

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON) NO. 16-164
)
) :SS
COUNTY OF KING) AFFIDAVIT FOR SEARCH WARRANT

Detective Daljit Gill, being first duly sworn on oath, deposes and says:

Upon sworn complaint made before me, attached and incorporated hereto, there is probable cause to believe that the crime(s) of **RCW 9.68A.070 Possession of Depictions of Minor Engaged in Sexually Explicit Conduct and RCW 9.68A.050 Dealing in Depictions of Minor Engaged in Sexually Explicit Conduct** is/are being committed, has/have been committed, and/or are about to be committed in King County, and that evidence of that/those crime(s); or contraband, the fruits of crime, or things otherwise criminally possessed; or weapons or other things by means of which a crime has been committed or reasonably appears about to be committed; or a person for whose arrest there is probable cause, or who is unlawfully restrained is/are concealed in or on certain premises, vehicles or persons.

Evidence of the crime of **RCW 9.68A.070 Possession of Depictions of Minor Engaged in Sexually Explicit Conduct, and RCW 9.68A.050 Dealing in Depictions of Minor Engaged in Sexually Explicit Conduct,**

Contraband, the fruits of a crime, or things otherwise criminally possessed, and

Weapons, or other things by which a crime has been committed or reasonably appears about to be committed, and

A person for whose arrest there is probable cause, or who is unlawfully restrained is/are located in, on, or about the following described premises, vehicle or person:

Is/are located on or about the following premises:

[REDACTED] located in the City of Seattle, County of King, and State of Washington.

Affidavit for Search Warrant (Continued)

My belief is based upon the following facts and circumstances:

TRAINING AND EXPERIENCE

Your affiant is a Seattle Police Detective with the Seattle Police Department since 2007. I am assigned to the Internet Crimes Against Children's Unit, where I am tasked with investigating electronic-facilitated crimes against children, sexual exploitation of children, and depictions of minors engaged in sexually explicit conduct.

Of my eight (8) + years in law enforcement, my training and experience has included the following. I have had classroom as well as on the job training in crime scene investigation, evidence collection and handling, as well as interview and interrogation. I have training and experience in the areas of: search warrant preparation and service, Internet Exploitation of Children Investigations, Internet Service Providers, Online Undercover and Sting Operations. My training and experience has been through supervisors and other experienced local, state and federal Detectives/Agents who have conducted numerous Sexual Exploitation of Children/Child Pornography investigations as well as case detective assignments and training/seminars since November 2011.

I have attended several webinars specific to the sexual exploitation to include: CyberTip Training, Interpreting CyberTip Reports, Introduction to Computer Crimes, Tracing IP Part 1 & 2. I attended several web based training courses to include: CyberTips Overview, Basic Computer Skills for Law Enforcement.

In addition, I have attended and successfully completed the following training specific to my current assignment:

- 32 hours of Child Interviewing & Investigation (Washington State Criminal Justice Training Commission)
- NW3C (National White Collar Crime Center) Courses as follows:

Affidavit for Search Warrant (Continued)

- ISEE-T3 (Identification & Seizure of Electronic Evidence)
- STOP/Cyber-Investigation (Secure Techniques for Onsite Preview);
- BDRA training (Basic Data Recovery & Acquisition)
- 40 hours of Victim Support Team
- Innocence Lost Conference-Seminar (WSCJTC)
- ICAC Investigative Techniques Training Program

Prior to my career in law enforcement I was a Medical Assistant/X-ray Technician. I assisted in child well-check physicals and provided physician ordered immunizations. I attended several Anatomy and Physiology and continuing medical education seminars.

BACKGROUND

For the purposes of this affidavit, a “minor” refers to any person less than eighteen years of age and for the purpose of this search warrant, ‘child pornography’ means depictions of minors engaged in sexually explicit conduct.

Based on my training, experience and collaboration with ICAC detectives, 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

Affidavit for Search Warrant (Continued)

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 computer. 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 myriad 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.

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.

Affidavit for Search Warrant (Continued)

An IP address is typically comprised of a series of four (4) 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 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 child pornography 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 child pornography.

When an ISP receives such a complaint or other notice of suspected child pornography, 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 child pornography 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 child pornography, 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.

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

The ISPs 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 child pornography.

Affidavit for Search Warrant (Continued)

The hash values in the transmitted file(s) are contained in the “metadata” associated with the files. This “metadata” is “data about data,” e.g. information about the file that is created and used at various times along the creation, transmission, and receipt of the file. For example metadata may include information about what language it is written in, what tools were used to create it, sender information, and what sort of files are associated with it.

When the ISP detects a file passing through its network that has, in its metadata, the same hash value as an image or video file of suspected child pornography 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 ISP or ISP has a duty to report to NCMEC any apparent child pornography it discovers “as soon as reasonably possible.” 18 U.S.C. § 2258A(a)(1). The CyberTipline 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 child pornography. 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 child pornography to the identical hash value in the suspect transmission.

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 WHOIS is a query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of Internet resources, such as a domain name or an IP address block.

The act of ‘downloading’ is commonly described in computer networks 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, FTP server, 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 established in 1984 by the United States Congress. Primarily funded by the Justice Department, the NCMEC acts as an information 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, child sexual abuse and child pornography.

The Center provides information to help locate children reported missing (by parental abduction, 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 child pornography; 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.

Affidavit for Search Warrant (Continued)

Internet Crimes Against Children (ICAC) is a task-force started by the 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 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 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. The Seattle Police Department has been designated as the Regional ICAC Task Force by the Office of Juvenile Justice and Delinquency Prevention (OJJDP).

Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of depictions of minors engaged in sexually explicit conduct (child pornography):

- a. Child pornography collectors 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;
- b. Collectors of child pornography 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. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification, often to relive past sexual experiences with children. 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 desired sexual acts;
- c. Collectors of child pornography sometimes 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, such as a private office. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, images of child erotica, and video tapes for many years;

d. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. These photographs/videos are often maintained in computer files or external digital storage devices. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

From the Internet, I know that the Internet Service Provider (ISP) known as Condointernet is now called Wave G. The company provides high-speed internet services to customers throughout the West Coast.

From the Internet, I know 4chan community support LLC operates 4chan.org. 4chan.org is an image bulletin board service where anyone can upload images and post comments without first registering an account. The site is subdivided into many interest based "boards". On these boards, users create "threads" to discuss specific topics, and can reply to threads with text and images. 4chan receives upwards of 1 million posts per day from users around the world, and relies on its users and a team of volunteer moderators to report and enforce its content guidelines. 4chan generally does not maintain records for postings that have expired, however a few exceptions exist such as when a posting is deleted by a moderator or a user is blocked from posting.

THE INVESTIGATION

For the purposes of this affidavit, a "minor" refers to any person less than eighteen years of age and for the purpose of this search warrant, 'child pornography' means depictions of minors engaged in sexually explicit conduct.

Affidavit for Search Warrant (Continued)

On or about February 05, 2016, 4chan community support LLC, an image bulletin board service, discovered one of their users had uploaded one or more files of suspected child pornography to the internet at <https://boards.4chan.org/int/thread/54655488#p54657951>. 4chan subsequently made a report to National Center for Missing & Exploited Children (NCMEC), who documented the complaint(s) in CyberTip #8308166. The CyberTip report was then forwarded to the Seattle Police Department ICAC Unit.

In CyberTip #8308166, identifying information provided to NCMEC, by 4chan, included the IP address which was reportedly used to facilitate the upload of the file(s) [REDACTED]. This associated upload was reported to be 02-05-2016 @ 21:13:49 UTC.

Using a publicly available website, MAXMIND, I conducted a lookup of IP [REDACTED] which revealed the registrant was Condointernet (also known as Wave G), as reported on the CyberTip, and furthermore, appears to geo-locate to the approximate area of Seattle, WA.

4chan provided one (1) file in their report to NCMEC. I reviewed the file and describe it as follows:

NCMEC CyberTip # 8308166 contains a file name as reported by 4chan to be 1454706829391.webm. The pre-upload file name is reported to be "london keys.webm".

File 1454706829391.webm is a video file. The video depicts a 2-3 year old, white male child with light brownish blonde hair, and a fully nude, adult white female, with brown hair pulled into a bun. The female appears to adjust the camera several times as to capture what she is doing. The video appears to be filmed inside a bedroom, on the floor next to a bed. The female and the 2-3 year old child are on top of sheets and blankets located on the floor, which have a green and burgundy floral pattern.

The 2-3 year old child is wearing an orange long sleeved top with white sleeves and is initially wearing dark underwear; however the adult female removes the underwear. The child is then nude from the waist down. The (nude) adult female then places the child's penis inside her mouth as he

Affidavit for Search Warrant (Continued)

is lying on his back. She then lifts the child up, lies down on her back and brings the child to straddle her neck area with his small feet tucked under her armpits, as she inserts his penis into her mouth. The adult female then moves the child down to her vaginal area, and then lifts the child up to her chest, brings his face into hers and begins to kiss him mouth to mouth.

Based upon general lack of development, size and overall stature I believe the child to be approximately 2-3 years of age. I believe this file depicts the sexual exploitation of a child as outlined in RCW 9.68A.

On February 24, 2016, I contacted King County Superior Court Honorable Judge Ken Schubert and obtained a legally valid search warrant for 4chan and Condointerent "Wave G".

Wave G's response for IP address [REDACTED] for the date/time of 02-05-2016 @ 21:13:49 UTC indicated the IP address was issued to the subscriber David Robinson with the service address of [REDACTED]

I verified utilizing Department of Licensing, public records that David Robinson, Janice Bultmann and [REDACTED] have [REDACTED] as their listed address. I physically responded to [REDACTED]

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

Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when the files have been deleted, they can be recovered using forensic tools. This is so because when a person believes they have deleted a file they are usually only deleting the index to the file and the file space is listed to the computer as

“available” and will only be overwritten when the computer needs to store something else in its place. The actual data still exists on the actual hard drive.

Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example registry information, configuration files, user profiles, e-mails, e-mail address books, “chats”, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the storage medium at a relevant time.

PLACES TO BE SEARCHED

Based on the above facts and circumstances I believe that one or more person(s) and/or computer(s) located at [REDACTED] are or were involved in violation of RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit and RCW 9.68A.050 Dealing in Depictions of Minor Engaged in Sexually Explicit Conduct.

I believe that the seizure and subsequent examination of the items listed below will assist in identifying the individual(s) engaged in these offenses. Based upon this I request that a search warrant be issued directing the search of:

Premise of:

[REDACTED] located in the City of Seattle, County of King, and State of Washington.

ITEMS TO BE SEARCHED FOR

From locations listed above [REDACTED] and for any computer, computer hard drive, or other physical object upon which computer or digital data can be recorded (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant, I am requesting permission to search for, seize, and subsequently examine the following:

Affidavit for Search Warrant (Continued)

- A. Personal computer hardware to include: the computer system case with internal components, motherboard, Central Processing Unit (CPU), memory, etc., internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, zip drives, optical storage devices, transistor-like binary devices, video cameras, digital cameras, cell phones, and any other memory storage devices); peripheral input / output devices (such as keyboards, mouse/track ball/pad, video display monitor); and all related cables, power cords and connections, RAM or ROM units or CD ROM; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).
- B. Computer software applications used by the computer system and any related components. Software is stored in electronic, magnetic, optical, or other digital form.
- C. Computer-related documentation that explains or illustrates how to configure or use the computer hardware, software, or other related items/devices. The documentation consists of written, recorded, printed, or electronically stored material.
- D. Computer-related passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security may consist of hardware, software or other programming code.
- E. Digital data that may be kept on any computer related storage device as listed in 'A' above. The specific data will be (or will contain or incorporate) digital video and/or image files depicting minors engaged in sexually explicit conduct, any digital data related to the trading or exchange of depictions of minors engaged in sexually explicit conduct, and any digital "user attribution" evidence to include, but not limited to, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) that may be evidence of who used or controlled the computer or storage medium at a relevant time.
- F. Photographs of the interior and exterior of the listed residence.
- G. Papers showing dominion and control.
- H. Any other evidence of the crime(s) of RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct to include, but not limited to, videotapes, books,

Affidavit for Search Warrant (Continued)


magazines, catalogs, photographs, film, notebooks, diaries, or other documents pertaining to the possession or dealing of child pornography, to include printed material documenting any communication with other persons regarding the trading or exchange of depictions of minors engaged in sexually explicit conduct.

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

I certify under penalty of perjury under the laws of the State of Washington that the foregoing is true and correct.

Affiant Signature:


Detective Daljit Gill
Seattle Police Department #7419



Judge

BILL BOWMAN

Printed or Typed Name of Judge

3/28/16 2:55am/gmj

Date/ Time

Issuance of Warrant Approved:
DANIEL T. SATTERBERG
King County Prosecuting Attorney

By: s/ Cecelia Gregson, WSBA # 31439
Senior Deputy Prosecutor Criminal Division