


FILED

UNITED STATES DISTRICT COURT

OCT 07 2015

for the
Eastern District of California

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY 
DEPUTY CLERK

In the Matter of the Search of)
ONE CELLULAR TELEPHONE, MEID:)
268435460813070093, MODEL NUMBER: SCH-)
R720, CURRENTLY LOCATED AT THE U.S.)
HOMELAND SECURITY INVESTIGATIONS)
OFFICE, 650 CAPITOL MALL SUITE 3-100,)
SACRAMENTO, CALIFORNIA, 95814)

Case No.

2:15 - SW - 568

KJN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE ATTACHMENT A, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed (*identify the person or describe the property to be seized*):

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

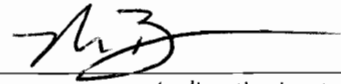
Code Section
18 U.S.C. 2252(a)(2)
18 U.S.C. 2252(a)(4)(B)

Offense Description
Receipt or Distribution of Child Pornography
Possession of Child Pornography

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- Continued on the attached sheet.
- Delayed notice days (give exact ending date if more than 30 days:) is requested
- under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Michael Barge, Special Agent, Homeland Security
Investigations

Printed name and title

Sworn to before me and signed in my presence.

Date: Oct 7, 2015

City and state: Sacramento, California



Judge's signature

Kendall J. Newman, U.S. Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF A
SAMSUNG CELLULAR TELEPHONE,
MEID: 268435460813070093, MODEL
NUMBER: SCH-R720, CURRENTLY
LOCATED AT THE U.S. HOMELAND
SECURITY INVESTIGATIONS OFFICE,
650 CAPITOL MALL SUITE 3-100,
SACRAMENTO, CALIFORNIA, 95814

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Michael Barge, Special Agent, Homeland Security Investigations, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — an electronic device — which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. As described below, I believe there is probable cause that the described electronic device has been used in the commission of Possession, Distribution, and Transportation of Child Pornography (18 U.S.C. §§ 2252 and 2252A) and that evidence, fruits, and instrumentalities of these criminal offenses will be found in the described electronic device.

2. I am a Special Agent with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI), presently assigned to the Office of the Assistant Special

Agent in Charge Sacramento, California. I have been employed as an HSI special agent since March 2004. My duties as an HSI special agent include the investigation of criminal violations relating to child exploitation, including violations pertaining to the illegal production, distribution, receipt and possession of visual depictions of minors engaged in sexually explicit conduct and child pornography in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program and the U.S. Immigration and Customs Enforcement Special Agent Training Program.

3. I have conducted and participated in numerous child exploitation search warrants involving the use of computers and the Internet, and have assisted in the gathering of evidence during execution of those warrants.

4. The information contained in this affidavit is based on my personal knowledge, my training and experience, and information from other law enforcement personnel. I submit this affidavit for the limited purpose of establishing probable cause for the requested search warrant. Accordingly, I have not included each and every fact known to me and other law enforcement officers involved in this investigation.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual

depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Section 2252(a)(4)(B) prohibits any person from knowingly possessing or accessing with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is a Samsung cellular telephone, model number SCH-R720, MEID 268435460813070093, FCC ID A3LSCHR720, hereinafter the "Device." The Device is currently located in an evidence room at the U.S. Homeland Security Investigations Office, 650 Capitol Mall Suite 3-100, Sacramento, California, 95814.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. On or about October 2, 2012, HSI Sacramento Special Agent Nicole Solander accessed a Peer to Peer (P2P) file-sharing network named EDonkey for the purposes of locating computers currently sharing, or that had recently shared, images of child pornography. EDonkey is a system that allows individuals to use their computers to exchange files directly over the Internet without having to go through or access a specific Web site in an arrangement that can be described as computer to computer (or person to person, hence the name "Peer to Peer"). As a result, Special Agent Solander provided me with the Internet Protocol (IP) address of 24.7.174.37, which originated within the Eastern District of California. Upon locating this IP address, Special Agent Solander and I were able to receive a publicly available listing from the suspect's shared folder. The folder contained approximately 92 files that were suspected to contain child pornography (based on a combination of file names and MD4 values) and which were available for distribution by the individual connecting to the EDonkey network through the aforementioned IP address. Message-Digest Algorithm (MD4) is a cryptographic hash function that results in the creation of an associated value often referred to as a digital signature because it provides certainty exceeding 99.99 percent that two or more files with the same MD4 signature are identical copies of the same file regardless of their file names. A review of the information presented to agents indicated that the files were made available on the P2P networks from April 16, 2012, at 9:05 a.m. GMT, through at least October 2, 2012, at 12:16 a.m. GMT. At all of the above times, the available files were continuously associated with IP address 24.7.174.37.

9. Two of the files associated with the IP address 24.7.174.37 are as follows:
- a. ?????? ?? 3? fdsa5-3yo girl pedo r@ygold hussyfan lolitaguy lsm p.mpg

- b. 9yo Jenny nude with legs spread wide apart showing pussy – underage lolita
r@ygold pthc ptsc ddogprn pedo young child sex preteen hussyfan kiddie kiddy
porn.jpg

10. I examined the MD4 values included in the full file list and confirmed that the MD4 values associated with the files in the paragraph above matched files previously identified by law enforcement, and subsequently added into a law enforcement database, as child pornography as defined by Title 18 U.S.C. § 2256. The MD4 values for the image files listed in paragraph 8 are, in order, as follows:

- a. J4BWECEXE7MSVXKMNNOSWKHRNOYXRTEF37
- b. 2VJDD35GIUYPJKNPED4OHI7ZKW4C3RJC

11. Pursuant to this investigation, on October 23, 2012, I examined a copy of the file with the MD4 value of J4BWECEXE7MSVXKMNNOSWKHRNOYXRTEF37. This video is approximately 3 minutes and 25 seconds in length. The video shows a young girl, who appeared to be approximately 4-7 years old, performing oral sex on an unidentified adult male while standing in a bathtub.

12. Pursuant to this investigation, on October 23, 2012, I examined a copy of the file with the MD4 value of 2VJDD35GIUYPJKNPED4OHI7ZKW4C3RJC. This picture depicts a prepubescent girl who appeared to be approximately 7-10 years old lying down with her legs spread and her genital area exposed to view. The prepubescent girl is bound with yellow rope around her thighs, ankles and hands, which are positioned above her head.

13. I can also conclude from training and experience that the search results indicated that a computer connected to the P2P EDonkey network via IP address 24.7.174.37 possessed

and/or distributed child pornography during the time period of April 16, 2012, at 9:05 a.m. GMT, through at least October 2, 2012, at 12:16 a.m. GMT.

14. The IP address 24.7.174.37 is owned by Comcast Cable Communications (hereinafter "Comcast"), and the numbers contained therein indicate that the user was located in the Sacramento, California area. I issued a DHS Summons to Comcast requesting subscriber information associated with the IP address 24.7.174.37 that was utilized between April 16, 2012, at 9:05 a.m. GMT, through at least October 2, 2012, at 12:16 a.m. GMT, which encompasses the dates and times that the IP address referenced above is known to have made numerous files containing suspected child pornography available for distribution over the P2P network.

15. On or about October 15, 2012, Comcast responded to the aforementioned DHS Summons. According to Comcast, the IP address referenced above was registered to customer Ernestine Carlos Mitchell since November 14, 2011. Comcast registration information listed Ernestine Mitchell as residing at 7527 Salton Sea Way, Sacramento, CA 95831.

16. On October 19, 2012, at approximately 12:40 p.m., I conducted a check of the wireless networks in the direct vicinity of 7527 Salton Sea Way, Sacramento, CA. The check revealed no unsecured networks in the area. Sacramento Municipal Utilities District (SMUD) records obtained on October 19, 2012 showed that Albert Mitchell, telephone number (916) xxx-9459, was the account holder for 7527 Salton Sea Way, Sacramento, CA. Public database checks indicated that Albert MITCHELL and Ernestine Mitchell are husband and wife.

17. On October 31, 2012, I obtained a federal search warrant for 7527 Salton Sea Way, CA 95831, signed by the Honorable Judge Dale A. Drozd. The warrant authorized the search and seizure of documents, communications, images and other materials for evidence of

possession and distribution of child pornography including, but not limited to, computers, hard-drives, and cellular telephones.

18. On November 5, 2012, I, along with a team of law enforcement agents, executed the search of 7527 Salton Sea Way, Sacramento, California. Agents conduct a knock and announcement and the front door was answered by Albert MITCHELL (A. MITCHELL). No forced entry was made. Inside the residence agents contacted Ernestine Mitchell as she emerged from a hallway. Both residents were detained momentarily while the residence was secured. As this happened, A. MITCHELL lied when I asked where his pistol was located. An earlier law enforcement database check revealed A. MITCHELL is the registered owner of an 11mm semi-automatic pistol. A. MITCHELL responded that he does not have any pistols and added that he has rifles in the garage against the wall but no pistols. This statement was later proved to be incorrect because agents found 24 pistols inside the residence. Some of the pistols were located inside a locked gun safe in the garage. A. MITCHELL refused to provide the combination to the gun safe until after he spoke with his attorney. Inside the safe agents also found a loose external computer hard drive, which was later found to contain over a thousand image files and hundreds of movie files of suspected child pornography.

19. Seized pursuant to the warrant were the following items: six desktop computers, three laptop computers, two cellular telephones (including the Device), four thumb-drives, ten hard-drives, one tablet computer, eight compact discs, four VHS tapes, seven Betamax tapes, one SD memory card, one backpack, one camera, and miscellaneous documents including A. MITCHELL's U.S. passport. The Device was found on top of a desk next to a computer in a room A. MITCHELL identified as his home office along with several other items that contained suspected child pornography.

20. On November 5, 2012, I interviewed A. MITCHELL regarding this investigation and the execution of the search warrant. A. MITCHELL was advised of and voluntarily waived his rights under Miranda v. Arizona and told me, among other things, that: (a) he used the back bedroom as his home office; (b) he is the only person who used the desktop computer in his office; (c) the desktop computer and a laptop computer in his office are password protected; and (d) he had plans to travel alone to Argentina the next day for a vacation. A desktop computer found in a back bedroom, which had been converted into a home office, contained over two thousand image files and hundreds of movie files of suspected child pornography.

21. Items found during the search confirmed that A. MITCHELL had airline reservations to travel to Cordoba, Argentina with a stop in Lima, Peru. A packed suitcase was also found at the residence which contained children's clothing, a Hello Kitty notepad, pencils, stickers and children's bracelets.

22. HSI Special Agent Kurt Blackwelder conducted an on-scene forensic preview of the desktop computer located in A. MITCHELL's home office. Special Agent Kurt Blackwelder is a trained computer forensic agent. The preview revealed the computer was installed with a P2P file-sharing program named Emule. The program was set up to download files with file names consistent with child pornography. Among the terms found in the titles were "PTHC 2009," "12yo," "10 years," "11 yo," "Susie 8 yo," "PTHC Jenny," and "little slut." Based on my training and experience I know that "PTHC" is a common search term for individuals searching for child pornography and stands for "Pre-Teen Hard-Core," and the term "12yo" is commonly understood to mean 12 years old. After being confronted with the fact that a computer forensic agent had examined the computer in his office and found that it was running Emule (P2P) software and downloading child pornography, A. MITCHELL invoked his right to counsel.

23. On November 5, 2012, A. MITCHELL was placed under arrest based on probable cause that he received child pornography. Based on the above facts, a criminal complaint and federal arrest warrant were signed by Honorable Judge Gregory G. Hollows in the Eastern District of California for A. MITCHELL.

24. On November 15, 2012, A. MITCHELL was indicted in the Eastern District of California for one felony count of receiving child pornography in violation of 18 U.S.C. 2252.

25. Beginning in January 2013 and ending in July 2013, I reviewed a forensic image of the original evidence to include the computers and hard-drives; the image was created by the HSI San Francisco forensics laboratory. Special Agent Blackwelder and I reviewed the documents, digital media and camera for child pornography with negative results. HSI San Francisco Computer Forensic Agent Orin Clapp told me that his lab was unable to examine one of the cellular telephones due to its poor physical condition. The other cell phone, a Samsung with a red back, model number SCH-R720 (the "Device"), was locked with a 9-dot pattern passcode. Attempts to obtain the passcode from either the defendant or the defense team have not been successful. The Device was placed in airplane mode at the so it would remain isolated from the network.

26. During my review, I found suspected child pornography on the following ten items: (1) Iomega Prestige desktop Hard-drive, serial number 6FAB110799; (2) Iomega external Hard-drive, serial number 6FA22800B2; (3) HP desktop Computer tower, serial number 4CE04301SY; (4) Dell Laptop, product key KWJBD-MFY69-KBRG6-38X8M-PTCK8; (5) Averatec Laptop, product key WYVJW-2X3J9-3473P-9H8YM-2HKW8; (6) My Book external Hard-drive, serial number WCASU4890595; (7) Hitachi Hard-drive, serial number K5V3XMLH; (8) Systium Technologies Computer tower, serial number 52000001025, which

contained a Seagate 80 GB hard-drive, serial number 3HV0L7P3; (9) white Computer tower with no identifiers that contained a Western Digital hard-drive, serial number WCA8E6028320; and (10) white Computer tower with no identifiers that contained two hard-drives, one of which was a Western Digital hard-drive, serial number WCAS87826742.

27. Approximately 350 videos and 2,023 images of suspected child pornography were found on two of the ten items: the Iomega Prestige desktop Hard-drive and the HP desktop Computer tower. These items are significant because the Iomega Prestige desktop Hard-drive was found inside a locked gun safe located in the garage (referenced in paragraph 18) and the HP desktop Computer tower was found in a back bedroom that A. MITCHELL identified as his office home (referenced in paragraph 20). Approximately seven of the items were found in A. MITCHELL's home office.

28. On August 14, 2013, a hard-drive containing digital evidence from this case was sent to the National Center for Missing and Exploited Children (NCMEC) to run suspect files against the Child Recognition Identification System. On October 31, 2013, HSI Sacramento received NCMEC report number 73634 relating to suspect files in this case. The NCMEC reported that 406 image files and 68 video files were found that appeared to contain child victims who have been identified by law enforcement based on a review in the Child Recognition Identification System.

29. The Device is currently in an evidence room at the U.S. Homeland Security Investigations Office, located at 650 Capitol Mall Suite 3-100, Sacramento, California, 95814. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Homeland Security Investigations.

The Device has remained powered off and has not been connected to the network while in the HSI evidence room.

30. In my training and experience, examining data stored on devices of this type can also uncover evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. I believe there is probable cause that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. 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.
- b. 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.

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

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. 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 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.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic 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.

- e. Further, in finding evidence of how a device 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.
- f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim's electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL
INTEREST IN CHILDREN OR WHO RECEIVE OR POSSESS
CHILD PORNOGRAPHY**

36. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography:

a. Individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or produce, receive, or possess images 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. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the

inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography almost always 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. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer or cell phone. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone

numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or produce, receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

CONCLUSION

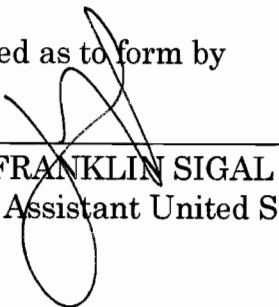
37. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



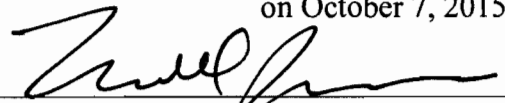
MICHAEL BARGE
Special Agent
Homeland Security Investigations

Approved as to form by



JOSH FRANKLIN SIGAL
Special Assistant United States Attorney

Subscribed and sworn to before me
on October 7, 2015:



KENDALL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a Samsung cellular telephone with the following identification numbers: model number SCH-R720, A0000030C76F0D, 268435460813070093, FCC ID A3LSCHR720, hereinafter the "Device." The Device is currently located at an evidence room at the U.S. Homeland Security Investigations Office, 650 Capitol Mall Suite 3-100, Sacramento, California, 95814.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 2251, 2252(a) and 2252A and involve Albert MITCHELL since April 16, 2012, including:

- a. All stored electronic and wire communications and information in memory on the mobile device, including email, instant messaging, text messages, or other communications, contact lists, images, videos, travel records, information related to the identity of victims, and any other content or records on the phone.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, viewed or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of)
ONE CELLULAR TELEPHONE, MEID:)
268435460813070093, MODEL NUMBER: SCH-R720,)
CURRENTLY LOCATED AT THE U.S. HOMELAND)
SECURITY INVESTIGATIONS OFFICE, 650 CAPITOL)
MALL SUITE 3-100, SACRAMENTO, CALIFORNIA,)
95814)

Case No.

2:15 - SW - 568

KJN

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of California (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before October 20, 2015 (not to exceed 14 days)

[] in the daytime 6:00 a.m. to 10:00 p.m. [X] at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

[] Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

[] for ___ days (not to exceed 30) [] until, the facts justifying, the later specific date of _____.

Date and time issued: Oct 7, 2015 3:40 pm.

[Handwritten signature of Kendall J. Newman]

City and state: Sacramento, California

Kendall J. Newman, U.S. Magistrate Judge
Printed name and title

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date

ATTACHMENT A

The property to be searched is a Samsung cellular telephone with the following identification numbers: model number SCH-R720, A0000030C76F0D, 268435460813070093, FCC ID A3LSCHR720, hereinafter the "Device." The Device is currently located at an evidence room at the U.S. Homeland Security Investigations Office, 650 Capitol Mall Suite 3-100, Sacramento, California, 95814.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 2251, 2252(a) and 2252A and involve Albert MITCHELL since April 16, 2012, including:

a. All stored electronic and wire communications and information in memory on the mobile device, including email, instant messaging, text messages, or other communications, contact lists, images, videos, travel records, information related to the identity of victims, and any other content or records on the phone.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, viewed or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

1 BENJAMIN B. WAGNER
United States Attorney
2 JOSH F. SIGAL
Assistant United States Attorney
3 501 I Street, Suite 10-100
Sacramento, CA 95814
4 Telephone: (916) 554-2700
Facsimile: (916) 554-2900
5

FILED

OCT 07 2015

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
BY _____
DEPUTY CLERK

6 Attorneys for Plaintiff
United States of America
7

8 IN THE UNITED STATES DISTRICT COURT
9 EASTERN DISTRICT OF CALIFORNIA

10 IN RE ORDER REQUIRING GOOGLE, INC.
11 TO ASSIST IN THE EXECUTION OF A
12 SEARCH WARRANT ISSUED BY THIS
13 COURT.

CASE NO.

ORDER

215 - SW - 568

KJN

14 Before the Court is the Government's motion for an order requiring Google, Inc.
15 ("Google") to assist law enforcement agents in the search of an Android Device. Upon
16 consideration of the motion, and for the reasons stated therein, it is hereby

17 ORDERED that Google assist law enforcement agents in the examination of the Samsung
18 cellular telephone with identification numbers: model number SCH-R720, A0000030C76F0D,
19 268435460813070093, FCC ID A3LSCHR720, (the "Android Device"), acting in support of a search
20 warrant issued separately by this Court;

21 FURTHER ORDERED that Google shall, if necessary, reactivate the Google account
22 associated with the Android Device;

23 FURTHER ORDERED that Google shall: (1) provide a single password reset for the mobile
24 device; (2) provide the new password to the law enforcement officer executing the search warrant; and
25 (3) upon unlocking the target mobile device, again reset the Google account password promptly upon
26 notice that the imaging of the phone is complete, without providing it to the law enforcement officer or
27 agency so as to prevent future access;


28 ///

1 FURTHER ORDERED that the reset process need not be unobtrusive to the subject, the subject
2 may receive notice to one or more accounts of the reset, and such notice is not a violation of any seal or
3 nondisclosure requirement;

4 FURTHER ORDERED that the law enforcement agent executing the search warrant is
5 prohibited from using or attempting to use the new password to attempt to access the subject's online
6 accounts other than as synchronized on and stored in memory within the target device at the time of
7 execution of the warrant.

8 Date: Oct 7 2015

Signed,

9
10 
11 Hon. Kendall J. Newman
12 UNITED STATES MAGISTRATE JUDGE