

SUPERIORCOURT FOR KING COUNTY

STATE OF WASHINGTON)
) ss.
COUNTY OF KING)

NO. 14-130

SEARCH WARRANT

TO ANY PEACE OFFICER IN THE STATE OF WASHINGTON:

Upon sworn complaint made before me there is probable cause to believe that the crime(s) of **RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct** has been committed and that evidence of the crime(s); or contraband, the fruits of the crime, or things otherwise criminally possessed; or weapons or other things by means of which a crime has been 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.

YOU ARE COMMANDED TO:

1. Search, within 10 days of this date, the premise, vehicle, or person described as follows:

A. **Comcast Cable Communications, 650 Centerton Road, Moorsetown, New Jersey 08057**

This warrant is issued pursuant to RCW 10.96.020. A response is due within twenty business days of receipt, unless a shorter time is stated herein, or the applicant consents to a recipient's request for additional time to comply.

2. Seize if located, the following property or person (s):

From location "A" above and for the Internet Protocol addresses of:

Search Warrant Continued

- 2601:8:b100:dc1:41d4:193b:16d4:ac09 on 12-29-2013 04:45:28 UTC
- 2601:8:b100:dc1:616b:6150:1768:1c45 between 12-13-2013 00:28:40 UTC and 12-29-2013 02:48:31 UTC,

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** to include:

1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address.
5. Subscriber's email account names
6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Any other information relating to the identity of the subscriber

3. Promptly return this warrant to me or the clerk of this court; the return must include an inventory of all property seized.

A copy of the warrant and a receipt for the property taken shall be given to the person from whom or from whose premises property is taken. If no person is found in possession, a copy and receipt shall be conspicuously posted at the place where the property is found.

Date: 1-31-2014 Time: 10:00 (AM/PM)

JUDGE Alex J. Raep

Helen H. Halper
Printed or Typed Name of Judge

Search Warrant Continued

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

SUPERIOR COURT FOR KING COUNTY

In the Matter of the Search of)

NO. 14-130

IP 2601:8:b100:dc1:41d4:193b:16d4:ac09) ss.

IP 2601:8:b100:dc1:616b:6150:1768:1c45)

~~[proposed]~~ ORDER

PROHIBITING DISCLOSURE

Based upon the application of your affiant for a search warrant in the above captioned matter and the representations made therein, and the preclusion of notice provisions of 18 U.S.C. § 2705(b), it is HEREBY ORDERED that:

Comcast Cable Communications, Inc shall not provide notification to any person, including the subscriber or customer to whom the requested materials relate, of the existence of the search warrant for a period of ninety (90) days from the date of this order.

Date/ Time: 1-21-2014 10 AM

JUDGE *Helan L. Halpert*

Helan L. Halpert
Printed or Typed Name of Judge

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON)
) ss.
COUNTY OF KING)

NO. 14-129

SEARCH WARRANT

TO ANY PEACE OFFICER IN THE STATE OF WASHINGTON:

Upon sworn complaint made before me there is probable cause to believe that the crime(s) of **RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct** has been committed and that evidence of the crime(s); or contraband, the fruits of the crime, or things otherwise criminally possessed; or weapons or other things by means of which a crime has been 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.

YOU ARE COMMANDED TO:

1. Search, within 10 days of this date, the premise, vehicle, or person described as follows:

A. Google, Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043

This warrant is issued pursuant to RCW 10.96.020. A response is due within twenty business days of receipt, unless a shorter time is stated herein, or the applicant consents to a recipient's request for additional time to comply.

2. Seize if located, the following property or person (s):

From location "A" above and for the email address rckllnjns@gmail.com, reported in CyberTip #2254437, evidence of the crime of **RCW 9.68A.070 Possession of depictions of minor**

Search Warrant Continued

engaged in sexually explicit conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct to include:

1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address
5. Subscriber's additional email account name(s)
6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Contents of all email for the listed account as well as any associated email accounts *(limited in time to 11-29-2013 to date)*
9. Contents of Google Drive account for the listed account as well as any associated accounts
10. Contents of all related Picasa photos and videos for the listed account as well as any associated accounts
11. Any other information relating to the identity of the subscriber

3. Promptly return this warrant to me or the clerk of this court; the return must include an inventory of all property seized.

A copy of the warrant and a receipt for the property taken shall be given to the person from whom or from whose premises property is taken. If no person is found in possession, a copy and receipt shall be conspicuously posted at the place where the property is found.

Date: 1-31-2014 Time: 9:59 AM/PM

JUDGE R. J. Nagler

Helen L. Halpert
Printed or Typed Name of Judge

warrant served HHH

Search Warrant Continued

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

SUPERIOR COURT FOR KING COUNTY

In the Matter of the Search of)

rckllnjns@gmail.com) ss.

)

NO. 14-129

~~Proposed~~ ORDER

PROHIBITING DISCLOSURE

Based upon the application of your affiant for a search warrant in the above captioned matter and the representations made therein, and the preclusion of notice provisions of 18 U.S.C. § 2705(b), it is HEREBY ORDERED that:

Google, Inc shall not provide notification to any person, including the subscriber or customer to whom the requested materials relate, of the existence of the search warrant for a period of ninety (90) days from the date of this order.

Date/ Time: 1-31-2014 10:02 am

JUDGE

Helen L. Halpert

Helen L. Halpert

Printed or Typed Name of Judge

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON)

NO. 14-129 / 130

:ss

COUNTY OF KING)

AFFIDAVIT FOR SEARCH WARRANT

The undersigned on oath states: I believe that:

Evidence of the crime of **RCW 9.68A.070 Possession of Depictions of Minors 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 in, on or about the following described premise, vehicle or person:

1. **Google, Inc, 1600 Amphitheater Parkway, Mountain View, California 94043**
2. **Comcast Cable Communications, 650 Centerton Road, Moorsetown, New Jersey 08057**

My belief is based upon the following facts and circumstances:

Your Affiant, Detective Ian Polhemus, #5789, has been employed as a Seattle Police Officer since July 7th, 1992 and since November 2007, has been assigned as an investigator with the Internet Crimes Against Children Task Force with the primary responsibility of investigating

Affidavit for Search Warrant (Continued)

electronic-facilitated crimes against children, sexual exploitation of children, and depictions of minors engaged in sexually explicit conduct.

Of my twenty-one (21) + 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 and am also a Certified Digital Forensic Examiner (CyberSecurity Institute). 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 2007.

I participate regularly in the sharing, exchange, and discussion of information related to child sexual exploitation with local, state and federal law enforcement agencies as well as relevant reading/training materials.

I have attended several seminars specific to the sexual exploitation of children to include attendance at the 2008, 2012 and 2013 Dallas Crimes Against Children Conference, the 2008 Project Safe Childhood National Conference sponsored by the United States Department of Justice, the National Law Center for Children and Families National Seminar (Confronting the Challenge of Sexual Exploitation), the 2009 Digital Crimes Consortium and Law Enforcement Technology Expo as well as both the 2010 and 2011 National ICAC Conferences.

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

- 24 hours of Advanced Responders Search & Seizure of Small Office & Home Office Networks

Affidavit for Search Warrant (Continued)

- 36 hours of ICAC Task Force Investigative Techniques
- 36 hours of ICAC Undercover Operations
- 36 hours of Multi-disciplinary Investigation & Prosecution of Computer-Facilitated Child Sexual Exploitation
- Completion of Computer Forensics Fundamentals, Core Competencies, as well as 40 hours of Computer Forensics Core Competencies certification (CyberSecurity Institute)
- Over 125 hours of undercover peer-to-peer (P2P) investigations training, to include 36 hour certification as an ICAC P2P instructor. Trained in the operation of RoundUp, Ephex and ARES undercover investigative software tools.
- 32 hours of Child Interviewing & Investigation (Washington State Criminal Justice Training Commission)
- Successful completion of the 100 hour 'Fast Track Program' sponsored by NW3C (National White Collar Crime Center). Courses included ISEE-T3 (Identification & Seizure of Electronic Evidence: Train the Trainer); STOP/Cyber-Investigation (Secure Techniques for Onsite Preview); BDRA training (Basic Data Recovery & Acquisition); and IDRA training (Intermediate Data Recovery & Analysis).
- osTriage and TUX4N6 on-scene preview tools
- 8 hrs of Forensic Medical Analysis of Child Development & Maturation

BACKGROUND

For the purposes of this affidavit, a "minor" refers to any person under 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 and experience 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,

Affidavit for Search Warrant (Continued)

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 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.

Affidavit for Search Warrant (Continued)

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 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.

Nowadays, in addition to every computer, nearly every cellular telephone and gaming console is connected to the Internet, not to mention the infrastructure hardware required to make these devices work. As a result of this rapid growth, IPv4 addresses are running out, and fast. According to the Number Resource Organization, less than ten percent of them remained in the Internet Assigned Numbers Authority (IANA) free pool as of the beginning of 2010.

Affidavit for Search Warrant (Continued)

Through the use of tools like Network Address Translation (NAT), users have extended the life of IPv4, because NAT allows multiple devices to speak to the Internet through a single IP address, while the router in that particular household or business keeps track of which device(s) are receiving and sending information.

The solution to IP address depletion is simple: developing a more robust numbering system will allow for far more IP addresses. IPv6 (the newer Internet Protocol) holds 340,282,366,920,938,463,463,374,607,431,768,211,456 IP addresses. This exponentially larger pool of IP addresses is the key to the future growth of the Internet, and companies that use and distribute IP addresses will need to adapt their networks and systems to use IPv6. Without IPv6, the Internet's expansion and innovation could be limited, and the underlying infrastructure will become increasingly complex to manage.

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,

Affidavit for Search Warrant (Continued)

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

Affidavit for Search Warrant (Continued)

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.

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 ESP 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.

Affidavit for Search Warrant (Continued)

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; extrafamilial 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.

Affidavit for Search Warrant (Continued)

- 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'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;

Affidavit for Search Warrant (Continued)

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 "Google" is an American multinational public corporation invested in Internet search, cloud computing, advertising technologies, and search engines. Google hosts and develops a number of Internet-based services and products. Google's rapid growth since its incorporation has triggered a chain of products, acquisitions, and partnerships beyond the company's core web search engine. The company offers online productivity software, such as its Gmail email service, and social networking tools, including Orkut and, more recently, Google Buzz and Google+. Google's products extend to the desktop as well, with applications such as the web browser Google

Affidavit for Search Warrant (Continued)

Chrome, the Picasa photo organization and editing software, and the Google Talk instant messaging application.

From the Internet, I know that the Internet Service Provider (ISP) known as Comcast Corporation (through its operating company subsidiaries) is the nation's leading provider of cable, entertainment, and communications products and services, currently with nearly 22.8 million cable customers, nearly 17.6 million high-speed Internet customers and over 9 million voice customers as of January 2012. More information about Comcast and its products and services is available at <http://www.comcast.com>.

THE INVESTIGATION

On or about December 29, 2013, the Internet Service Provider (ISP) known as Google, discovered one of their subscribers had uploaded one or more files of suspected child pornography to the Internet on 12-29-2013 @ 04:45:28 UTC. Google subsequently made a report to the National Center for Missing & Exploited Children (NCMEC), who documented the complaint(s) in CyberTip #2254437.

Identifying information provided to NCMEC, by Google, included the IP address reportedly used to facilitate the upload of the image (2601:8:b100:dc1:41d4:193b:16d4:ac09), an email address of rckllnjns@gmail.com and IP logs dating from November 30, 2013 to December 29, 2013.

A WHOIS lookup of IP 2601:8:b100:dc1:41d4:193b:16d4:ac09 revealed that the registrant was Comcast, as reported on the CyberTip, and furthermore, appears to geo-locate to the approximate area of Seattle, WA.

I reviewed the reported one (1) file and further describe it as follows:

The file titled, "jimmy bs arlos.jpg", is an image file that depicts three (3) persons. One of the persons, a young, male child, is receiving a blowjob from another person. Based upon the primary child's lack of physical development, to include the lack of any pubic hair, miniature

Affidavit for Search Warrant (Continued)

penis and testicles, I'd estimate his age at approximately 8-12 years. The child performing the sex act also appears to be a male and based upon his facial features and lack of shoulder development, I'd estimate his age to be approximately the same. The third person depicted in the photo is not visible enough to provide a description of age or sex.

I believe this file depicts the sexual exploitation of a child as outlined in RCW 9.68A.

PLACES TO BE SEARCHED

Based upon the above facts and circumstances I request that a search warrant be issued directing the search of location #1 and #2 above (Google and Comcast respectively). I also request that any of the below listed items located during this search be seized. The items to be seized will be furnished by Google and Comcast. The obtainment of this information I believe will assist in identification of the individual(s) engaged in activities in violation of RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct.

ITEMS TO BE SEARCHED FOR

From location #1 listed above (Google), and for the email address rckllnjns@gmail.com, reported in CyberTip #2254437, I am requesting permission to search for and seize the following:

1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address
5. Subscriber's additional email account name(s)

Affidavit for Search Warrant (Continued)

6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Contents of all email for the listed account as well as any associated email accounts
9. Contents of Google Drive account for the listed account as well as any associated accounts
10. Contents of all related Picasa photos and videos for the listed account as well as any associated accounts
11. Any other information relating to the identity of the subscriber

From location #2 listed above (Comcast), and for the Internet Protocol addresses of:

- **2601:8:b100:dc1:41d4:193b:16d4:ac09** on 12-29-2013 04:45:28 UTC
- **2601:8:b100:dc1:616b:6150:1768:1c45** between 12-13-2013 00:28:40 UTC and 12-29-2013 02:48:31 UTC,

I am requesting permission to search for and seize the following:


1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address.
5. Subscriber's email account names
6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Any other information relating to the identity of the subscriber

Affidavit for Search Warrant (Continued)

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.

REQUEST FOR NONDISCLOSURE AND SEALING

Your affiant requests, pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), that Google, Inc and Comcast Cable Communications be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for a period of ninety days from the date the warrant is issued. The government submits that such an order is justified because notification of the existence of this warrant could jeopardize the ongoing investigation. For example, such a disclosure would give the subscriber an opportunity to notify confederates with whom he has exchanged images of child pornography of this warrant and/or to destroy, conceal or otherwise obfuscate evidence.



Affiant
Seattle Police, Detective, Serial # 5789
(Agency, Title, and Personnel Number)

Subscribed and sworn to me on 1-31-2014 at 10 (AM/PM):



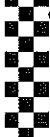
Judge

Affidavit for Search Warrant (Continued)

Issuance of Warrant Approved:
DAN SATTERBERG

By _____
Deputy Prosecuting Attorney

Originals to Court File
Copies to Police File
Copies to Judge



FACSIMILE TRANSMITTAL SHEET

TO: Detective Ian Polhemus	FROM: Comcast Legal Response Center
COMPANY: Seattle Police Department	DATE: 2/3/14
FAX NUMBER: (206) 684-4635	TOTAL NO. OF PAGES INCLUDING COVER: 2
PHONE NUMBER:	SENDER'S REFERENCE NUMBER: 531290-531291
RE: Search Warrant	YOUR REFERENCE NUMBER:

URGENT
 FOR REVIEW
 PLEASE COMMENT
 PLEASE REPLY
 PLEASE RECYCLE

NOTES/COMMENTS:

Attached you will find Comcast's response to the above referenced Search Warrant. If you have any questions regarding this matter, please contact the Legal Response Center at 866-947-8572.

Sincerely,

Comcast Legal Response Center



NE&TO
650 Centerton Road
Moorestown, NJ 08057
866-947-8572 Tel
866-947-5587 Fax

CONFIDENTIAL

January 31, 2014

VIA FACSIMILE

Detective Ian Polhemus
Seattle Police Department
610 5th Avenue, Unit ICAC
Seattle, WA 98104-1886
Fax: (206) 684-4635

Re: Search Warrant
Comcast File #: 531290-291

Dear Detective Polhemus:

The Search Warrant received on 1/31/2014 with respect to the above-referenced matter has been forwarded to the Legal Response Center for a reply. The Search Warrant requests Comcast to produce certain subscriber records pertaining to the following IP addresses:

- 2601:8:b100:dc1:41d4:193b:16d4:ac09 assigned on 12/29/2013 at 04:45:28 UTC.
- 2601:8:b100:dc1:616b:6150:1768:1c45 assigned between 12/13/2013 at 00:28:40 UTC and 12/29/2013 at 02:48:31 UTC.

Based on the information provided pursuant to the Search Warrant, the subscriber information obtained has been provided below:

Subscriber Name: RICK JONES
Service Address: 1530 NW MARKET ST UNIT 211
SEATTLE, WA 98107-5243
Telephone #: 206-786-9081
Type of Service: High Speed Internet Service
Account Number: 8498320013701317
Start of Service: 01/07/2011
Account Status: Active
IP Assignment: Dynamically Assigned
Current IP Address: 2001:0558:600A:0062:0434:6030:8BD3:72E2 as of 01/31/2014
24.22.131.195 as of 01/31/2014
E-mail User Ids: jonesrick211
(the above user ID(s) end in @comcast.net)
Method of Payment: Statement sent to above address

If you have any questions regarding this matter, please feel free to call 866-947-8572.

Very Truly Yours,

Comcast Legal Response Center

Google Inc.
1600 Amphitheatre Parkway
Mountain View, California 94043



USLawEnforcement@google.com
Fax: 650.249.3429
www.google.com

February 3, 2014

Via Express Courier Only
206-684-8651

Detective Ian Polhemus
Seattle Police Department
610 5th Avenue, Unit B741, Post Office Box 34986
Seattle, Washington 98124

Re: Search Warrant dated January 31, 2014 (Internal Ref. No. 63115-397459)
SW No.: 14-129

Dear Detective Polhemus:

Pursuant to the Search Warrant issued in the above-referenced matter, we have conducted a diligent search for documents and information accessible on Google's systems that are responsive to your request. Our response is made in accordance with state and federal law, including the Electronic Communications Privacy Act. See 18 U.S.C. § 2701 et seq.

We understand that you have requested information regarding the Gmail account(s), *RCKLLNJNS*, as specified in the Search Warrant. Accompanying this letter is responsive information to the extent reasonably accessible from our system, and a signed Certificate of Authenticity which includes a list of hash values corresponding to each file. Google may not retain a copy of this production but does endeavor to keep a list of the files and their respective hash values. To the extent any document provided herein contains information exceeding the scope of your request, protected from disclosure or otherwise not subject to production, if at all, we have redacted such information or removed such data fields.

Finally, in accordance with Section 2706 of the Electronic Communications Privacy Act, Google may request reimbursement for reasonable costs incurred in processing your request.

Regards,

Angelo Christian Nono
Google Legal Investigations Support



CERTIFICATE OF AUTHENTICITY

I hereby certify:

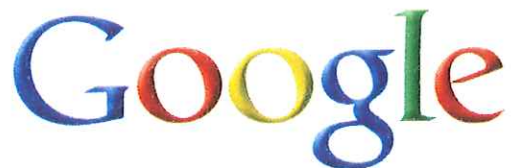
1. I am employed by Google Inc. ("Google"), located in Mountain View, California. I am authorized to submit this affidavit on behalf of Google. I have personal knowledge of the following facts, except as noted, and could testify competently thereto if called as a witness.
2. Google provides Internet-based services to its subscribers, including Gmail, its free email service. Google does not verify any personal information that is submitted by a user at the time of a Gmail account creation.
3. Attached is a true and correct copy of 1 DVD of data pertaining to the Gmail account-holder(s) identified as *RCKLLNJS*, with Internal Ref. No. 63115-397459 ("Document"). Accompanying this Certificate of Authenticity as Attachment A is a list of hash values corresponding to each file.
4. The Document attached hereto is a record made and retained by Google. Google servers record this data automatically at the time, or reasonably soon after, it is entered or transmitted by the user, and this data is kept in the course of this regularly conducted activity and was made by regularly conducted activity as a regular practice of Google.
5. Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

A handwritten signature in blue ink, appearing to read "Angelo Nono".

(Signature of Records Custodian)

Date: February 3, 2014

Angelo Christian Nono
(Name of Records Custodian)



Attachment A: Hash Values for Production Files (Internal Ref. No. 63115-397459)

reckljinjs.AccountInfo.txt:

MD5- f44feac4eb84bee587a2559fd9234608
SHA512-
3c5c765a06a970ef1aa78e885f8715eea3e5498ebc6dc10557900cbd8eb2402cdeee4d158e19dd3fe8
511ef47815d2d96fef129bb145a3c3b3ad7a49e1d0e943

reckljinjs.Drive.zip:

MD5- 3d7b58d1f8e7e073f2781a8fd0df121
SHA512-
012d5be205f3ab70776e5eb64e7ea967373b1db67c14ec60bdba26a3967dd566484987c718e37e31
dc5afeeaa891a11bad68079224428be9be23dc6371dd251c

reckljinjs@gmail.com.Gmail.Content.mbox:

MD5- 653bd30d929f263a603835e1691b6330
SHA512-
536f5f089bf3584b7a5f027ff26a9985ef9acba06a7493f52fd8d0314c47eabb3d808ea6ebd7753add
30cb545ef5f9e7d63daf238a407617c602ca4d42ba565

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON)
)
COUNTY OF KING)

ss.

NO. 14-268
SEARCH WARRANT

TO ANY PEACE OFFICER IN THE STATE OF WASHINGTON:

Upon sworn complaint made before me 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** has been committed and that evidence of the crime(s); or contraband, the fruits of the crime, or things otherwise criminally possessed; or weapons or other things by means of which a crime has been 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.

YOU ARE COMMANDED TO:

1. Search, within 3 days of this date, the premise, vehicle, or person described as follows:

A. 1530 NW Market St #211, City of Seattle, County of King, State of Washington. Property is further described as “Hjarta Condominium”, a mixed-use condominium and retail structure consisting of approximately 16,000 square feet (combined retail and condominium) on 8 floors. Per King County Department of Assessments, Unit #211 is listed as a one (1) bedroom, one (1) bath residence measuring 792 square feet. The owner is listed as “Rick Jones” as of 12/27/2010.

Search Warrant Continued

2. Seize if located and forensically examine the following property or person (s):

Evidence of 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** to include:

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,

Search Warrant Continued

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 minor engaged in sexually explicit conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct to include, but not limited to, videotapes, books, 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.

3. Promptly return this warrant to me or the clerk of this court; the return must include an inventory of all property seized.

A copy of the warrant and a receipt for the property taken shall be given to the person from whom or from whose premises property is taken. If no person is found in possession, a copy and receipt shall be conspicuously posted at the place where the property is found.

Date: 3/19/14 Time: 9:46 AM/PM

JUDGE


R. Roop
Printed or Typed Name of Judge

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON) NO. 14-268
 :SS)
COUNTY OF KING) AFFIDAVIT FOR SEARCH WARRANT

The undersigned on oath states: I believe that:

Evidence of the crime of **RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct and RCW 9.68A.070 Possession of depictions of minor engaged in sexually explicit conduct**, and

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 in, on or about the following described premise, vehicle or person:

1. 1530 NW Market St #211, City of Seattle, County of King, State of Washington. Property is further described as "Hjarta Condominium", a mixed-use condominium and retail structure consisting of approximately 16,000 square feet (combined retail and condominium) on 8 floors. Per King County Department of Assessments, Unit #211 is listed as a one (1) bedroom, one (1) bath residence measuring 792 square feet. The owner is listed as "Rick Jones" as of 12/27/2010.

My belief is based upon the following facts and circumstances:

Your Affiant, Detective Ian Polhemus, #5789, has been employed as a Seattle Police Officer since July 7th, 1992 and since November 2007, has been assigned as an investigator with the

Affidavit for Search Warrant (Continued)

Internet Crimes Against Children Task Force with the primary responsibility of investigating electronic-facilitated crimes against children, sexual exploitation of children, and depictions of minors engaged in sexually explicit conduct.

Of my twenty one (21) + 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 and am also a Certified Digital Forensic Examiner (CyberSecurity Institute). 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 2007.

I participate regularly in the sharing, exchange, and discussion of information related to child sexual exploitation with local, state and federal law enforcement agencies as well as relevant reading/training materials.

I have attended several seminars specific to the sexual exploitation of children to include attendance at the 2008, 2012 and 2013 Dallas Crimes Against Children Conference, the 2008 Project Safe Childhood National Conference sponsored by the United States Department of Justice, the National Law Center for Children and Families National Seminar (Confronting the Challenge of Sexual Exploitation), the 2009 Digital Crimes Consortium and Law Enforcement Technology Expo as well as both the 2010 and 2011 National ICAC Conferences and the 2014 Regional ICAC Conference.

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

Affidavit for Search Warrant (Continued)

- 24 hours of Advanced Responders Search & Seizure of Small Office & Home Office Networks
- 36 hours of ICAC Task Force Investigative Techniques
- 36 hours of ICAC Undercover Operations
- 36 hours of Multi-disciplinary Investigation & Prosecution of Computer-Facilitated Child Sexual Exploitation
- Completion of Computer Forensics Fundamentals, Core Competencies, as well as 40 hours of Computer Forensics Core Competencies certification (CyberSecurity Institute)
- Over 150 hours of undercover peer-to-peer (P2P) investigations training, to include 36 hour certification as an ICAC P2P instructor. Trained in the operation of RoundUp Ephex, ARES and BitTorrent undercover investigative software tools.
- 32 hours of Child Interviewing & Investigation (Washington State Criminal Justice Training Commission)
- Successful completion of the 100 hour 'Fast Track Program' sponsored by NW3C (National White Collar Crime Center). Courses included ISEE-T3 (Identification & Seizure of Electronic Evidence: Train the Trainer); STOP/Cyber-Investigation (Secure Techniques for Onsite Preview); BDRA training (Basic Data Recovery & Acquisition); and IDRA training (Intermediate Data Recovery & Analysis).
- osTriage and TUX4N6 on-scene preview tools
- 8 hrs of Forensic Medical Analysis of Child Development & Maturation

TECHNICAL TERMS

IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

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

Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

For the purposes of this affidavit, a “minor” refers to any person under eighteen (18) years of age and ‘child pornography’ means depiction(s) of minor(s) engaged in sexually explicit conduct.

INVESTIGATION

Affidavit for Search Warrant (Continued)

Pursuant to a complaint of suspected child pornography initiated by the Internet Service Provider known as Google, I conducted a preliminary investigation that resulted in the obtainment of a search warrant and associated affidavit for Comcast Cable Communications and Google. These documents are hereby incorporated by reference to this affidavit and attached as "Addendum A".

On February 3, 2014, and in response to the search warrant issued upon Comcast, I received their response, which included subscriber name (Rick Jones), service address (1530 NW Market St Unit 211, Seattle 98107), telephone (206-786-9081) and email address (jonesrick211@comcast.net).

On February 25, 2014, and in response to the search warrant issued upon Google, I received their response, which included limited email content, content from the subscriber's 'Drive' account (online storage) and basic account information (disable date of 12/29/13, list of additional Google services, additional email address of rickjones@msn.com and account creation date of 5/22/2010).

In reviewing some of the content within the included emails from Google I observed several instances in which the email address rckllnjns@gmail.com was responsible for the distribution of pornographic images. Most of these images depicted younger males, who appeared to be in their mid to late teens and/or contained images considered be erotica.

One email, sent on 12/15/2013, contained 39 image attachments. The subject of the email was, "knee pads?" and the included text read, "Here are some more pictures to keep you on your knees". The attachments appeared to depict the same male child and most were sexually explicit. The boy, who was naked in all but one of the images, had a thin frame, little to no pubic hair and small features. He had an erect penis in several of the images and/or was depicted masturbating. I would estimate the age of the child as approximately 13 years of age.

I believe this file depicts the sexual exploitation of a child as outlined in RCW 9.68A.

Affidavit for Search Warrant (Continued)

On 12/17/2013, rckllnjns@gmail.com received an email in response to “knee pads?” that said, “Hey Rick, I have the complete set. His name is Jessie, he was 15 when the pics were taken. Yes, he is really cute. He was a trouble maker, the juvie assigned a probation officer to supervise him, he is not in jail. I heard there were about 4000 pics, less then 100 made it on the net. Cute kid though....”.

rckllnjns@gmail.com continued this email thread on 12/18/2013 by replying with, “I would have loved to have been the probation officer. I could have saved him from trouble. Hehe. Full staff just thinking about it”.

In an email sent by rckllnjns@gmail.com on 12/21/2013, the writer states in part, “51 years young next month”.

An email sent by rckllnjns@gmail.com on 12/27/2013, and posted on the “hjarta-owners” Google group page, states, “Rick”, is in unit #211.

rckllnjns@gmail.com sent an email on 12/28/2013, containing 65 attachments. Many of these image attachments depicted the same child, in sexually explicit poses. Based upon the overall diminutive stature of the boy and lack of any visible pubic hair, I estimate his age as approximately 9-12 years. Additional attached images depicted other male children, also in sexually explicit poses and many consistent in age with that as described above.

I initiated both investigative and open-source intelligence searches for additional information relating to the aforementioned subscriber and address and determined the following:

- A subject with the name Rick Allen Jones (hereinafter JONES), born 1/20/1963 (51 years of age), with the above listed address per records maintained by the Washington State

Affidavit for Search Warrant (Continued)

Department of Motor Vehicles. This DOB is consistent with the above email sent on 12/21/2013 whereby the writer indicates he will turn 51 in January 2014.

- Washington license ADU2868, registered to JONES at the above listed address per records maintained by the Washington State Department of Motor Vehicles.
- “Rick Jones” receives mail at the above listed address per information obtained from the United States Postal Service.

Additionally, I drove to the residence and confirmed the address. The numbers “1530” are clearly visible on the main entrance to the lockout building as well as the name, “hjarta”. Hanging from the front of the building is a sign that reads, “hjarta”. This sign is adjacent to the front doors.

There is a call box on the exterior of the building, also adjacent to the front doors. I scrolled through the directory and located the name, “Jones R”.

Unit 211, located on the second floor of the building, has a lighted placard to the right of the door. This placard clearly displays the numbers “211” and is consistent with other placards that I observed on other units within the building.

This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

Based on the above facts and circumstances I believe that one or more person(s) and/or computer(s) located at 1530 NW Market St #211, Seattle, are or were involved in violation of RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct and RCW 9.68A.070 Possession of 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.

PLACES TO BE SEARCHED

Based upon the above facts and circumstances I request that a search warrant be issued directing the search of location #1 above (1530 NW Market St #211).

As described above, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information.

I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

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 files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

Affidavit for Search Warrant (Continued)

Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

This application seeks permission to locate not only computer files that might serve as direct evidence of the crime(s) described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the PREMISES because:

Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs may store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

Affidavit for Search Warrant (Continued)

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-mail, e-mail address books, “chat,” 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 computer or storage medium at a relevant time.

A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user’s intent.

In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible

Affidavit for Search Warrant (Continued)

to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, as one example, and would be impractical and invasive to attempt on-site.

Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

Based on the foregoing, and consistent with other investigations of like kind, when persons executing the warrant conclude that it would be impractical to review the media on-site, the

Affidavit for Search Warrant (Continued)

warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Because more than one (1) person(s) may share the PREMISES as a residence, it is possible that the PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

The obtainment of this information I believe will assist in identification of the individual(s) engaged in activities in violation of RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct and RCW 9.68A.070 Possession of depictions of minor engaged in sexually explicit conduct. I also request that any of the below listed items located during this search be seized.

ITEMS TO BE SEARCHED FOR

From location #1 above (1530 NW Market St #211), 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:

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

Affidavit for Search Warrant (Continued)

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.

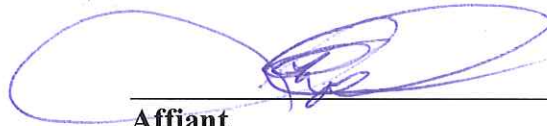
G. Papers showing dominion and control.

H. Any other evidence of the crime(s) of RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct and RCW 9.68A.070 Possession of depictions of minor engaged in sexually explicit conduct to include, but not limited to, videotapes, books, 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

Affidavit for Search Warrant (Continued)

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.



Affiant
Seattle Police, Detective, Serial # 5789
(Agency, Title, and Personnel Number)

Subscribed and sworn to me on March 19, 2014 at 9:45 AM / PM:


Judge R. Rogoff

Issuance of Warrant Approved:
DAN SATTERBERG

Originals to Court File
Copies to Police File
Copies to Judge

By Cecelia Gregson, WSBA #31439
Deputy Prosecuting Attorney

"ADDENDUM A"

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON)
) ss.
COUNTY OF KING)

NO. 14-129
14-268
SEARCH WARRANT

TO ANY PEACE OFFICER IN THE STATE OF WASHINGTON:

Upon sworn complaint made before me there is probable cause to believe that the crime(s) of **RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct** has been committed and that evidence of the crime(s); or contraband, the fruits of the crime, or things otherwise criminally possessed; or weapons or other things by means of which a crime has been 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.

YOU ARE COMMANDED TO:

1. Search, within 10 days of this date, the premise, vehicle, or person described as follows:

A. Google, Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043

This warrant is issued pursuant to RCW 10.96.020. A response is due within twenty business days of receipt, unless a shorter time is stated herein, or the applicant consents to a recipient's request for additional time to comply.

2. Seize if located, the following property or person (s):

From location "A" above and for the email address rckllnjns@gmail.com, reported in CyberTip #2254437, evidence of the crime of **RCW 9.68A.070 Possession of depictions of minor**

Search Warrant Continued

engaged in sexually explicit conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct to include:

1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address
5. Subscriber's additional email account name(s)
6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Contents of all email for the listed account as well as any associated email accounts *(limited in time to 11-29-2013 to date)*
9. Contents of Google Drive account for the listed account as well as any associated accounts
10. Contents of all related Picasa photos and videos for the listed account as well as any associated accounts
11. Any other information relating to the identity of the subscriber

3. Promptly return this warrant to me or the clerk of this court; the return must include an inventory of all property seized.

A copy of the warrant and a receipt for the property taken shall be given to the person from whom or from whose premises property is taken. If no person is found in possession, a copy and receipt shall be conspicuously posted at the place where the property is found.

Date: 1-31-2014 Time: 9:59 AM/PM

JUDGE R. L. Halper

Helen L. Halper
Printed or Typed Name of Judge

warrant served HHH

Search Warrant Continued

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

SUPERIOR COURT FOR KING COUNTY

In the Matter of the Search of
rcklnjns@gmail.com) ss.
)

NO. 14-129
14-268
~~Proposed~~ ORDER

PROHIBITING DISCLOSURE

Based upon the application of your affiant for a search warrant in the above captioned matter and the representations made therein, and the preclusion of notice provisions of 18 U.S.C. § 2705(b), it is HEREBY ORDERED that:

Google, Inc shall not provide notification to any person, including the subscriber or customer to whom the requested materials relate, of the existence of the search warrant for a period of ninety (90) days from the date of this order.

Date/ Time: 1-31-2014 10:02 am

JUDGE

Helen L. Halpert

Helen L. Halpert
Printed or Typed Name of Judge

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON)
) ss.
COUNTY OF KING)

NO. 14-130
14-268
SEARCH WARRANT

TO ANY PEACE OFFICER IN THE STATE OF WASHINGTON:

Upon sworn complaint made before me there is probable cause to believe that the crime(s) of **RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct** has been committed and that evidence of the crime(s); or contraband, the fruits of the crime, or things otherwise criminally possessed; or weapons or other things by means of which a crime has been 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.

YOU ARE COMMANDED TO:

1. Search, within 10 days of this date, the premise, vehicle, or person described as follows:

A. **Comcast Cable Communications, 650 Centerton Road, Moorsetown, New Jersey 08057**

This warrant is issued pursuant to RCW 10.96.020. A response is due within twenty business days of receipt, unless a shorter time is stated herein, or the applicant consents to a recipient's request for additional time to comply.

2. Seize if located, the following property or person (s):

From location "A" above and for the Internet Protocol addresses of:

Search Warrant Continued

- 2601:8:b100:dcl:41d4:193b:16d4:ac09 on 12-29-2013 04:45:28 UTC
- 2601:8:b100:dcl:616b:6150:1768:1c45 between 12-13-2013 00:28:40 UTC and 12-29-2013 02:48:31 UTC,

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** to include:

1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address.
5. Subscriber's email account names
6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Any other information relating to the identity of the subscriber

3. Promptly return this warrant to me or the clerk of this court; the return must include an inventory of all property seized.

A copy of the warrant and a receipt for the property taken shall be given to the person from whom or from whose premises property is taken. If no person is found in possession, a copy and receipt shall be conspicuously posted at the place where the property is found.

Date: 1-31-2014 Time: 10:00 (AM/PM)

JUDGE Allen J. Oesper

Allen J. Oesper
Printed or Typed Name of Judge

Search Warrant Continued

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

() This warrant was issued by the above judge, pursuant to the telephonic warrant procedure authorized JCrR 2.10 and CrR 2.3, on _____, _____ at _____

Printed or Typed Name of Peace Officer,
Agency and Personnel Number

Signature of Peace Officer Authorized
to Affix Judge's Signature to Warrant

SUPERIOR COURT FOR KING COUNTY

In the Matter of the Search of)

IP 2601:8:b100:dc1:41d4:193b:16d4:ac09) ss.

IP 2601:8:b100:dc1:616b:6150:1768:1c45)

NO. 14-130

14-268

[proposed] ORDER

PROHIBITING DISCLOSURE

Based upon the application of your affiant for a search warrant in the above captioned matter and the representations made therein, and the preclusion of notice provisions of 18 U.S.C. § 2705(b), it is HEREBY ORDERED that:

Comcast Cable Communications, Inc shall not provide notification to any person, including the subscriber or customer to whom the requested materials relate, of the existence of the search warrant for a period of ninety (90) days from the date of this order.

Date/ Time: 1-31-2014 10 AM

JUDGE

Mel D. Halpern

Helen L. Halpert

Printed or Typed Name of Judge

SUPERIOR COURT FOR KING COUNTY

STATE OF WASHINGTON

:ss

COUNTY OF KING

)

NO.

14-129 / 130 14-268

)

AFFIDAVIT FOR SEARCH WARRANT

The undersigned on oath states: I believe that:

Evidence of the crime of **RCW 9.68A.070 Possession of Depictions of Minors 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 in, on or about the following described premise, vehicle or person:

1. **Google, Inc, 1600 Amphitheater Parkway, Mountain View, California 94043**
2. **Comcast Cable Communications, 650 Centerton Road, Moorsetown, New Jersey 08057**

My belief is based upon the following facts and circumstances:

Your Affiant, Detective Ian Polhemus, #5789, has been employed as a Seattle Police Officer since July 7th, 1992 and since November 2007, has been assigned as an investigator with the Internet Crimes Against Children Task Force with the primary responsibility of investigating

Affidavit for Search Warrant (Continued)

electronic-facilitated crimes against children, sexual exploitation of children, and depictions of minors engaged in sexually explicit conduct.

Of my twenty-one (21) + 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 and am also a Certified Digital Forensic Examiner (CyberSecurity Institute). 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 2007.

I participate regularly in the sharing, exchange, and discussion of information related to child sexual exploitation with local, state and federal law enforcement agencies as well as relevant reading/training materials.

I have attended several seminars specific to the sexual exploitation of children to include attendance at the 2008, 2012 and 2013 Dallas Crimes Against Children Conference, the 2008 Project Safe Childhood National Conference sponsored by the United States Department of Justice, the National Law Center for Children and Families National Seminar (Confronting the Challenge of Sexual Exploitation), the 2009 Digital Crimes Consortium and Law Enforcement Technology Expo as well as both the 2010 and 2011 National ICAC Conferences.

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

- 24 hours of Advanced Responders Search & Seizure of Small Office & Home Office Networks

Affidavit for Search Warrant (Continued)

- 36 hours of ICAC Task Force Investigative Techniques
- 36 hours of ICAC Undercover Operations
- 36 hours of Multi-disciplinary Investigation & Prosecution of Computer-Facilitated Child Sexual Exploitation
- Completion of Computer Forensics Fundamentals, Core Competencies, as well as 40 hours of Computer Forensics Core Competencies certification (CyberSecurity Institute)
- Over 125 hours of undercover peer-to-peer (P2P) investigations training, to include 36 hour certification as an ICAC P2P instructor. Trained in the operation of RoundUp, Ephex and ARES undercover investigative software tools.
- 32 hours of Child Interviewing & Investigation (Washington State Criminal Justice Training Commission)
- Successful completion of the 100 hour 'Fast Track Program' sponsored by NW3C (National White Collar Crime Center). Courses included ISEE-T3 (Identification & Seizure of Electronic Evidence: Train the Trainer); STOP/Cyber-Investigation (Secure Techniques for Onsite Preview); BDRA training (Basic Data Recovery & Acquisition); and IDRA training (Intermediate Data Recovery & Analysis).
- osTriage and TUX4N6 on-scene preview tools
- 8 hrs of Forensic Medical Analysis of Child Development & Maturation

BACKGROUND

For the purposes of this affidavit, a "minor" refers to any person under 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 and experience 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,

Affidavit for Search Warrant (Continued)

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 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.

Affidavit for Search Warrant (Continued)

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 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.

Nowadays, in addition to every computer, nearly every cellular telephone and gaming console is connected to the Internet, not to mention the infrastructure hardware required to make these devices work. As a result of this rapid growth, IPv4 addresses are running out, and fast. According to the Number Resource Organization, less than ten percent of them remained in the Internet Assigned Numbers Authority (IANA) free pool as of the beginning of 2010.

Affidavit for Search Warrant (Continued)

Through the use of tools like Network Address Translation (NAT), users have extended the life of IPv4, because NAT allows multiple devices to speak to the Internet through a single IP address, while the router in that particular household or business keeps track of which device(s) are receiving and sending information.

The solution to IP address depletion is simple: developing a more robust numbering system will allow for far more IP addresses. IPv6 (the newer Internet Protocol) holds 340,282,366,920,938,463,374,607,431,768,211,456 IP addresses. This exponentially larger pool of IP addresses is the key to the future growth of the Internet, and companies that use and distribute IP addresses will need to adapt their networks and systems to use IPv6. Without IPv6, the Internet's expansion and innovation could be limited, and the underlying infrastructure will become increasingly complex to manage.

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,

Affidavit for Search Warrant (Continued)

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

Affidavit for Search Warrant (Continued)

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.

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 ESP 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 CyperTipline 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.

Affidavit for Search Warrant (Continued)

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; extrafamilial 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.

Affidavit for Search Warrant (Continued)

- 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 USFIS 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'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;

Affidavit for Search Warrant (Continued)

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 "Google" is an American multinational public corporation invested in Internet search, cloud computing, advertising technologies, and search engines. Google hosts and develops a number of Internet-based services and products. Google's rapid growth since its incorporation has triggered a chain of products, acquisitions, and partnerships beyond the company's core web search engine. The company offers online productivity software, such as its Gmail email service, and social networking tools, including Orkut and, more recently, Google Buzz and Google+. Google's products extend to the desktop as well, with applications such as the web browser Google

Affidavit for Search Warrant (Continued)

Chrome, the Picasa photo organization and editing software, and the Google Talk instant messaging application.

From the Internet, I know that the Internet Service Provider (ISP) known as Comcast Corporation (through its operating company subsidiaries) is the nation's leading provider of cable, entertainment, and communications products and services, currently with nearly 22.8 million cable customers, nearly 17.6 million high-speed Internet customers and over 9 million voice customers as of January 2012. More information about Comcast and its products and services is available at <http://www.comcast.com>.

THE INVESTIGATION

On or about December 29, 2013, the Internet Service Provider (ISP) known as Google, discovered one of their subscribers had uploaded one or more files of suspected child pornography to the Internet on 12-29-2013 @ 04:45:28 UTC. Google subsequently made a report to the National Center for Missing & Exploited Children (NCMEC), who documented the complaint(s) in CyberTip #2254437.

Identifying information provided to NCMEC, by Google, included the IP address reportedly used to facilitate the upload of the image (2601:8:b100:dc1:41d4:193b:16d4:ac09), an email address of rckllnjns@gmail.com and IP logs dating from November 30, 2013 to December 29, 2013.

A WHOIS lookup of IP 2601:8:b100:dc1:41d4:193b:16d4:ac09 revealed that the registrant was Comcast, as reported on the CyberTip, and furthermore, appears to geo-locate to the approximate area of Seattle, WA.

I reviewed the reported one (1) file and further describe it as follows:

The file titled, "jimmy bs arlos.jpg", is an image file that depicts three (3) persons. One of the persons, a young, male child, is receiving a blowjob from another person. Based upon the primary child's lack of physical development, to include the lack of any pubic hair, miniature

Affidavit for Search Warrant (Continued)

penis and testicles, I'd estimate his age at approximately 8-12 years. The child performing the sex act also appears to be a male and based upon his facial features and lack of shoulder development, I'd estimate his age to be approximately the same. The third person depicted in the photo is not visible enough to provide a description of age or sex.

I believe this file depicts the sexual exploitation of a child as outlined in RCW 9.68A.

PLACES TO BE SEARCHED

Based upon the above facts and circumstances I request that a search warrant be issued directing the search of location #1 and #2 above (Google and Comcast respectively). I also request that any of the below listed items located during this search be seized. The items to be seized will be furnished by Google and Comcast. The obtainment of this information I believe will assist in identification of the individual(s) engaged in activities in violation of RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct and RCW 9.68A.050 Dealing in depictions of minor engaged in sexually explicit conduct.

ITEMS TO BE SEARCHED FOR

From location #1 listed above (Google), and for the email address rckllnjns@gmail.com, reported in CyberTip #2254437, I am requesting permission to search for and seize the following:

1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address
5. Subscriber's additional email account name(s)

Affidavit for Search Warrant (Continued)

6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Contents of all email for the listed account as well as any associated email accounts
9. Contents of Google Drive account for the listed account as well as any associated accounts
10. Contents of all related Picasa photos and videos for the listed account as well as any associated accounts
11. Any other information relating to the identity of the subscriber

From location #2 listed above (Comcast), and for the Internet Protocol addresses of:

- **2601:8:b100:dc1:41d4:193b:16d4:ac09** on 12-29-2013 04:45:28 UTC
- **2601:8:b100:dc1:616b:6150:1768:1c45** between 12-13-2013 00:28:40 UTC and 12-29-2013 02:48:31 UTC,

I am requesting permission to search for and seize the following:


1. Subscriber's name
2. Subscriber's address
3. Length of service including start date
4. Subscriber's telephone number, instrument number or other subscriber number or identity, including a temporarily assigned network address.
5. Subscriber's email account names
6. Means and source of payment for such service (including any credit card or bank account number)
7. Logs of Internet Protocol (12/29/2013 to date of this warrant)
8. Any other information relating to the identity of the subscriber

Affidavit for Search Warrant (Continued)

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.

REQUEST FOR NONDISCLOSURE AND SEALING

Your affiant requests, pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), that Google, Inc and Comcast Cable Communications be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for a period of ninety days from the date the warrant is issued. The government submits that such an order is justified because notification of the existence of this warrant could jeopardize the ongoing investigation. For example, such a disclosure would give the subscriber an opportunity to notify confederates with whom he has exchanged images of child pornography of this warrant and/or to destroy, conceal or otherwise obfuscate evidence.



Affiant
Seattle Police, Detective, Serial # 5789
(Agency, Title, and Personnel Number)

Subscribed and sworn to me on 1-31-2014 at 10 (AM/PM):


Judge

Affidavit for Search Warrant (Continued)

Issuance of Warrant Approved:
DAN SATTERBERG

By _____
Deputy Prosecuting Attorney

Originals to Court File
Copies to Police File
Copies to Judge

SUPERIOR

COURT FOR KING COUNTY

STATE OF WASHINGTON)
COUNTY OF KING)

NO. 14-268
INVENTORY AND RETURN
OF SEARCH WARRANT

1. I received a search warrant for the premise(s), vehicle(s), or person(s) specifically described as follows:

A. - 1530 NW MARKET ST #211, CITY OF SEATTLE, COUNTY OF KING, STATE OF WASHINGTON, PROPERTY IS FURTHER DESCRIBED AS "HARTA CONDOMINIUM" AND RETAIL STRUCTURE CONSISTING OF APPROXIMATELY 16,000 SQUARE FEET (COMBINED RETAIL AND CONDOMINIUM) ON 8 FLOORS. PER KING COUNTY DEPARTMENT OF ASSESSMENTS UNIT #211 IS LISTED AS A ONE (1) BEDROOM, ONE (1) BATH RESIDENCE MEASURING 792 SQUARE FEET. THE OWNER IS LISTED AS "RICK JONES" AS OF 12/27/2010

2. On the 20 day of MARCH, 2014, I made a diligent search of the above-described premise(s), vehicle(s), or person(s) and found and seized the item(s) listed in section #7.

3. Name(s) of person(s) present when the property was seized:

SEATTLE POLICE OFFICERS

4. The inventory was made in the presence of:

The person(s) named in section #3 from whose possession the property was taken.

Others: _____

5. Name of person(s) served with a copy or description of the place where the copy is posted:

WARRANT AND RETURN OF SERVICE LEFT ON KITCHEN COUNTER.

6. Location where property is currently being retained:

Seattle Police Department Evidence Unit

Other: _____

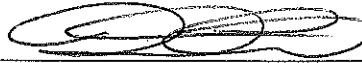
(Continued on next page)

INVENTORY AND RETURN OF SEARCH WARRANT (continued)

Description and location of property and/or person(s) when seized:

- 1- EXTERNAL HDD - KYBURZ - LIVING ROOM COMPUTER DESK
- 2- HP LAPTOP PAUL HP DU 7 - LIVING ROOM COMPUTER DESK - KYBURZ
- 3- HP COMPUTER TOWER A6857C - LIVING ROOM COMPUTER DESK
- 4- VHS VIDEOS - HUPNH - BOTTOM OF HALL CLOSET
- 5- MISC DOCS + PAPERS OF PTC - HENS - LIVING ROOM BAR RACK
- 6- OPTICAL DISCS - ADKINS - BEDROOM BEOSIDE DRAWER
- 7- DIGITAL CAMERA w/MEDIA - HENS - LIVING ROOM SHELVES
- 8- MISC DIGITAL MEDIA - INMAN - BEDROOM CLOSET
- 9- PHOTOS + CD - INMAN - BEDROOM CLOSET
- 10- VHS TAPE - HENS - LIVING ROOM GLASS SHELF

Date: 03-20-2014



Signature of Law Enforcement Officer

SEATTLE POLICE # 6753

Agency and Personnel Number

DETECTIVE CONINC

Print or Type Name

Inventory and Return

Page 2 of 2

White Copy: Court File

Canary Copy: Police File

Pink Copy: Left at premises searched