

THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE)
SEARCH OF:)
THE PREMISES KNOWN AS)
XXXX XXXXX XXXX)
XXXXXXXXXXXXX, XXXXXXXX XXXXX)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, XXXXX XXXXXX, a Special Agent with the Federal Bureau of Investigation (FBI), Kansas City, Missouri, being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a sworn officer with the Bureau of Investigation since xxx xxxx, and am currently assigned to the FBI Cyber Crimes Task Force, Kansas City, Missouri. Since xxxx xxxx, I have been assigned to investigate computer crimes to include violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended training such as Missing and Abducted Children provided by the National Center for Missing and Exploited Children (NCMEC) and Innocent Images provided by the FBI.

2. As a SA, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. At all times throughout this affidavit I use the term “child pornography” merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms “visual depiction,” “minor,” and “sexually explicit conduct” as those terms are defined in 18 U.S.C. § 2256 (See Definition Section below).

3. I am investigating the activities of XXXX XXXX XXXXX of **XXXX XXXXX XXXX, XXXXXXXXXXXXXXX, XXXXXXXXXXX XXXXX**. As will be shown below, I submit that there is probable cause to believe that XXXXX has received, possessed, and/or transmitted child pornography, in violation of 18 U.S.C. § 2252. I am submitting this affidavit in support of a search warrant authorizing a search of the residence, located at **XXXX XXXXX XXXX, XXXXXXXXXXXXXXX, Missouri 64058** (the “Premises”), and is more particularly described below, for the items specified in **Attachment A** hereto, which items constitute instrumentalities, fruits, and evidence of the foregoing violations. I am requesting authority to search the entire Premises, including the residential dwelling and any computer and computer media located therein where the items specified in **Attachment A** may be found, and to seize all items listed in **Attachment A** as instrumentalities, fruits, and evidence of crime.

4. The statements in this Affidavit are based in part on information provided by Special Agent xxxx xxxxx of the FBI and my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. § 2252, are presently located at xxxx xxxxxx xxxx, xxxxxxxxxxxxxx, Missouri 64058.

DEFINITIONS

5. The following definitions apply to this Affidavit, as well as **Attachment A** to this Affidavit:
- a. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions;
 - b. “Child Pornography,” means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produce by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. (See 18 U.S.C. § 2256(8)(a) only);
 - c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. (See 18 U.S.C. § 2256(5));
 - d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. (See 18 U.S.C. § 2256(2));
 - e. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;”
 - f. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks);
 - g. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities;

- h. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items;
- i. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it;
- j. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet;
- k. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- l. “Minor” means any person under the age of eighteen years. (See 18 U.S.C. § 2256(1)).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

7. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

13. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

14. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

15. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

16. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying various file directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;
- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment A**; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment A**.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

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

- a. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.
- b. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.
- c. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.
- d. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

- e. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. **THEY ALMOST ALWAYS MAINTAIN THEIR COLLECTIONS IN THE PRIVACY AND SECURITY OF THEIR HOMES OR OTHER SECURE LOCATION.**

YAHOO! GROUPS

18. Yahoo! Inc. is a commercial computer service company that provides services to Internet users that include e-mail, Groups, Internet search capability, games, personal ads, chat, instant messaging, and other services. Using these services is accessed as follows:

- Persons who want to access Yahoo!'s Groups are required to register with Yahoo! to obtain a Yahoo! ID;
 - b. A Yahoo! ID is a unique identifier of a user's account. The registration process requires the selection of an ID (sometimes referred to as a screen name, Login Name, or profile), a password, and the voluntary supply of some personal information;
 - c. Yahoo! Groups is a free service that allows users to bring together family, friends, or associates through a web site and e-mail list. Users with a common interest can create and manage their own Internet-based forum for that interest. There are over two million Groups on Yahoo!. The Groups are organized by categories. Yahoo! Groups include pornographic Groups, some of which contain child pornography;
 - d. Groups provide a web site where members can post photographs, and other files, such as video files;
 - e. In order to access the web features of the Yahoo! Groups service, a user must have a Yahoo! ID, and must sign in. Users would not be able to access the web features (such as the posted photos and files sections on the Group's website) without signing in with their login name and associated password; and
 - f. No one can use another person's login name, unless the initial person registering under that name has divulged both the login name and his password associated with the name.

THE INVESTIGATION

CONCLUSION

FURTHER AFFIANT SAYETH NOT.

xxxx xxxxxxxxxxx, Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me
this ___ day of xxx 2005.

Xxxxxxxxx xxxxxxxxxxx
CHIEF UNITED STATES MAGISTRATE JUDGE