms and many others. In addition to information Google obtains from a user using their services, Google collects data on a user from other companies doing business on the internet. They amalgamate the data in order to sell advertising aimed at the specific user.

Google identifies accounts in a variety of ways, primarily by Gmail account, but also telephone number, or IMEI number of an Android device. Basic data that Google stores about users include:

* Name, gender, and date of birth
* Email addresses
* Phone numbers
* Websites visited
* Searches made on Google Search
* Ad preferences
* YouTube search history and recently watched videos

Location data is also collected and stored by Google. They use advanced location recognition technology in order to routinely calculate your location. Android phones, which run off of Google’s services, and Pixel, Google’s own phone, track and record a user’s location through several means, including Wi-Fi, GPS, and cellular networks. Other more specific types of information collected and stored by Google include the following:

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

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

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

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

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

6. Documents – All user created documents stored by Google;

7. Finance - Records of securities, funds, and portfolios associated with the target Google account and/or target device;

8. Gmail - All email messages, including inbox messages, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages include information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the ‘cc’ (carbon copy) or the ‘bcc’ (blind carbon copy), the message content or body, and attached files;

9. Google Photos - Images, graphic files, video files, and other media files stored in the Google Photos service;

10. Location History - Location data including that derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data typically includes the GPS coordinates and the dates and times of all location recordings;

11. Play Store - Applications downloaded, installed, and/or purchased by the associated account and/or device;

12. Search History - All search history and queries;

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

14. Google Home – Information related to Google Home including, but not limited to, device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times.

15. Google Assistant – Information related to Google Assistant including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times.

16. Android Auto – Information related to Android Auto including, but not limited to, device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs and text messages, voice actions, and location data.

17. Android Drive – Data stored in the Google Drive for the listed account.

AGENCY is a member of the North Florida Internet Crimes against Children (ICAC) Task Force. The ICAC Task Force provides AGENCY with an opportunity to continue its history of proactive intervention and to target sex offenders. The ICAC program is a national network of 61 task forces representing more than three thousand federal, state, and local law enforcement agencies.

Between the dates of XXXXXXX and XXXXXXX, AGENCY received the following CyberTipline Reports which were generated by the specified ESP/ISP companies:

|  |  |  |
| --- | --- | --- |
| **CyberTip Creation Date and Time** | **CyberTip Number** | **ESP / ISP** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Through issuance of this warrant, YA is requesting advanced permission from the court, to open and view the reported files that have been reported as CSAM (Child Sexual Abuse Material) to confirm the presence of child pornography, or the presence of minors engaged in sexually explicit activities. Based on the representations of NCMEC in conjunction with the underlying companies, and the HASH matches documented, supported by the explanations provided above, YA believes the reported files will contain evidence of a violation of Florida Statute 827.071. Given a recent United States Court of Appeals Ninth Circuit ruling, which is in opposition to other cases decided on the matter, in an abundance of caution, YA is now requesting a search warrant to view the files and conduct further investigation in order to determine if a crime has been committed. See United States v. Luke Wilson, United States Court of Appeal, 9th Circuit, September 21, 2021. “The reliability of Google's proprietary technology, in our estimation, is pertinent to whether probable cause could be shown to obtain a warrant, not to whether the private search doctrine precludes the need for the warrant. And, as the district court noted, and we have noted as well, the warrant application here contained inadequate information about Google's proprietary technology to establish probable cause without reliance on the descriptions of the actual images.” In said case the court suppressed the images supporting the prosecution of the Defendant based upon law enforcement’s review of them, without warrant, after they were transferred from an ESP/ISP to NCMEC and then forwarded to law enforcement.

But see *U.S. v. Montijo*, United States District Court, M.D. Florida, 2022 WL 93535. In *Montijo*, the Middle District of Florida reached the opposite conclusion on a significantly similar series of facts. In addition to the similarity of the facts the Court determined that specific reliance on descriptors of the images was not needed, given the standardized identification of child pornography within the industry, coupled with the Defendant’s lack of a reasonable expectation of privacy once the items had been uploaded or distributed. “In reaching this decision, the Court is mindful of the legal split on this issue. It also recognizes that the Ninth Circuit in *Wilson* recently decided a factually similar case and reached the opposite conclusion. But the Eleventh Circuit has not yet weighed in whether the Fourth Amendment prohibits an officer from opening and reviewing the files after a private party has determined that the files’ hash values matched known child pornography images in its database. So, the Court has anchored its analysis to the original precedents announced in *Walter* and *Jacobsen* and applied those principles to deny Defendant's motion.” *United States v. Montijo*, No. 2:21-CR-75-SPC-NPM, 2022 WL 93535, at \*6 (M.D. Fla. Jan. 10, 2022).

See also *U.S. v. Brillhart*, United States District Court, M.D. Florida, 2023 WL 3304278. Similarly situated to *Montijo* and *Wilson*, the Defendant in *Brillhart* argued that investigators exceeded the private search exception by reviewing material provided within the NCMEC Cybertip without a warrant, however, the Court in *Brillhart* reached the same conclusion as that in *Montijo* and denied suppression of the evidence seized. “Here, it is undisputed that Yahoo and Google are private entities that acted independently of law enforcement and without the government's knowledge or participation in discovering the child pornography files. Still, Defendant makes much ado about not knowing the identities of the individuals at Yahoo and Google who viewed the files. Without names, Defendant asserts Yahoo's and Google's custodians only offer hearsay evidence about the human review, which violates his right to confront those individuals. But this argument misses the mark for two basic reasons. First, Yahoo and Google, along with their employees and contractors are private people. So, the who and how those private companies search their programs does not lessen the private search doctrine's application here. See *United States v. Montijo*, No. 2:21-cr-75-SPC-NPM, 2022 WL 93535, at \*5 (M.D. Fla. Jan. 10, 2022); see also *United States v. Bonds*, No. 521CR00043KDBDCK, 2021 WL 4782270, at \*4 (W.D.N.C. Oct. 13, 2021) (rejecting the defendant's argument that the anonymous Google employee was unreliable because law enforcement could not contemporaneously verify the information before conducting its search).” *United States v. Brillhart*, No. 2:22-CR-53-SPC-NPM, 2023 WL 3304278, at \*5 (M.D. Fla. May 7, 2023).

I am requesting permission from the court to open and view the reported files that have been reported as CSAM to determine if there is evidence of a crime. Based on the HASH match and the explanation above, I believe the reported files will contain evidence of a violation of Florida Statute 827.071, but due to a recent United States Court of Appeals, Ninth Circuit ruling, in an abundance of caution, I am now requesting a search warrant to view the files and conduct further investigation in order to determine if a crime has been committed (United States v. Luke Wilson, United States Court of Appeal, 9th Circuit, September 21, 2021).

I am also requesting an extension well beyond the 10-day rule with respect to search warrants. Each CyberTip Report will typically require an additional search warrant and work and it is not usually possible to complete all the CyberTips listed within the 10-day time frame. I believe this is a reasonable request because the content is already reported and waiting to be viewed.

Due to the nature of the CyberTip reports, it is rare that the subject of the investigation is identifiable with only the limited information contained in the CyberTip. I am requesting that I be authorized to notify only the California Department of Justice to fulfill the requirements of PC1546(c) and Cal ECPA. Outside the scope of this warrant, a new warrant would be sought for any additional information and the appropriate PC1546(b) or PC1546(c) rules would be followed, per Cal ECPA.

Lastly, I am requesting that any material that is unrelated to the objective of this warrant be sealed and not subject to further review, use, or disclosure without further order from this court.

**BASED ON THE FOREGOING**, YA has reason to believe and does believe that the structure in question has contained in the past, and does contain now, certain instrumentalities and contraband, including one or more cellular telephones, which constitutes a violation of the laws of the State of Florida, or certain evidence which constitutes proof of a violation of the laws of the State of Florida, and based upon the foregoing, requests issuance of a search warrant for the above-described premises to allow seizure of the above-described items.

**ALL OF WHICH WHEREFORE**, YA prays that a search warrant be issued according to law commanding the Sheriff and/or duly constituted Deputy Sheriffs of COUNTY County, Florida, and/or Detectives and/or Law enforcement officers of the LIST ALL LOCAL LAW ENFORCEMENT AGENCIES THAT COULD POTENTIALLY HELP SERVE WARRANT, and/or Special Agents of the Florida Department of Law Enforcement, and/or Special Agents of the United States Drug Enforcement Administration, and/or Special Agents of the United States Bureau of Alcohol, Tobacco, Firearms, and Explosives, and/or any of their duly constituted Agents, with proper and necessary assistance, to search the above-described premises for the above-described items, and for the seizure and safekeeping thereof, and for **authorization to search all of the said items** **seized,** either in the daytime or in the nighttime, or on Sunday, as the exigencies of the occasion may demand, in order that the evidence may be procured to be used in the prosecution of such person or persons unlawfully possessing or using the same in violation of the laws of the State of Florida.

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

                                                          YOUR RANK YOUR NAME, Affiant

SWORN TO AND SUBSCRIBED before me this \_\_ day of MONTH, 20\_\_.

    SWORN TO AND

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

                                                                          Notary or Assistant State Attorney

The above Application for Search Warrant coming on to be heard and having examined the application made under oath and the above sworn affidavit set forth and other facts and thereupon being satisfied that there is probable cause to believe that the grounds set forth in said Application and the facts do exist and that the law is being violated, I so find, and a search warrant is hereby allowed and issued.

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

                                                                         JUDGE

 S.A. review: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ATTORNEY NAME

Assistant State Attorney

IN THE CIRCUIT COURT OF THE EIGHTH JUDICIAL CIRCUIT

IN AND FOR COUNTY COUNTY, FLORIDA

STATE OF FLORIDA, AGENCY CR #: 00-00-000000

Plaintiff,

-vs- SEARCH WARRANT

SUSPECT(S),

Defendant.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

IN THE NAME AND BY THE AUTHORITY OF THE STATE OF FLORIDA,

TO: ALL AND SINGULAR THE SHERIFF AND/OR DULY CONSTITUTED DEPUTY SHERIFFS OF COUNTY COUNTY, FLORIDA, AND/OR DETECTIVES AND/OR LAW ENFORCEMENT OFFICERS OF LIST ALL LOCAL LE AGENCIES THAT MAY ASSIST WITH SERVICE, THE FLORIDA DEPARTMENT OF LAW ENFORCEMENT, AND/OR SPECIAL AGENTS OF THE UNITED STATES DRUG ENFORCEMENT ADMINISTRATION, AND/OR SPECIAL AGENTS OF THE UNITED STATES BUREAU OF ALCOHOL, TOBACCO, FIREARMS, AND EXPLOSIVES, AND/OR ANY OF THEIR DULY CONSTITUTED AGENTS,

WHEREAS, complaint on oath and in writing, supported by affidavit has been made to me, the undersigned Judge of COUNTY County, Florida, by YOUR RANK YOUR NAME, a law enforcement officer employed by the YOUR AGENCY, who was first duly Sworn, deposes and says that HE/SHE (BASED ON YOU) has reason to believe the laws of the State of Florida have been violated and are now being violated and there is now being kept in or on the below-described premises and/or the curtilage of the same certain evidence, fruits, or instrumentalities, including one or more cellular telephones, of that crime to be found in or on the following described premises located in COUNTY County, Florida:

EXACT SAME DESCRIPTION USED IN YOUR APPLICATION (PAGE 1)

EXACT SAME DIRECTIONS TO PHONE USED IN YOUR APPLICATION (PAGE 1).

SAID PREMISES being located in the County of COUNTY, State of Florida, in the control of the WHO HAS CONTROL OF STRUCTURE, and being the property of WHO OWNS STRUCTURE, and Affiant having stated probable cause to believe that the following described items are upon/within said premises, the following are to be seized:

|  |  |  |
| --- | --- | --- |
| **CyberTip Creation Date and Time** | **CyberTip Number** | **ESP / ISP** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

ALL OF WHICH are being kept and/or used and/or obtained in and/or is evidence of a felony violation of the laws of the State of Florida, to-wit:

Florida Statute 827.071- Sexual performance by a child; child pornography

NOW THEREFORE, you or either of you, YOUR RANK YOUR NAME and officers with the above agencies, with such lawful assistance as may be necessary, are hereby commanded, in the daytime or in the nighttime, or on Sunday, or as the exigencies of the occasion may demand, to enter the said premises and the curtilage thereof, and then and there to search diligently for said property described in this warrant, and if the same or any part thereof be found on said premises, you are hereby authorized to seize, search, and secure the same, **and to conduct a further search, on-site and/or off-site, of any item seized**, and to make return of your doings under this warrant to a court with jurisdiction within ten days from the date hereof, and you are likewise commanded in the event you seize or take property or materials mentioned in the warrant to safely keep the same until otherwise ordered by a court having jurisdiction thereof, and that you give proper receipt for said property and deliver a copy of this warrant to the person from whom taken or those in whose possession it is found or in the absence of any such person to leave said copy in the place where said property or material is found, and you are further directed to bring said property so found and any person arrested in connection therewith before the court having jurisdiction of this offense to be disposed of according to law. You, or either of you, with such lawful assistance as may be necessary, are also authorized and commanded to search those vehicles and structures which you may encounter on the premises or curtilage thereof pursuant to the execution of this warrant.

WITNESS, my hand and official seal this \_\_\_ day of MONTH, 20\_\_.

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

JUDGE