

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

2015 SEP 24 AM 9:52

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Apple iPod, Model A1421, bearing serial number
CCQMXDVKG22T, blue and white in color

Case No.

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-2

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

See Attachment B-2

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

See Attachment C-2

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ 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.

Andrea R. Kinzig

Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

9-24-15

City and state: Dayton, Ohio

Sharon L. Ovington

Judge's signature

Sharon L. Ovington, Chief U.S. Magistrate Judge

Printed name and title

ATTACHMENT A-2

The property to be searched is an Apple iPod, Model A1421, bearing serial number CCQMXDVKG22T, blue and white in color ("Device-2"). The Device-2 is currently located at the Federal Bureau of Investigation, 7747 Clys Road, Centerville, Ohio, 45459.

This warrant authorizes the forensic examination of Device-2 for the purpose of identifying the electronically stored information described in Attachment B-2.

ATTACHMENT B-2

1. All records on Device-2 described in Attachment A-2 that relate to violations of involving: (1) possession of child pornography and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) and 2252(a)(4)(B); (2) receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) and 2252(a)(2)(B); (3) production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e); and (4) coercion and enticement, in violation of 18 U.S.C. §2422, involving Robert Jones from August 1, 2013 to the present, including:

- a. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;
- b. Any visual depictions of minors;
- c. Any Internet history indicative of searching for child pornography;
- d. Any Internet or cellular telephone communications (including email, social media, and online chat programs) with others in which child exploitation materials and offenses are discussed and/or traded, and any contact / identifying information for these individuals;
- e. Any Internet or cellular telephone communications (including email, social media, and online chat programs) with minors, and any contact / identifying information for these minors;
- f. Evidence of utilization of email accounts, social media accounts, online chat programs, and Peer-to-Peer file sharing programs, including any account / user names;
- g. Evidence of utilization of aliases and fictitious names;
- h. Any information related to Internet Protocol (IP) addresses accessed by Device-2;
- i. Any GPS information on Device-2;

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

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT C-2

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B)	Possession of Child Pornography and Access with Intent to View Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(2)	Possession of Child Pornography and Access with Intent to View Child Pornography
18 U.S.C. §2252(a)(2)(B)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2)(A) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2251(a) and (e)	Production of Child Pornography
18 U.S.C. §2422	Coercion and Enticement

3:15mj-385

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including computer media.
2. Along with other agents and task force officers of the Federal Bureau of Investigation, I am currently involved in an investigation of child pornography and coercion and enticement offenses committed by ROBERT STEVEN JONES (hereinafter referred to as "JONES"). This Affidavit is submitted in support of Applications for search warrants for the following:
 - a. Apple iPhone, Model A1533, bearing FCCID BCG-E2642A and IMEI 013888008166962, gold and white in color, currently located at the Federal Bureau of Investigation, 7747 Clys Road, Centerville, Ohio, 45459 (hereinafter referred to as "**DEVICE-1**", and as more fully described in Attachment A-1);
 - b. Apple iPod, Model A1421, bearing serial number CCQMXDVKG22T, blue and white in color, currently located at the Federal Bureau of Investigation, 7747 Clys Road, Centerville, Ohio, 45459 (hereinafter referred to as "**DEVICE-2**", and as more fully described in Attachment A-2);
3. The above noted devices are more fully described in Attachments A-1 and A-2. The purpose of these Applications is to seize evidence of the following violations: (1) possession of child pornography and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) and 2252(a)(4)(B); (2) receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) and 2252(a)(2)(B); (3) production of child pornography, in violation of 18 U.S.C. § 2251(a) and (e); and (4) coercion and enticement, in violation of 18 U.S.C. § 2422. The items to be searched for and seized are described more particularly in Attachments B-1 and B-2 hereto.
4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other officers involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted devices (as described in Attachments A-1 and A-2).
6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§2252, 2252A, and 2422, are present within the information associated with the above noted devices (as described in Attachments A-1 and A-2).

JURISDICTION

7. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

8. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.
9. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;
10. 18 U.S.C. § 2252(a)(2)(B) prohibits a person from knowingly receiving or distributing any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, 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 from knowingly reproducing 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 mail if the producing of such

visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

11. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
12. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters 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 producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
13. 18 U.S.C. § 2422(b) states that is a violation for any person to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so. 18 U.S.C. §2427 states that the term “sexual activity for which any person can be charged with a criminal offense” includes the production of child pornography.
14. For purposes of these statutes, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2) as:
 - a. “Actual or simulated –
 - i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
 - ii. Bestiality;
 - iii. Masturbation;
 - iv. Sadistic or masochistic abuse; or
 - v. Lascivious exhibition of genitals or pubic area of any person.”

BACKGROUND INFORMATION

Definitions

15. The following definitions apply to this Affidavit and attachments hereto:

- a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.
- b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- c. "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, legally obscene or that do not necessarily depict minors in sexually explicit conduct.
- d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- 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 Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

- g. "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).
- h. "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.
- i. "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.
- j. "Computer passwords, pass-phrases 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 or pass-phrase (a string of alphanumeric characters) usually operates as 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 progress to restore it.
- k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
- l. "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;
- m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.
- n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other

communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- p. "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 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. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- q. Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.
- r. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- s. 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, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- t. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

- u. “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 person. See 18 U.S.C. § 2256(2).
- v. “URL” is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.
- w. “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).
- x. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”);

Characteristics of Child Pornographers

16. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors 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. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
 - d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (*e.g.*, mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large

percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors 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.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives, including ICE's "Operation Emissary" and the FBI's "Ranchi message board" investigation. For example, in the "Ranchi" investigation a national take-down occurred during the week of March 1, 2007. Approximately 83 subjects were contacted, 28 by court-authorized search warrants and 55 by "knock and talks." Of the 83 contacts, 46 individuals (or 55%) confessed to accessing the Ranchi message board and/or downloading child pornography from Ranchi. Multiple other new cases were opened without confessions based on strong evidence obtained during the Ranchi search warrants and knock-and-talks.

Apple Services and iPhones

- 17. Apple designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV, a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and Mac App Store.
- 18. The following represents a summary of some of the applications offered by Apple:
 - a. **iTunes** is a free software application which customers use to organize and play digital music and video on their computers. It's also a store that provides content for customers to download for their computers and iOS devices. The iTunes Store is also available on the iPhone, iPad, and iPod Touch. Through the iTunes Store, users can purchase and download music, music videos, television shows, audiobooks, podcasts,

movies, and movie rentals in some countries, and ringtones, available on the iPhone and iPod Touch (fourth generation onward). Application software for the iPhone, iPad and iPod Touch can be downloaded from the App Store.

- b. **FaceTime** is a videotelephony product. The video version of FaceTime supports any iOS device with a forward-facing camera and any Macintosh computer equipped with a FaceTime Camera, formerly known as an iSight Camera. FaceTime Audio is available on any iOS device that supports iOS 7 or newer, and any Macintosh with a forward-facing camera running Mac OS X 10.9.2 and later.
- c. **iCloud** is a cloud storage and cloud computing service from Apple Inc. launched on October 12, 2011. The service provides its users with means to store data such as documents, photos, and music on remote servers for download to iOS, Macintosh or Windows devices; to share and send data to other users; and to manage their Apple devices if lost or stolen. The service also provides the means to wirelessly back up iOS devices directly to iCloud, instead of being reliant on manual backups. Service users are also able to share photos, music, and games instantly by linking accounts via AirDrop wireless. It replaced Apple's MobileMe service, acting as a data syncing center for email, contacts, calendars, bookmarks, notes, reminders (to-do lists), iWork documents, photos and other data.
- d. **Game Center** is an online multiplayer social gaming network released by Apple. It allows users to invite friends to play a game, start a multiplayer game through matchmaking, track their achievements, and compare their high scores on a leader board.

19. According to Apple's Law Enforcement Guide, as published on its website, information maintained by Apple on its servers related to its products and applications includes the following:

- a. Device Registration: Basic registration or customer information, including, name, address, email address, and telephone number, is provided to Apple by customers when registering an Apple device prior to iOS 8 and OS Yosemite 10.10. Apple does not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running OS Yosemite 10.10 and later versions, is received when a customer associates a device to an iCloud Apple ID.
- b. Customer Service Records: Contacts that customers have had with Apple's customer service regarding a device or service may be obtained from Apple. This information may include records of support interactions with customers regarding a particular Apple device or service. Additionally, information regarding the device, warranty, and repair may also be available.
- c. iTunes: When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided. Additionally, information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections may also be available.

- d. iCloud: All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers. The following information may be available from iCloud:
 - i. Subscriber Information: When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. Connection logs are retained up to 30 days.
 - ii. Mail Logs: Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. iCloud mail logs are retained up to 60 days.
 - iii. Email Content: iCloud only stores the emails a subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. Apple is unable to provide deleted content.
 - iv. Other iCloud Content: Photo Stream, Docs, Contacts, Calendars, Bookmarks, and iOS Device Backups: iCloud only stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include stored photos, documents, contacts, calendars, bookmarks and iOS device backups. iOS device backups may include photos and videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. iCloud content may be provided in response to a search warrant issued upon a showing of probable cause.
- e. Game Center: Information regarding Game Center connections for a user or a device may be available. Connection logs with IP addresses, transactional records, and specific game(s) played may also be available.
- f. iOS Device Activation: When a customer activates an iOS device or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available.
- g. Apple Online Store Purchases: Apple maintains information regarding online purchases including name, shipping address, telephone number, email address, product purchased, purchase amount, and IP address of the purchase.
- h. Find My iPhone: Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch or Mac and/or take certain actions, including putting the device in lost mode, locking or wiping the device. Find My iPhone connection logs are available for a period of approximately 30 days. Find My iPhone transactional activity for requests to remotely lock or erase a device may be available

- i. Sign-on Activity: Sign-on activity for a user or a device to Apple services such as iTunes, iCloud, My Apple ID, and Apple Discussions, when available, may be obtained from Apple.
- j. My Apple ID: My Apple ID and iForgot logs for a user may be obtained from Apple. My Apple ID and iForgot logs may include information regarding password reset actions.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

20. Robert Jones, who currently resides at 307 South Second Street in Anna, Ohio, has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as "Website A."¹

The Network²

21. "Website A" operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application.³ Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.
22. Websites that are accessible only to users within the Network can be set up within the Network and "Website A" was one such website. Accordingly, "Website A" could not generally be accessed through the traditional Internet.⁴ Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to the Network, however, a user had to know the exact web address of

¹ The actual name of "Website A" is known to law enforcement. Disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as "Website A."

² The actual name of the Network is known to law enforcement. The network remains active and disclosure of the name of the network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

³ Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

⁴ Due to a misconfiguration, prior to February 20, 2015, Website A was occasionally accessible through the traditional Internet. In order to access Website A in that manner, however, a user would have had to know the exact IP address of the computer server that hosted Website A, which information was not publicly available. As of on or about February 20, 2015, Website A was no longer accessible through the traditional Internet.

“Website A” in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of “Website A,” obtain the web address for “Website A,” and click on a link to navigate to “Website A.” Rather, a user had to have obtained the web address for “Website A” directly from another source, such as other users of “Website A,” or from online postings describing both the sort of content available on “Website A” and its location. Accessing “Website A” therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon “Website A” without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

23. The Network’s software protects users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address which could otherwise be used to identify a user.
24. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

Description of “Website A” and its Content

25. “Website A” was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting “Website A” was seized from a web-hosting facility in Lenoir, North Carolina. The website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time “Website A” ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of “Website A.” Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of “Website A,” which are described below.
26. According to statistics posted on the site, “Website A” contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either

side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that: "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A;" and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with '[Website A].'" Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

27. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.
28. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.
29. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, I know that "jailbait" refers to underage but post-pubescent minors; the abbreviation "HC" means hardcore (i.e., depictions of penetrative sexually explicit conduct); and "scat" refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.
30. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The "last post" section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred

- to as ".rar" files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.
31. A review of the various topics within the "[Website A] information and rules," "How to," "General Discussion," and "Security & Technology discussion" forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.
 32. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:
 - a. On February 3, 2015, a user posted a topic entitled "Buratino-06" in the forum "Pre-teen – Videos - Girls HC" that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;
 - b. On January 30, 2015, a user posted a topic entitled "Sammy" in the forum "Pre-teen – Photos – Girls" that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and
 - c. On September 16, 2014, a user posted a topic entitled "9yo Niece - Horse.mpg" in the "Pre-teen Videos - Girls HC" forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.
 33. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, "Website A" contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.
 34. "Website A" also included a feature referred to as "[Website A] Image Hosting." This feature of "Website A" allowed users of "Website A" to upload links to images of child pornography that are accessible to all registered users of "Website A." On February 12, 2015, an FBI Agent accessed a post on "Website A" titled "Giselita" which was created by a particular "Website A" user. The post contained links to images stored on "[Website A] Image Hosting." The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.
 35. Text sections of "Website A" provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse. The following provides an example of one of these forums:

- a. On January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum "Stories - Non-Fiction" that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote "...it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms..." The user ended his post with the question, "should I try to proceed?" and further stated that the girl "seemed really interested and was smiling a lot when she felt my cock." A different user replied to the post and stated, "...let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful..."

Court Authorized Use of Network Investigative Technique

36. Websites generally have Internet Protocol ("IP") address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of "Website A" to access the site. A publicly available lookup could then be performed to determine what Internet Service Provider ("ISP") owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.
37. However, because of the Network software utilized by "Website A," any such logs of user activity would contain only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of "Website A."
38. Accordingly, on February 20, 2015, the same date "Website A" was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to allow law enforcement agents to deploy a Network Investigative Technique ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other identifying information of computers used to access "Website A." Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into "Website A" by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing "Website A." That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been

delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

User "billypedo" on "Website A"

39. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, a user with the user name "billypedo" engaged in activity on "Website A", as detailed below.
40. The profile page of the user "billypedo" indicated that this user originally registered an account on "Website A" on or around February 11, 2015. Profile information on "Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the user profile for "billypedo", this user had a group membership title of "Newbie" on "Website A". Further, according to the Statistics section of this user's profile, the user "billypedo" had been actively logged into the website for a total of approximately one hour and thirty-four minutes between the approximate dates of February 11, 2015 and March 2, 2015.

IP Address and Identification of User "billypedo" on "Website A"

41. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on February 26, 2015, the user "billypedo" engaged in the following activity on "Website A" from the IP address 71.67.116.75. During the session described below, this user browsed "Website A" after logging into the site with a username and password.
 - a. On February 26, 2015, the user "billypedo", using the IP address 71.67.116.75, accessed a post entitled "Really Hot Vines - Thread" on the forum "Pre-teen Videos/Girls HC". This post contained various hyperlinks to files and two image files. The two image files are described as follows:
 - i. One of the image files contained a "contact sheet" (a sheet containing a series of images, which often represent a series of still images from a video file) with the following file name noted at the top of the sheet: "luvsex.avi". The contact sheet contained sixteen images that primarily depict a pre-pubescent white female child. Some of the images display close-up images of the child's nude vagina and/or anus. In one of the images, an object is inserted into the child's vagina or anus. In another image, the child is depicted urinating. Based on my training and experience, I believe that at least seven of the images on the contact sheet depict child pornography (as defined by 18 U.S.C. § 2256).
 - ii. The second image file contained a contact sheet with the following file name noted at the top of the sheet: "ohmy.mkv". The contact sheet contained

twenty-five images that depict a pre-pubescent white female child who is nude from the waist down. All of the images display close-up images of the child's vagina. In approximately nineteen of the images, a yellow object is inserted into the child's vagina. In approximately six of the images, one or more fingers are inserted into the child's vagina or anus. Based on my training and experience, I believe that all of the images on the contact sheet depict child pornography (as defined by 18 U.S.C. § 2256).

42. The user "billypedo" also browsed "Website A" after logging into the site with a username and password on a number of occasions during the approximate time period of February 26, 2015 to March 2, 2015. During this time period, the user accessed approximately forty-three threads in total, each containing various posts. A number of the posts contained image files depicting child pornography (as defined by 18 U.S.C. § 2256). During the sessions, the user's IP address information was not collected. However, the account name "billypedo" is a uniquely assigned name specific to the registered user of the website. Examples of three of the threads that were accessed are as follows:
 - a. On or around February 26, 2015, the user "billypedo" accessed a thread entitled "Vnights (10yo girl fuck and cum)(v good – hot cum shot) little asgirl fucked" on the forum "Girls HC". The first post on the thread contained various hyperlinks to files, a file name, a password, and an image file. The image file contained a contact sheet with the following file name noted at the top of the sheet: "Vnights (10yo girl fuck and cum)(v good – hot cum shot).avi". The contact sheet contained sixteen images that depict a pre-pubescent Asian female child and an adult male, both of whom are completely nude. The images primarily display close-up images of the child's vagina and/or the adult male engaging in sexual intercourse with the child on a bed. Based on my training and experience, I believe that at least twelve of the images on the contact sheet depict child pornography (as defined by 18 U.S.C. § 2256). Another user responded to this post by stating, "Thanks antonSPA. It is great how these little asian girls get properly penetrated, very rare elsewhere!"
 - b. On or around March 2, 2015, the user "billypedo" accessed a thread entitled "Emy 12 Years Thai Prostitution In Thailand full sex" on the forum "Girls". The first post on the thread contained various hyperlinks to files and an image file. The image file contained a contact sheet with the following file name noted at the top of the sheet: "(Emy 12 Years Thai Also R@Ygold Lolita ([][] [] [13[Child Prostitution in Thailand – Japanese Guy Fucks a Poor Little Girl.mpg". The contact sheet contained thirty-five images that depict an Asian female child. Some of the images display the child taking off her clothing, and other images display close-up images of her nude vagina. Some of the images depict an adult white male engaging in sexual intercourse with the child and the child being digitally penetrated. Based on my training and experience, I believe that at least twenty-seven of the images on the contact sheet depict child pornography (as defined by 18 U.S.C. § 2256).
 - c. On or around March 2, 2015, the user "billypedo" accessed a thread entitled "'Senorita' Mexican girl age 4/5/6 trying to befucked by Dad." in the forum "Girls

HC". The first post on the thread contained a hyperlink to a file, a password, and the following text: "Little Mexican girl age 4-6 years, her Dad is trying to fuck her, but he has a big floppy cock!!!! Sorry, no preview as I could not get this vid to register on the preview thing. Worth the DL just to see a girl of this age being sort of fucked. 12.4mb about 1 minute long." Another user responded to this post by posting an image file and the following text: "Here's a preview." The image file contained a contact sheet with the following file name noted at the top of the contact sheet: "senorita.wmv". The contact sheet contained twenty images, nineteen of which depict a pre-pubescent white female child and an adult white male. The child is wearing a purple shirt but is nude from the waist down, and the adult male appears to be completely nude. The images primarily display the adult male engaging in sexual intercourse with the child on a bed with a blue cover. Based on my training and experience, I believe that at least eighteen of the images on the contact sheet depict child pornography (as defined by 18 U.S.C. § 2256).

43. Among the information collected by the NIT when it was deployed against "billypedo" was the hostname and logon name for the computer utilized by the user. This information identified that the hostname for the computer was "Dulaney-HP" and the logon name was "Dulaney".
44. Using publicly available websites, FBI Special Agents were able to determine that the above noted IP Address (71.67.116.75) was operated by the Internet Service Provider ("ISP") Time Warner Cable. In March 2015, an administrative subpoena/summons was served to Time Warner Cable requesting information related to the user of this IP address on the date and approximate time it was used to access "Website A" (as collected by the NIT). According to information received from Time Warner Cable in response to the subpoena, the IP address was subscribed to JONES at 2368 Collins Drive, Sidney, Ohio, 45365. Records indicated that the account was activated on or around July 13, 2014, and that the service was active as of March 3, 2015.
45. A search of the Accurint information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) was conducted for Robert Jones. These public records indicated that JONES previously resided at 2368 Collins Drive, Sidney, Ohio, 45365.
46. Records from the Shelby County (Ohio) Sheriff's Office identified that JONES was currently required to register as a sex offender based on a conviction in 2003 in Illinois. The records from the Sheriff's Office identified that during the approximate time period of August 12, 2014 to June 24, 2015, JONES completed paperwork identifying that he resided at 2368 Collins Drive, Sidney, Ohio, 45365. Heather Dulaney also completed paperwork in July 2014 stating that she was JONES' girlfriend and that they lived together. Heather Dulaney provided her cellular telephone number on this paperwork.
47. Records from the Shelby County Sheriff's Office identified that JONES completed paperwork on or around June 24, 2015, identifying that he had moved to 3025 Seminole Way, Piqua, Ohio, 45356 (located in Miami County, Ohio). Records from the Miami County Sheriff's Office identified that JONES completed paperwork on or around July 31, 2015, identifying that he had moved to 307 South Second Street in Anna, Ohio. He

identified on both sets of paperwork that he could be contacted at his girlfriend's cellular telephone number. This telephone number matched the number that was provided by Heather Dulaney in July 2014.

Search Warrant and Interview of Robert Jones

48. Based on the results of the investigation of the "billypedo" user, a federal search warrant was authorized by the United States District Court for the Southern District of Ohio for the residence at 307 South Second Street in Anna, Ohio. Agents and officers of the FBI and Anna Police Department executed the warrant on August 21, 2015. JONES and two juvenile children were present when agents and officers arrived. Among other items, the following were seized pursuant to the warrant from the Master Bedroom:
- a. Dell Inspiron 11 laptop
 - b. ZTE cellular telephone, Model ZTE-N9100
 - c. All-In-One HP computer, Model 310-1020
 - d. iPhone, Model A1549, FCCID BCG-E28164, IMEI 358372062039301
 - e. SanDisk Cruzer Glide 32 GB thumb drive
49. During the search, JONES agreed to be interviewed after being advised of his Miranda rights. In summary, JONES provided the following information:
- a. Since approximately July 27, 2015, JONES resided at 307 South Second Street along with his fiancé, Heather Dulaney; Heather Dulaney's juvenile daughter; and JONES' and Heather Dulaney's infant son. JONES and Heather Dulaney shared the Master Bedroom.
 - b. Prior to living at 307 South Second Street, JONES and Heather Dulaney lived at 3025 Seminole Way in Piqua, Ohio for a period of approximately one and a half months. Prior to living at the house in Piqua, JONES and Heather Dulaney lived at 2368 Collins Drive in Sidney, Ohio for a period of approximately one year. JONES stated that his friend, John Leonard, lived with JONES and Heather Dulaney at the houses in Sidney and Piqua, from approximately May 2015 to June 2015.
 - c. Prior to meeting and living with Heather Dulaney, JONES resided in Illinois.
 - d. JONES identified that there was a Dell laptop and HP Touchscreen computer in the residence. The Dell laptop was JONES' laptop, which he obtained approximately one year and three months ago. The HP Touchscreen computer previously belonged to Heather Dulaney's mother, and the mother gave it to Heather Dulaney approximately one year and three months ago. JONES and Heather Dulaney shared this computer. JONES previously had another laptop, but he disposed of it a few months ago.
 - e. JONES identified that the iPhone was his telephone. When asked for the telephone number to this device, JONES stated that he could not recall the number. Agents noted that the device was locked and required JONES' fingerprint and/or a numerical passcode to access it. Agents asked JONES on a number of occasions to provide his fingerprint or the numerical password, but JONES refused.

- f. JONES and Heather Dulaney received wireless Internet service through an account with Time Warner Cable. A password was currently required to access the wireless account, and only JONES and Heather Dulaney knew the password. A password was not required to access the Internet account that he and HEATHER DULANEY had at their residence in Piqua. JONES could not recall if a password was required to access the Internet account at the house in Sidney.
- g. JONES stated that he viewed adult pornography on a regular basis, but he denied viewing child pornography. He acknowledged that there were some occasions that he saw child pornography on a website located at www.4chan.com, but he denied that he ever accessed or saved the files.
- h. JONES denied any knowledge of or use of the nickname "billypedo".
- i. During the previous year, while JONES was living with Heather Dulaney, he met a girl on an online dating application called Badoo⁵. JONES stated that this girl's profile identified that she was 20 years old, but he learned that she was 16 years old after they dated for a few weeks. JONES was arrested for a contributing to the delinquency of a minor charge after he and the girl were caught having sexual contact in Bellefontaine, Ohio.

50. During the execution of the search warrant, Heather Dulaney arrived at the residence. Heather Dulaney consented to be interviewed and provided the following information:

- a. Heather Dulaney confirmed that she was JONES' fiancé, and that they had resided at 307 South Second Street for approximately one month. She also confirmed that they previously resided at the houses in Piqua and Sidney. Heather Dulaney reported that John Leonard and his fiancé and juvenile daughter also lived at their houses in Sidney and Piqua for a period of one to two months.
- b. Similar to JONES, Heather Dulaney reported that there was a Dell laptop and an HP Touchscreen computer in the residence. Heather Dulaney was unaware that JONES previously had another laptop that he disposed of a few months ago.
- c. Also similar to JONES, Heather Dulaney reported that she and JONES had a wireless Internet account through Time Warner Cable. Heather Dulaney identified that a password was required to access the current Internet account at their residence in Anna. Heather Dulaney was responsible for setting up the Internet service at the house in Sidney, and she was confident that a password was required to access the account. John Leonard and his fiancé knew the password while they were living there, but Heather Dulaney otherwise had not shared the passwords with any other individuals.
- d. Heather Dulaney denied viewing adult or child pornography on any of the computers in the residence. Heather Dulaney was not aware of JONES viewing child pornography.

⁵ Badoo is a dating-focused social networking service founded in 2006 and headquartered in London. It allows users to chat with other users and upload photographs and videos.

51. As noted above, the NIT deployed during the investigation of "Website A" captured an IP address utilized by the "billypedo" user in February 2015, which was subscribed to JONES at 2368 Collins Drive in Sidney, Ohio. Based on the information provided by JONES and Heather Dulaney during the interviews (as detailed above), they lived at this residence alone with their children during this time period. Based on the information provided by Heather Dulaney, a password was required to access the Internet account at this residence.

Preliminary Review of Computer Media Seized from Search Warrant

52. A preliminary examination has been conducted of the SanDisk Cruzer Glide 32 GB thumb drive and the ZTE cellular telephone seized from JONES' and Heather Dulaney's residence. Below is a summary of the information found during the examination:

SanDisk Cruzer Glide 32 GB Thumb Drive:

- a. Over 2,600 images were recovered from the deleted space of the thumb drive that depicted pre-pubescent female children in various states of undress. Many of these images depicted the children engaged in sexual activities and/or displayed the children's genitalia. Based on my training and experience, I believe that more than 2,300 of the images depict child pornography (as defined by 18 U.S.C. § 2256). Two of the images are described as follows⁶:
- i. **431 04507168**: The image depicts a pre-pubescent white female child who is completely naked and lying on a bed. What appears to be an adult white male (whose face is not captured in the image) is standing over the child's head. The penis of the adult male is in the child's mouth. The following caption appears in the top left-hand corner of the image: "Tara 7yr #25 Daddy calls this a "face fuck"."
 - ii. **456 04519619**: The image depicts a pre-pubescent white female child who is completely naked and kneeling on a bed. An adult white male who is wearing a peach-colored shirt is standing behind the child. Black boxes are superimposed over the child's eyes and the adult male's face. The adult male is holding the child's hair with his left hand and inserting a knife into the child's buttocks with his right hand.
- b. Recovered from the active space of the thumb drive were various other documents, including a Word document entitled "9_Autobiography". The document contained three paragraphs, with the following first sentence: "My name is Robert Steven Jones, born William Robert Johnson in Amarillo, Texas."
- c. Also recovered from the active space of the thumb drive were four pictures of Arizona drivers' licenses. Two of the drivers' licenses contained JONES' name and

⁶ Because the files were recovered from deleted space, the noted file names are names generated by the system utilized to examine the computer media and are not the names generated by the user.

photograph on them. The other two drivers' licenses contained the name John Raymond Leonard Jr. but had different drivers' license numbers and dates of birth – one of which matched JONES' date of birth. Based on records from the Arizona Department of Transportation, the driver's license number from the license containing the name of John Raymond Leonard Jr. and the date of birth matching JONES' date of birth was assigned to another individual. I have viewed the driver's license of the other individual and noted that the name, identifying information, and photograph on this driver's license did not match the photograph contained on the thumb drive. As such, the license depicted in the photograph on the thumb drive appears to be a fraudulent driver's license.

- d. Based on the files recovered from the thumb drive and the other information noted in this Affidavit, I believe that JONES was the user of the device.

ZTE Cellular Telephone, Model ZTE-N9100:

- e. When the telephone was powered on, the following notification was displayed: "Too many pattern attempts. To unlock, sign in with your Google account." Given that the telephone is locked, a full examination of the telephone has not been conducted at this time. However, the telephone contained an SD card, and files stored or previously stored on the card were recovered.
- f. More than five videos depicting child pornography (as defined by 18 U.S.C. § 2256) were recovered from the SD card – at least three of which were recovered from the active space of the card. One of the videos is described as follows:
 - i. **Vicky3[1]**: The video depicts a pre-pubescent white female child and an adult white male (whose face is not captured in the video). At the beginning of the video, both the female child and the adult male are wearing white shirts but are naked from the waist down. The video begins by depicting the child performing oral sex on the adult male's penis. The video then depicts the child completely nude and sitting on the adult male's lap. The adult male spreads apart the child's legs to expose her vagina to the camera, and an object is inserted into the child's vagina. The video then depicts the adult male anally penetrating the child with his penis. The video is approximately five minutes and fifty-four seconds in duration. The video was saved along with other video files in a zip file entitled "1234_Attachments_2013122". File property information indicates that the video file was saved on the SD card on or around December 1, 2013, and that the zip file was saved on the SD card or around December 2, 2013.
- g. More than 250 images depicting child pornography (as defined by 18 U.S.C. § 2256) were recovered from the deleted space of the SD card. Many of these images contained a banner at the top stating "Freenet Community" along with partial file names and/or website addresses. As such, these images appeared to be obtained from the Freenet website. Based on my training and experience, I know that the Freenet

website is an anonymous Peer-to-Peer file sharing program that is commonly used to trade child pornography. One of the image files is described as follows⁷:

- i. **1086 003468168**: The image depicts a pre-pubescent Asian female child who is completely naked and lying on a bed. What appears to be an adult white male (whose face is not captured in the image) is kneeling over the child's head. The penis of the adult male is in the child's mouth. The adult male is also digitally penetrating the child's vagina. The following caption appears at the top of the image: "Freenet Community: cock in ...".
 - h. Also recovered from the active and deleted space of the SD card were more than 30 images of JONES; at least two pictures of envelopes containing return addresses with JONES' name and an address in Westville, Illinois; and various screen prints of text messages and/or messages from messenger applications. Many of the screen prints of messages contained what appeared to be sexually explicit conversations between a male and various females. Based on the profile pictures, some of the females appeared to possibly be teenagers.
 - i. Three documents were also recovered from the SD card containing maps for bus lines in Illinois and a listing of Illinois medical facilities. As noted above, JONES identified that he previously resided in Illinois.
 - j. Of the various files recovered from the active space of the SD card, file property information indicates that the files were saved on the SD card during the approximate time period of August 2013 to September 2014.
 - k. Based on the files recovered from the SD card and other information noted in this Affidavit, I believe that the telephone was previously utilized by JONES.
53. The All-in-One HP computer, Dell Inspiron 11 laptop, and iPhone have not been examined at this time.

Previous Arrest of JONES and Original Seizure of Device 1 and Device 2

54. As part of the investigation, I obtained police reports from the Bellefontaine (Ohio) Police Department and Logan County (Ohio) Sheriff's Office regarding the arrest that JONES discussed during the interview for contributing to the delinquency of a minor. Review of the reports provided the following information:
- a. On or around July 22, 2014, officers of the Bellefontaine Police Department responded to a report that two individuals were engaged in sexual activities in a vehicle parked near a residence. Officers located the vehicle and identified that it was occupied by JONES and a juvenile female who will be referred to for purposes of this Affidavit as Minor Female A. Minor Female A had turned 16 years old

⁷ Because the file was recovered from deleted space, the noted file name is a name generated by the system utilized to examine the computer media and are not the names generated by the user.

approximately one month prior to the incident. When officers made initial contact with the occupants of the vehicle, Minor Female A identified that she had engaged in sexual activities with JONES earlier that day as well as on previous occasions. JONES admitted that he had engaged in sexual activities with Minor Female A in the past but denied doing so earlier that day.

- b. JONES was arrested for contributing to the delinquency of a minor and was booked into the Logan County Jail. Seized from JONES' person pursuant to his arrest were **DEVICE-1** and three credit cards with other individuals' names on them. **DEVICE-2** was seized from Minor Female A. Both devices have been stored at the Bellefontaine Police Department since that time and have not been accessed.
- c. Minor Female A provided additional written and verbal statements to deputies of the Logan County Sheriff's Office. Minor Female A identified that she met JONES on the Badoo online social media site approximately three weeks prior to the incident. Minor Female A stated that she told JONES her true age, and they communicated via the Badoo site and the Kik⁹ messenger application. Minor Female A and JONES had consensual sexual intercourse at Minor Female A's house on four to five occasions.
- d. As part of the investigation, Heather Dulaney was contacted by deputies of the Logan County Sheriff's Office. Heather Dulaney reported that after learning of JONES' arrest, she accessed a laptop belonging to JONES. Heather Dulaney found approximately twenty photographs on JONES' iCloud account depicting checks, social security cards, and financial documents in the names of various individuals with whom she was not familiar.
- e. Deputies of the Logan County Sheriff's Office conducted an additional interview of JONES the day after his arrest. In summary, JONES provided the following information during this interview:
 - i. JONES previously lived in both Illinois and Indiana but had lived with Heather Dulaney at 2368 Collins Drive in Sidney, Ohio since June 2014.
 - ii. JONES met Minor Female A via the Badoo online social media site approximately one month ago. JONES had been to Minor Female A's home on four to five occasions, and they had sexual intercourse on approximately 12 occasions. JONES stated that he first thought that Minor Female A was 18 years old but later learned that she was 16 years old.
 - iii. When asked about the prepaid credit cards he had in his possession with others' names, JONES reported that he obtained the cards online. JONES stated that he utilized fictitious names on the cards because he had poor credit and knew that the credit card company would not provide him with the cards if he utilized his true name.
 - iv. When asked about what computers he had at his residence, JONES first stated that he had a laptop computer. He then stated that he did not have a laptop but rather had an All-in-One computer. JONES said that this computer

⁹ Kik Messenger is an instant messaging application for mobile devices. The application is available on most iOS, Android, and Windows Phone operating systems free of charge.

was Heather Dulaney's computer, but that he used it. When further questioned about the existence of a laptop, JONES acknowledged that he did have a laptop that he purchased, but that he gave it to Heather Dulaney.

- v. JONES currently had an iPhone and previously had an iPod. JONES stated that he utilized these devices to communicate with Minor Female A.
- vi. JONES was asked about the photographs that Heather Dulaney found on his iCloud account. JONES stated that he had disabled his iCloud account, that the pictures were not his, and that he had no knowledge of the pictures.

55. As part of the current investigation, I contacted Minor Female A in September 2015. Minor Female A identified that she was 15 years old when she first began communicating with JONES, but they did not meet or engage in sexual activities until she was 16 years old. Minor Female A used **DEVICE-2** to communicate with JONES. Minor Female A recalled that JONES had an iPhone, and this iPhone required his fingerprint to unlock it. Minor Female A advised that JONES utilized the iPhone to take approximately two to three pictures of her when he was at her house. Minor Female A was completely nude in the photographs but was not engaged in sexual activities. Based on my training and experience, I believe that these photographs likely contain child pornography (as defined by 18 U.S.C. § 2256) that JONES produced. Minor Female A further stated that JONES had the iPhone he used to take the nude pictures of her when he was arrested. I therefore believe that **DEVICE-1** contains child pornography.

Results of Administrative Subpoenas

56. Also as part of the investigation, administrative subpoenas were served to Apple requesting subscriber and other information related to (1) the device associated with IMEI number **358372062039301** (the IMEI of the iPhone seized from JONES' residence) for the time period of January 1, 2015 to the present; and (2) any other accounts in JONES' name, with billing addresses of the residences in Sidney, Piqua, and Anna for the time period of July 1, 2014 to the present. Apple provided records in response to the two subpoenas for two Apple devices with the following device registration information:
- a. iPhone 5S Gold 16 GB bearing serial number DNPMK5PAFFDQ: The device was purchased on or about June 3, 2014. Apple's records identified the device was registered to a customer with a name of Robert Jones; a street address was 1409 South State Street in Westville, Illinois; and a telephone number was 217-304-4128. The account had an Apple logon ID of eight88eighty8@live.com. The following DSID's¹⁰ were associated with the device: 8327290835, 1496191780, and **1561319194**.
 - b. iPhone 6 Gold 64 GB AT&T USA bearing serial number DNPP46QFG5MJ: The device was purchased on or about February 10, 2015. The following DSID's were associated with the device: 8327290835, 1496191780, 1561319194, and 583937895.

¹⁰ A Destination Signaling Identifier (DSID) is a unique identification number assigned to each user when registering at iCloud.com.

The IMEI for the device was 358372062039301 (which matched the IMEI for the iPhone seized from JONES' residence). Because this device was running an operating system for iOS 8 or later, no further customer information was collected by Apple upon registration of the device.

57. Records provided by Apple also identified that the four DSID's noted above were utilized to register iCloud accounts and to access various Apple applications. The following was noted regarding the DSID's:

- a. **DSID 1496191780**: The DSID had a customer name of Robert Jones; a customer address of 206 South Division Street in Cayuga, Indiana; a customer telephone number of 765-505-3701; and a customer email address of eight88eightv8@live.com. The DSID was created on or around May 27, 2013. An iCloud Account Services account was associated with this DSID. The DSID accessed the iCloud Account Services application on approximately 19 occasions during the approximate time period of July 1, 2014 to February 10, 2015. The DSID also accessed the iTunes Music Store, Game Center, and FaceTime applications.
- b. **DSID 1561319194**: The DSID had three customer names associated with it: (1) Robert Jones, with a customer address of 2368 Collins Drive in Sidney, Ohio and a customer telephone number of 765-505-3701; (2) David Levi, with a customer address of 1501 South Missouri Avenue in Morton, Illinois and a customer telephone number of 765-505-3701; and (3) Frank Sinatra, with a customer address of 2368 Collins Drive in Sidney, Ohio and a telephone number of 765-505-3701. The email address associated with the DSID for the three customer names was xolker@yahoo.com. The DSID was created on or around August 13, 2014. An iCloud Account Services account was associated with this DSID. The DSID accessed the iCloud Account Services application on approximately 130 occasions during the approximate time period of August 14, 2014 to August 21, 2015. The DSID also accessed the iTunes Music Store, Game Center, FaceTime applications, GrandSlam, and My Apple ID applications.
- c. **DSID 8327290832**: The DSID had a customer name of Robert Jones; a customer address of 2368 Collins Drive in Sidney, Ohio; a customer telephone number of 937-658-4024; and a customer email address of preveus@outlook.com. The DSID was created on or around May 10, 2015. An iCloud Account Services account was associated with this DSID. The DSID accessed the iCloud Account Services application on approximately 50 occasions during the approximate time period of May 10, 2015 to August 20, 2015. The DSID also accessed the iTunes Music Store, Game Center, FaceTime, GrandSlam, and My Apple ID applications.
- d. **DSID 583937895**: The DSID had a customer name of William Johnson; a customer address of 3650 County Road 152 in Albin, Wyoming; a customer telephone number of 307-246-3209; and an email address of xolker88@gmail.com. The account DSID was created on or around June 22, 2015. An iCloud account was associated with this DSID. Records from Apple did not identify any applications that were accessed utilizing this DSID.

58. As part of the investigation, administrative subpoenas were served requesting subscriber information for telephone numbers 217-304-4128, 765-505-3701, 937-658-4024, and 307-246-3209. Records received in response to these subpoenas provided the following information:
- a. 937-658-4024: Records received from AT&T identified that during the time period of approximate May 30, 2014 to the present, JONES was the user of telephone number 937-658-4024. AT&T's records identified that JONES' address was 207 Meadowview Lane in Anna, Ohio (which I know to be the address of Heather Dulaney's mother), and that Heather Dulaney was the financially liable party.
 - b. 765-503-3701: Records from Verizon Wireless identified that during the approximate time period of April 30, 2014 to June 13, 2015, telephone number 765-503-3701 was subscribed to JONES at 206 South Division Street in Cayuga, Indiana.
 - c. 217-304-4218: Records from Sprint Corporation identified that during the approximate time period of October 6, 2013 to May 1, 2014, telephone number 217-304-4218 was subscribed to Andrea Griffin at 750 South State Street in Westville, Illinois.
 - d. 307-246-3209: Records received from RT Communications identified that no subscriber information is maintained for the telephone number.

Subsequent Seizure of Device 1 and Device 1

59. On September 22, 2015, the United States District Court for the Southern District of Ohio authorized search warrants for the following devices: (1) Apple iPhone, Model A1533, bearing FCCID BCG-E2642A and IMEI 013888008166962, gold and white in color (**DEVICE-1**); and (2) iPod bearing serial number CCQMXDVKG2T, blue and white in color (which matches the description of **DEVICE-2**, but the serial number is mis-stated by one number). The attachments to the warrants that more particularly described the devices, as well as the accompanying Affidavit, noted that the devices were located at the Bellefontaine Police Department.
60. On September 23, 2015, I traveled to the Bellefontaine Police Department to seize the devices. Upon arrival at the Bellefontaine Police Department, I learned that the devices were actually located at the Logan County Sheriff's Office. I traveled to the Logan County Sheriff's Office, and a deputy turned over **DEVICE-1** and **DEVICE-2** to me. Upon further inspection of the two devices, I noted that the serial number for **DEVICE-2** that had been provided to me and that was listed on the previous warrant was mis-stated by one letter. The devices were thereafter secured at the Federal Bureau of Investigation and have not been examined at this time.
61. Based on the discrepancies discovered on the previous warrants, I am seeking the present updated warrants out of an abundance of caution to examine and search **DEVICE-1** and **DEVICE-2**.

Evidence Available in Email and Social Media Accounts

62. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
63. Based on my training and experience, I know that individuals involved in child pornography offenses often trade images with each other via a variety of means, including email and social media accounts. Such individuals may share images they have produced as well as images obtained from others. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.
64. Based on my training and experience, I know that individuals involved in child exploitation offenses often utilize multiple accounts, aliases, and means to communicate about child exploitation offenses and obtain child pornography. Multiple aliases are used as a means to avoid detection from law enforcement. The pictures of the Arizona drivers' licenses recovered from the thumb drive, the credit cards seized from JONES' person pursuant to his arrest in July 2014, and the multiple names found on Apple's records indicate that JONES utilizes multiple aliases. Individuals also often attempt to obtain child pornography from a variety of sources, including those with whom they communicate via email; social media sites; Internet chat programs; and on Internet bulletin boards; Internet Peer-to-Peer file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email and social media communications.
65. Based on my training and experience, I know that many social media accounts and Internet websites require users to provide their email account when registering for the accounts. The social media account providers and Internet providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media and Internet accounts were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.
66. Also as noted above, social media and email providers maintain various subscriber and user information that its users provide when registering for its accounts. Such information is materially important in cases where social media and email accounts are utilized to trade child pornography, as this information can help in confirming the identity of the individuals using the accounts and committing the offenses.

67. Email and social media providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Available on Cellular Telephones

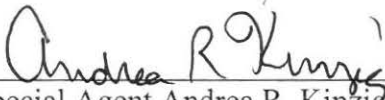
68. Based on my training and experience, I know that individuals are increasingly utilizing cellular telephones to do their computing. In my experience, I know that individuals involved in child pornography offenses often utilize both computer devices and their cellular telephones to obtain and store their child pornography files. Due to their portable nature, cellular telephones provide individuals easy access to their files.
69. In my experience, I know that due to the covert nature of the devices, individuals involved in child pornography offenses also utilize their cellular telephones to take photographs of children and produce child pornography. Based on my training and experience and examination of similar devices, I know that that **DEVICE-1** and **DEVICE-2** have digital cameras. The information provided by Minor Female A about JONES taking nude pictures of her is indicative that JONES utilizes his cellular telephones to produce child pornography.
70. Again based on my training and experience and examination of similar devices, I know that that **DEVICE-1** and **DEVICE-2** have the ability to connect to the Internet. Individuals involved in child pornography offenses often utilize their cellular telephones to access Internet websites, exchange email messages, and access social media accounts to search for, view, and download child pornography. The images recovered from ZTE cellular telephone from JONES residence indicate that JONES utilizes his cellular telephone to obtain and view child pornography.
71. In my experience, I know that many cellular telephones store information related to IP addresses that the telephone accessed and/or GPS data. This information helps in identifying the subjects and the locations where their computer devices are located.

Conclusion

72. Based all of the information detailed above, I submit that it is reasonable to believe that JONES has utilized the following devices to possess, view, receive, distribute, and/or produce child pornography and/or to coerce and entice others to engage in illegal sexual activities:
- a. Apple iPhone, Model A1533, bearing FCCID BCG-E2642A and IMEI 013888008166962, gold and white in color ("**DEVICE-1**");
 - b. iPod bearing serial number CCQMXDVKG2T, blue and white in color ("**DEVICE-2**");

CONCLUSION

73. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located in the devices described in Attachments A-1 and A-2: (1) possession of child pornography and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) and 2252(a)(4)(B); (2) receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) and 2252(a)(2)(B); (3) production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e); and (4) coercion and enticement, in violation of 18 U.S.C. §2422.
74. I, therefore, respectfully request that attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.
75. Because the warrants for **DEVICE-1** and **DEVICE-2** (described in Attachments A-1 and A-2) only seek permission to examine devices that are already in law enforcement's possession, the execution of these warrants do not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrants at any time in the day or night.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 24th of September 2015


Sharon L. Ovington
CHIEF UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN RE ORDER REQUIRING APPLE, INC.
TO ASSIST IN THE EXECUTION OF A
SEARCH WARRANT ISSUED BY THIS
COURT

Case No. _____

ORDER

FILED
RICHARD W. NAGEL
CLERK OF COURT
2015 SEP 24 AM 9:53
3:15 mj-385
U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV. DAYTON

Before the Court is the Government's motion for an order requiring Apple, Inc. ("Apple") to assist law enforcement agents in the search of an Apple iOS device. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Apple assist law enforcement agents in the examination of the iPad with Model A1421 and serial number CCQMXDVKG22T (the "iOS Device"), acting in support of a search warrant issued separately by this Court;

FURTHER ORDERED that Apple shall provide reasonable technical assistance to enable law enforcement agents to obtain access to unencrypted data ("Data") on the iOS Device.

FURTHER ORDERED that, to the extent that data on the iOS Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement, but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data;

FURTHER ORDERED that Apple's reasonable technical assistance may include, but is not limited to, bypassing the iOS Device user's passcode so that the agents may search the iOS Device, extracting data from the iOS Device and copying the data onto an external hard drive or other storage medium that law enforcement agents may search, or otherwise circumventing the iOS Device's security systems to allow law enforcement access to Data and to provide law enforcement with a copy of encrypted data stored on the iOS Device;

FURTHER ORDERED that although Apple shall make reasonable efforts to maintain the integrity of data on the iOS Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents.

Signed,


Sharon L. Ovington
CHIEF UNITED STATES MAGISTRATE
JUDGE

Date:

9-24-15