

FILED

OCT 11 2018

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

MAGISTRATE JUDGE
JEFFREY T. GILBERT

UNDER SEAL

In the Matter of the Search of:

Case Number: **18M633**

Apartment 2 of the subdivided two-story single family home located at 6122 South Marshfield, Chicago, Illinois, further described in Attachment A

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Kimberly Castro, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of Illinois, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is evidence, instrumentalities, fruits, and contraband.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, United States Code, Sections 2252 and 2252A	possession, receipt, and distribution of child pornography

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.




Applicant's Signature

KIMBERLY CASTRO, Special Agent, Federal Bureau of Investigation

Printed name and title

Sworn to before me and signed in my presence.

Date: October 12, 2018



Judge's signature

City and State: Chicago, Illinois

JEFFREY T. GILBERT, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Kimberly Castro, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately November 1995.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in multiple forms of media, including computer media. I also have participated in the execution of multiple federal search warrants, many of which have involved child exploitation and/or child pornography offenses. I have participated in the execution of multiple federal search warrants.

3. This affidavit is made in support of an application for a warrant to search Apartment 2 of the subdivided two-story single family home located at 6122 South Marshfield, Chicago, Illinois, described further in Attachment A (the "**Subject Premises**"), for evidence, instrumentalities, fruits, and contraband described further in Attachment B, concerning possession, receipt, and distribution of child

pornography offenses, in violation of Title 18, United States Code, Sections 2252 and 2252A.

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because 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 facts that I believe are sufficient to establish probable cause to believe that evidence, instrumentalities, fruits, and contraband of violations of Title 18, United States Code, Sections 2252 and 2252A, are located at 6122 South Marshfield, Chicago, Illinois.

I. BACKGROUND INFORMATION

5. On or about May 23, 2017, an FBI online covert employee (OCE) was investigating the production of child pornography on the mobile application “live.me”¹ and browsed to a website called “8ch.net.” On 8ch.net, the OCE observed a link entitled “camgirls” with the URL <https://discord.gg/qn4nKst>. Next to the link was an image that depicted two females who appeared to be children wearing bikinis.

6. The OCE clicked on the above link and was re-directed to the following URL: <https://discordapp.com/channels/24203551251531744>. This website was

¹ Live.me is a social media platform for sharing, creating and viewing live streaming videos. Live.me users can stream live video from mobile platforms like Apple iOS or Google Android. Videos streamed from Live.me users can be viewed through the Live.me mobile applications or an internet browser.

entitled “Camgirls,” and the title was accompanied by a thumbnail image of two minor female children kissing each other.

7. Discord owns and operates a free-access all in one voice and text chat application and website with the same name that can be accessed at <http://www.discordapp.com>. A user creates a Discord account and then can communicate with other Discord users. When signing up for a Discord account, a user must agree to Discord’s Terms of Service, which state in part: “You agree not to use the Service in order to: violate any applicable laws or regulations, or promote or encourage any illegal activity....”

8. Discord users can exchange private messages between each other, participate in text chat room discussions, and voice chat. Discord users can also create “servers,” which are like message boards that can be accessed only by users who have an “invitation link.” Within these “servers,” users can set up different “text channels,” wherein users can type written text, including links to files stored on external file-storage sites, and also upload files under eight megabytes which can be viewed by all users of the text channel. Discord users can share files larger than eight megabytes by providing hyperlinks to file sharing websites. Discord servers can have one or many moderators. Moderators have the ability to manage other users, including but not limited to removing users from the server, elevating users hierarchically, and granting users additional accesses. The moderators of a server can categorize users of the server into hierarchical groups with customized names

and can configure those groups to give users different levels of access to parts of the server.

9. The OCE's review of the Camgirls page revealed that the vast majority of its content consisted of: discussions about using web cameras and social-media applications to obtain sexually-explicit images and videos of minor children; images and videos of minor children exposing their vaginas, which at times were uploaded to the Camgirls page; and links to download child pornography images and videos from external file-storage sites. Most of the children viewed by the OCE appeared to be approximately between the ages of 11 and 17 years old. The Camgirls page also included some discussion of adults engaging in sexual activity via web camera. However, the majority of the activity focused on the depiction of minors engaged in sexually explicit activity on web cameras. For example, in the course of a discussion in the #help_requests text channel of Camgirls regarding the merits of utilizing virtual private network (VPN) technology to mask users' IP address² and identity, user "Lightzmare" commented on April 15, 2017: "Just the fact that we're all hanging in here, which is a chatroom where underaged sexual content is shared around is enough reason for one to get a VPN." Lightzmare continued, stating: "Fuck when you

² "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.

download something from dropfile Your ISP can see what you downloaded What if govt authorities read ISPs logfiles.”

10. Based on the OCE’s undercover observations on Camgirls, a federal search warrant was issued, on or about July 10, 2017, by the Honorable David R. Strawbridge, United States Magistrate Judge, Eastern District of Pennsylvania, for content stored on Discord’s servers related to Camgirls. In response to the search warrant, Discord disclosed to law enforcement officers IP address information for some users of Camgirls, the content of some text chats on Camgirls, and some private messages sent by users of Camgirls.

11. The Camgirls server was ultimately shut down by Discord. Members of the Camgirls server proceeded to open additional “servers” on the Discord website, including: Shaq Tribute, AppleFanBoys, ZeldaFanClub, and Thot Counselors. The OCE gained access to AppleFanBoys, ZeldaFanClub, Jizzbomb’s Bitches and Thot Counselors. The OCE observed each of these servers contained many of the same users as Camgirls and were operated for the purpose of discussing, obtaining, and distributing child exploitation material including child pornography files. The Thot Counselors server is the only Discord server that is still in operation.

II. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

12. The OCE observed a user of “Thot Counselors” using the online name “The Goat#7626” when using Discord. A review of the search warrant return from Discord and undercover recordings by the OCE located the following activity:

a. On January 18, 2018, The Goat#7626 posted the link <https://gyazo.com/43d99ff593682fa331db9910f0978cd0> on the Thot Counselors server. The OCE used the link to download an image file that depicted two prepubescent minor female children. One of the minor children removed her shirt and underwear and stood naked with her front facing the camera. The other minor child was in the process of removing her pants and underwear.

b. On January 19, 2018, The Goat#7626 posted the <https://ibb.co/d15qtb> on the Thot Counselors server. The OCE used the link to download an image file that depicted a film strip of a minor child removing her pants and underwear to expose her vagina and digitally penetrate herself.

13. On June 22, 2018, a Grand Jury Subpoena was issued for the user account TheGoat#7626, Discord ID 398315515396882432. Upon reviewing the results of this subpoena, it was noted that between June 25 and July 11, 2018, this account was accessed almost exclusively from either an IP address administered by T-Mobile, or IP address 73.75.185.102, which is administered by Comcast Communications. Because T-Mobile multiply assigned its IP addresses to customers, no information can be provided about a specific customer assigned a specific T-Mobile at any given specific date and time.

14. After an additional search warrant for the contents of the Discord page was executed, the results were reviewed, and undercover recordings by the OCE located the following activity:

a. On June 30, 2018, at 10:36 p.m. EDT, from IP address 73.75.185.102, The Goat#7626 posted “It’s crazy how after u get done fapping and as soon as u bust ur nut u just start thinking about life and shit...’why am I fapping to lolis’... why tf do I go so much cp.” Based on my training and experience, I understand “fapping” to mean masturbation, “lolis” to be a reference to underage minor females, and “cp” to be short for child pornography. On this same date, The Goat#7626 posted another hyperlink to mega.nz for a file titled “11yo lockie and 16yo girl suck and kiss (SC 2014).mkv.” The OCE downloaded and viewed this video, which depicted a female who appeared to be between the ages of 16 and 18 performing oral sex on a prepubescent male.

b. On July 8, 2018, at 5:29 a.m. EDT, from IP address 73.75.185.102, The Goat#7626 posted a hyperlink to mega.nz for a file titled “yolo-14760378407674400230—20161010023102.mpg.” The OCE downloaded and viewed this video, which depicted a minor female who appeared to be between the ages of 12 and 14 years old; the minor females exposed her vagina and anus to the camera.

c. On July 9, 2018, at 6:12 p.m. EDT, from IP 73.75.185.102, The Goat#7626 posted a hyperlink to mega.nz for a file titled “Meanwhile up stairs-LIVE-

165809-MERGED.mp4.” The OCE downloaded and viewed this video, which depicted a minor female who appeared to be under the age of 13 with no breast development; the camera focuses on the female’s genital area while the female masturbates underneath her underwear.

d. On July 11, 2018, at 1:40 p.m. EDT, from IP 73.75.185.102, The Goat#7626 posted an image that depicted what appeared to be a pubescent female exposing her vagina; the female has public hair but appears to be a minor.

15. An administrative subpoena was issued to Comcast for IP address 73.75.185.102 at the dates and times listed above, and Comcast identified the assigned customer at all requested dates and times as Individual A, 6122 S. Marshfield, Apt. 2, Chicago, Illinois.

16. On 7/10/2018, a mail check was conducted with the U.S. Postal Service, and they confirmed that the following individuals receive mail at this address: Individual A, Individual B, and Individual C. Using surveillance and mail checks, there appears to only be two units, one per floor, in the residence.

III. BACKGROUND INFORMATION CONCERNING CHILD PORNOGRAPHY

17. Based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers affect

the methods used by people who possess, receive, distribute, and transport child pornography in these ways:

18. Those who create child pornography can produce both still and moving images directly from a common video or digital camera, and other devices that create video and still images, including most cellular telephones and Personal Digital Assistants (“PDA”) (*e.g.*, a Blackberry). Images from such devices can be transferred to a computer by attaching the device to the computer using a cable, or by uploading images from the device’s memory card directly onto the computer or into a storage account accessible from any computer with the capability of accessing the internet (sometimes referred to as a “cloud” account). Once on the computer, images can then be stored, manipulated, transferred, or printed. This includes transfer to some of the same types of devices that are commonly used to create child pornography, such as cellular telephones and PDAs, as well as other computers. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography.

19. The Internet allows any computer to connect to another computer. Electronic contact can be made to millions of computers around the world. The Internet allows users, while still maintaining anonymity, to locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government

agencies, to communicate with each other and to distribute child pornography. They can also distribute and collect child pornography with peer-to-peer (“P2P”) file sharing, which uses software to link computers together through the Internet to form a network that allows for the sharing of digital files among users on the network. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet.

20. The computer’s capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise, optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media, such as floppy disks, also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child pornography search warrants often find electronic, optical, and/or electromagnetic

storage media containing child pornography in the same location as or near the computer that was used to obtain, access, and/or store child pornography.

21. My training and experience, and the training and experience of other agents whom I have consulted, have shown the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or other images, as well as literature describing sexually explicit activity involving children. Such individuals frequently store their child pornography on multiple electronic, optical, and/or electromagnetic storage media, including not only their computer, but also on external hard drives, floppy disks, CD-ROMs, DVDs, memory sticks, thumb drives, cell phones, PDAs, and other such media. Many of these individuals also collect child erotica, which consist of items that may not rise to the level of child pornography but which nonetheless serve a sexual purpose involving children.

b. Individuals who possess, transport, receive, and/or distribute 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. 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, Internet Relay Chat, newsgroups, instant messaging, and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute 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 address books or notebooks, on computer storage devices, or merely on scraps of paper.

d. The majority of individuals who possess, transport, receive, and/or distribute 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. These individuals almost always maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including filing cabinets, safes, or lockboxes. These individuals may also maintain their collections in password-protected or encrypted electronic media. They may keep these passwords, and other information concerning their use of the computer, on handwritten or printed notes that they store in personal areas and around the computer.

e. Possessors, traders and distributors of child pornography sometimes store their illegal images and videos online in remote storage accounts. Therefore, any records, documents, invoices and materials in any format or medium that concern online storage or other remote computer storage could indicate that a person at the Subject Premises is storing illegal material in an online storage account.

f. Files, logs, and records relating to P2P files can contain the names of files sent through the P2P service, as well as the date and time the files were transferred. These records could help identify the individual who transferred the child pornography images at the **Subject Premises**. Additionally, these records can provide historical information about the trading of child pornography by individuals at the Subject Premises.

IV. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

22. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) 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:

23. Electronic storage media 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 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.

24. Searching electronic storage media 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 an electronic storage media 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 electronic storage media 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.

25. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. 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. 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 disk drives or on external media).

26. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and are subject to seizure as such if they contain contraband or were used to obtain or store images of child pornography.

V. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

27. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

28. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

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

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 in Attachment B (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 file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;


d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

29. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

VI. CONCLUSION

30. Based on the above information, I respectfully submit that there is probable cause to believe that possession, receipt, and distribution of child pornography offenses, in violation of Title 18, United States Code, Sections 2252 and 2252A, have been committed, and that evidence, instrumentalities, fruits, and contraband relating to this criminal conduct, as further described in Attachment B, will be found in the Subject Premises, as further described in Attachment A. I therefore respectfully request that this Court issue a search warrant for apartment 2 of the subdivided two-story single family home located at 6122 South Marshfield, Chicago, Illinois, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.



Kimberly Castro
Special Agent
Federal Bureau of Investigation

Subscribed and sworn
before me this 12th day of October, 2018



Honorable JEFFREY T. GILBERT
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

6122 S. Marshfield Ave., Apt. 2, Chicago, IL 60636

The premises to be searched (the "SUBJECT PREMISES") is 6122 S. Marshfield Ave., Apt. 2, Chicago, Illinois. The SUBJECT PREMISES is a subdivided, two-story single family home. The premises to be searched includes any electronic device or digital storage medium located within the SUBJECT PREMISES, which may be fully searched pursuant to this warrant for the items enumerated in Attachment B.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence, instrumentalities, fruits and contraband concerning violation of Title 18, United States Code, Sections 2252 and 2252A, as follows:

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, on whatever medium (e.g. digital media, optical media, books, magazines, photographs, negatives, videotapes, CDs, DVDs, etc.), including those in opened or unopened e-mails. These include both originals and copies, and authorization is granted to remove videotapes without viewing them at the time and place of seizure, and to view them at a later time.

2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened e-mails, text messages, chat logs, and Internet history, pertaining to the possession, receipt, access to, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed.

3. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or efforts to meet a minor.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

7. Documents and records regarding the ownership and/or possession of the searched premises.

8. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

9. All evidence pertaining objects present in the background of the produced child pornography images and videos including bedding, clothing, framed photographs, rugs, carpeting, and decorations.

10. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

11. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any of the items described in paragraph 1-3 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.

12. The following may be seized and searched for all items listed above, and for any items specifically noted in the paragraphs below:

a. Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware are any electronic devices capable of data processing (such as central processing units, laptop or notebook or netbook or tablet computers, personal digital assistants, gaming consoles, and wireless communication devices to include cellular telephone devices capable of Internet access); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for

removable media); related communications devices (such as modems, wireless routers, cables and connections, web cameras, microphones); storage media, defined below; and security devices, also defined below.

b. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

c. Computer related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

d. Data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

e. All storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment, such as fixed hard disks, external hard disks, removable hard disks (including micro drives), floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, thumb drives, ipods, digital cameras, memory cards (e.g. CF or SD cards), Xboxes, flash drives, or other memory storage devices. This also includes areas with digital storage capability on devices such as printers, scanners, wireless routers, etc.

13. The above seizure of computer and computer related hardware relates to such computer-related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting. Upon a determination that such examination would be more appropriately made in a controlled environment, this storage media may be removed and examined at a laboratory location.

ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- 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 in Attachment B (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 file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

Case Number:

18M633

Apartment 2 of the subdivided two-story single family home located at 6122 South Marshfield, Chicago, Illinois, further described in Attachment A

SEARCH AND SEIZURE WARRANT

To: Kimberly Castro and 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 Northern District of Illinois:

See Attachment A

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:

See Attachment B

YOU ARE HEREBY COMMANDED to execute this warrant on or before October 26, 2018 in the daytime (6:00 a.m. to 10:00 p.m.).

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 the issuing United States Magistrate Judge.

Date and time issued: October 12, 2018

1:16 p.m.



Judge's signature

City and State: Chicago, Illinois

JEFFREY T. GILBERT, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

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 declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

6122 S. Marshfield Ave., Apt. 2, Chicago, IL 60636

The premises to be searched (the "SUBJECT PREMISES") is 6122 S. Marshfield Ave., Apt. 2, Chicago, Illinois. The SUBJECT PREMISES is a subdivided, two-story single family home. The premises to be searched includes any electronic device or digital storage medium located within the SUBJECT PREMISES, which may be fully searched pursuant to this warrant for the items enumerated in Attachment B.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence, instrumentalities, fruits and contraband concerning violation of Title 18, United States Code, Sections 2252 and 2252A, as follows:

1. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, on whatever medium (e.g. digital media, optical media, books, magazines, photographs, negatives, videotapes, CDs, DVDs, etc.), including those in opened or unopened e-mails. These include both originals and copies, and authorization is granted to remove videotapes without viewing them at the time and place of seizure, and to view them at a later time.

2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, photographs, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened e-mails, text messages, chat logs, and Internet history, pertaining to the possession, receipt, access to, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing possession of any child pornography possessed.

3. All communications and files with or about potential minors involving sexual topics or in an effort to seduce the minor or efforts to meet a minor.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission in or affecting interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

6. All records which evidence operation or ownership or use of computer or electronic equipment or devices, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the computer or device.

7. Documents and records regarding the ownership and/or possession of the searched premises.

8. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

9. All evidence pertaining objects present in the background of the produced child pornography images and videos including bedding, clothing, framed photographs, rugs, carpeting, and decorations.

10. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

11. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any of the items described in paragraph 1-3 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.

12. The following may be seized and searched for all items listed above, and for any items specifically noted in the paragraphs below:

a. Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware are any electronic devices capable of data processing (such as central processing units, laptop or notebook or netbook or tablet computers, personal digital assistants, gaming consoles, and wireless communication devices to include cellular telephone devices capable of Internet access); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for

removable media); related communications devices (such as modems, wireless routers, cables and connections, web cameras, microphones); storage media, defined below; and security devices, also defined below.

b. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

c. Computer related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

d. Data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

e. All storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment, such as fixed hard disks, external hard disks, removable hard disks (including micro drives), floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, thumb drives, ipods, digital cameras, memory cards (e.g. CF or SD cards), Xboxes, flash drives, or other memory storage devices. This also includes areas with digital storage capability on devices such as printers, scanners, wireless routers, etc.

13. The above seizure of computer and computer related hardware relates to such computer-related items as being the instrumentalities of crime and also to allow for analysis/search for evidence of crime in an appropriate forensic setting. Upon a determination that such examination would be more appropriately made in a controlled environment, this storage media may be removed and examined at a laboratory location.

ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- 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 in Attachment B (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 file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.