AO 106 (Rev. 04/10) Application for a Search Warrant

SEALED COPY

UNITED STATES DISTRICT COURT

for the

District of Nebraska

FILED
US DISTRICT COURT
DISTRICT OF NEBRASKA
NOV 16 2012
OFFICE OF THE CLERK

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

computers that access the website "Bulletin Board A" located at http://jkpos24pl2r3urlw.onion

Case No. 8:12MJ 356

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, incorporated herein,

located in the _____ District of Nebraska and elsewhere, there is now concealed *(identify the person or describe the property to be seized)*:

see Attachment B, incorporated herein.

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	*Offense Description*
18 U.S.C. Sections 2252A(g), 2251(d)(1) and (e), 2252A(a)(2) and (b), and 2252A(a)(5)(B)	Engaging in a Child Exploitation Enterprise, Conspiracy to Advertise, Receive and Distribute Child Pornography, Knowing Access or Attempted Access With Intent to View Child Pornography

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 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.

United States District Court District of Nebraska

Jeffrey Tarpinian
Applicant's signature

Jeffrey Tarpinian - Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/15/12

Judge's signature

City and state: OMAHA NE

F.A. GOSSETT U.S. MAG JUD.
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

IN THE MATTER OF THE SEARCH OF COMPUTERS THAT ACCESS THE WEBSITE "BULLETIN BOARD A"	)))	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Jeffrey Tarpinian, being first duly sworn, hereby depose and state:

A. INTRODUCTION AND AGENT BACKGROUND

1. I am presently employed as a Special Agent of the Federal Bureau of Investigation (FBI), and am assigned to the Cyber Crime Task Force of the Omaha Field Office in the District of Nebraska. I have been employed by the FBI since May of 1988, including four months of training at the FBI academy in Quantico, Virginia. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography, including violations pertaining to the production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. § 2252(a) and 2252A. My current duties include the full-time investigation of computer related crimes, and I have conducted over forty search warrants relating to crimes against children. As a result of my training and experience, I am familiar with information technology and its use in criminal activities. 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 all forms of media including computer media. I have also participated in the execution of many state, local, and federal search warrants, a number of which involved child exploitation and/or child pornography offenses. I am an "investigative or law enforcement officer" of the United States within the meaning of Section

2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

2. I make this affidavit in support of an application for a search warrant to use a network investigative technique ("NIT") further described in this affidavit and its attachments.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies as described below; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by federal agents; independent investigation and analysis by FBI agents/employees and U.S. Department of Justice computer forensic professionals; my experience, training and background as a Special Agent with the FBI, and communication with computer forensic professionals assisting with the design and implementation of the NIT. This affidavit includes only those facts that I believe are necessary to establish probable cause and does not include all of the facts uncovered during the investigation.

B. RELEVANT STATUTES

4. This investigation concerns alleged violations of: 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. § 2252A(a)(5)(B), Knowing Access or Attempted Access With Intent to View Child Pornography.

a. 18 U.S.C. § 2252A(g) prohibits a person from engaging in a child exploitation enterprise. A person engages in a child exploitation enterprise if the person violates, inter alia, federal child pornography crimes listed in Title

18, Chapter 109A, as part of a series of felony violations constituting three or more separate incidents and involving more than one victim, and commits those offenses in concert with three or more other persons;

b. 18 U.S.C. §§ 2251(d)(1) and (e) prohibits a person from knowingly conspiring to make, print or publish, or causing to be made, printed or published, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

c. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) prohibits a person from knowingly 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;

d. 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.

C. DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

5. The following definitions apply to this Affidavit:

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" refers to a linked series of posts and reply messages. Message threads 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 bulletin board administrator.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256 (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).

d. "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."

e. "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 DNS (domain name system) 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.

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written,

recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, 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 alpha-numeric 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.

j. "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.

k. "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 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.

l. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

m. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

n. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. "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).

p. "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).

q. "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).

D. PROBABLE CAUSE

The Tor Network

6. "Bulletin Board A" operates on an anonymity network available to Internet users known as "The Onion Router" or "Tor" network. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.

7. The Tor 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. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user's physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP

address, shows up in the website's IP log. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor network operates similarly to a proxy server. Tor accordingly allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features, such as Torbutton and Torbrowser bundle. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

8. Tor 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 Tor network itself, entire websites can be set up as "hidden services." "Hidden services" 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 Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor 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 that website server.

Finding and Accessing "Bulletin Board A"

9. As described below, U.S. authorities were alerted to the location and contents of "Bulletin Board A," which remains active and operating, by Dutch authorities in or about August of 2011. Because "Bulletin Board A" is a Tor hidden service, it cannot be accessed from the traditional

Internet. Only a user who has installed Tor software on his/her computer may access the board. A user installs Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org. Even after connecting to the Tor network, however, a user must know the web address of "Bulletin Board A" in order to access it. Rather than a plain language address like www.cnn.com, a Tor web address is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of "Bulletin Board A" on Tor and obtain the web address for the board. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on "Bulletin Board A" as well as its location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. "Bulletin Board A" is listed in that section. Accessing "Bulletin Board A" therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon "Bulletin Board A" without understanding its purpose and content. Moreover, the name of "Bulletin Board A" contains a direct reference to the sexual abuse of children. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses "Bulletin Board A" has knowingly accessed with intent to view child pornography, or attempted to do so.

Description of "Bulletin Board A" and Its Content

10. As of the present date, "Bulletin Board A" remains an active and operating child

pornography bulletin board dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including methods and tactics of perpetrating child sex abuse and the safety and security of individuals who seek to sexually exploit children online. The URL of "Bulletin Board A" is http://jkpos24pl2r3urlw.onion. Between September and November of 2012, law enforcement agents operating on the Tor network documented portions of the board as it appeared to a registered user of the board, via computer screen shots and video capture. Law enforcement agents have continued to monitor the website and its contents up until the present date. The name of the board itself makes reference to a sexual interest in children. The home page of the board, which is immediately visible to any user who accesses the board, contains at the top of the page an image of a nude prepubescent female, depicted from the chest up. As of November 12, 2012, the board home page states that it has over 6,000 members, over 3,000 message threads, and over 23,000 postings. Each of those numbers increases every day. Users may browse through all of the various forums, access the content of the board, and post messages as a "guest" without signing in as a member.

11. In order to sign up to be member of the board, a user must provide a username and password. Users of "Bulletin Board A" do not use their real names on the board. Rather, usernames or "screen names" are aliases that board members use to communicate on the board. Board members are also given a particular "rank" depending upon the number of their posts. A member's rank increases on each of the following occasions: after the member's first posting; after the member's second posting; after the member's tenth posting; and after the member's fiftieth posting. Other honorary ranks are given to some members by the board administrator. Registered members who have signed up with a username and password, but not guests, can communicate with other members

through private messages, which are similar to e-mail messages and which are only accessible to the user who sent or received such a message and possibly to the website administrator. Some examples of public postings on the board where "Bulletin Board A" users discuss the use of private messaging include: On June 14, 2012, a registered user of "Bulletin Board A" posted a message in the "Pedo Talk" section of the board soliciting advice on how to "find [a] [boy] who [she] can tease and get him to do things I want [in] exchange for sex." The user also asked which age would be best. Between June 19 and June 25, 2012, numerous "Bulletin Board A" users responded with advice, including that the user should attempt to get a job as a babysitter for young boys. On June 25, 2012, a registered "Bulletin Board A" user suggested that the original user who posted the inquiry should "send me a private message if you need help." On October 15, 2012, a registered "Bulletin Board A" user posted a message in reply to a message thread titled "Molesting" in which members discussed experiences with sexually abusing children. The registered user of the board stated "its lovely with kids that don't speak, saying and doing things with them. Whispering to them that ur a pedo, taking out your cock to show them, smiling at them and rubbing it on their mouths, putting your hand up her clothing to feel her body, nothing is hotter. Message me if you like it or have done it."

12. "Bulletin Board A" has three main categories: "Board," "Images" and "Text." Within the "Board" forum there are three subforums: "Information," "Question" and "Comments." Within the "Images" forum there are six subforums: "Babies," "Boys," "Girls," "JB Boys," "JB Girls," and "Misc." Within the "text" forum there are five subforums: "Pedo Talk," "Links," "Freenet," "Misc," and "Stories." The main page of the board also contains what is commonly referred to as a "shoutbox," where board members may post short messages and chat with one another. Topics of conversation in that shoutbox consistently involve the sexual exploitation of children. For example,

on September 10, 2012, a shoutbox user posted the question: "anyone know of a pedo social network?" Another user answered that message stating: "PEDOBOOK BUT ITS NOT THAT SAFE." Some recent postings to the board are described as follows. On October 27, 2012, a guest user of "Bulletin Board A" posted a message titled "This LS girl" in which the user stated "hey fellow child lovers, wondering if any one [sic] can post anymore of this stunning beauty...I have spilt my share of cream over what I have found over the years..." Attached to the posting was a single digital image of a prepubescent female child posing nude outdoors and exposing her vagina to the camera. Between October 28 and November 1, 2012, three different "Bulletin Board A" users posted replies to that posting including additional images of the same prepubescent female posing nude and exposing her genitals, stating her name, and directing other users to where they could find additional lascivious images of her on the Internet. On October 28, 2012, a registered "Bulletin Board A" user posted a message titled "thanks for all" which contained five digital images, three of which depict the vagina of an infant child whom the author states is his daughter. On October 31, 2012, a registered "Bulletin Board A" user posted a message titled "pedo mommys" which contained four digital images, three of which depicted adult women engaging in oral and manual sex with prepubescent boys, and one of which depicted an adult woman posing with a prepubescent female, where both were exposing their vaginas. Another registered user posted in reply, on November 1, 2012, stating "the 2nd one is a doll." On October 31, 2012, a guest user of "Bulletin Board A" posted multiple messages that included numerous close-up photographs of a prepubescent female's vagina, some of which depicted her with panties and others which depicted her genitals. On November 1, 2012, another guest user of "Bulletin Board A" posted a message in reply stating "spread her legs, rub your cock on her soft cunt and cum all over her . . .[p]ost the pics and I will post

more of this girl." That posting included a single image of a toddler-aged female child lying nude with an adult male resting his penis on top of her vagina. On November 01, 2012, a registered user of "Bulletin Board A" posted the message titled "Just a lil bit of [name]" which contained five digital images focusing on the vaginal area of a prepubescent girl, one of which shows the exposed vagina of prepubescent girl and a piece of paper next to her with "["Bulletin Board A"] Sept 12 2012" written on it.

13. The "babies" subforum contains nearly 100 message threads, each of which message thread contains postings by board members, including images of child pornography depicting infant and toddler-aged children posed to expose their genitals or being subjected to sexually explicit conduct by adults. Some images depict infant children nude and covered in what appears to be semen. Postings in the "babies" section contain message thread titles, among others, such as: "Yummy baby getting fucked by daddy," "Ideas and baby rape fantasys!!!," "Baby whores" and "baby bestiality." The "boys" and "girls" categories respectively are described by the board as including preteen boys and girls. Review of images posted by members in those categories demonstrates that the categorization is accurate – i.e., that images depicting preteen boys and girls posed nude to expose their genitals or engaging in sexually explicit conduct with adults or other children are contained within that category of postings. The "JB boys" and "JB girls" categories are described by the board as including teen boys and girls. In my training and experience, "JB" is a reference to "jailbait," a term for minor children who are or appear to be near the age of majority. Review of images posted by members in those categories demonstrates that the categorization is accurate – i.e., that images depicting teenage boys and girls posed nude to expose their genitals or engaging in sexually explicit conduct with adults or other children are contained within that category

of postings. In total, "Bulletin Board A" contains thousands of postings and messages containing child pornography images. Those images include depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

14. "Bulletin Board A" users frequently discuss security, anonymity, and preventing detection by law enforcement, including specifically how to use the TrueCrypt encryption program to avoid law enforcement detection upon a search. For example, on January 4, 2012, a "Bulletin Board A" user posted a question in the "Text – Pedo Talk" section of the board asking whether and how law enforcement would know that a particular file on the user's computer was actually a hidden encrypted TrueCrypt volume. Multiple users posted responses to that question extensively discussing the proper use of TrueCrypt encryption. On July 11, 2012, another user of "Bulletin Board A" posted an extensive guide about how to set up one's computer and storage drives to be properly encrypted. That user also detailed how to browse the Internet and download child pornography in such as way as to maintain the user's anonymity online and to keep the user's child pornography collection encrypted and therefore protected from a search by law enforcement in the event the user was identified.

15. Text sections of "Bulletin Board A" provide forums for discussion of methods and tactics to use to perpetrate child sexual abuse. For example, message thread titles in the "Text – Pedo Talk" section of "Bulletin Board A" include: "[m]olesting;" "[h]ow to lure a child in my car?;" "[m]eeting other pedos in real life;" [a]nyone here met other pedophiles and had a good experience;" [d]o kids LIKE anal sex?" and "SEA: Where would you go?" In my training and experience and after reviewing that message thread, "SEA" refers to Southeast Asia and that thread was a forum for

discussion of where in Southeast Asia to go to find sexual access to children. Although there are some postings of child sex fantasy stories in the "Pedo talk" section, it is primarily dedicated to persons seeking practical advice regarding how to sexually abuse children.

"Administrator" on Bulletin Board A

16. "Bulletin Board A" has only one administrator, whose username is "Administrator." Your affiant submits that there is probable cause to believe that the administrator of "Bulletin Board A" is Aaron McGrath of Omaha, Nebraska. According to "Bulletin Board A," user "Administrator" joined the board on January 15, 2009. That date appears to be the inception of the board. To date, "Administrator" has made 175 posts to the board; is most active in the board category: "boys," with 30 posts in that category; and most actively posted in the message thread titled: "Hi-Res Boycock," with 16 posts in that topic. Many posts by "Administrator" contain child pornography. For example, on September 18, 2012, "Administrator" posted numerous messages to the board that included digital photos depicting prepubescent minor boys posing nude and exposing their genitals, and adult males performing manual and oral sex on the genitals of prepubescent boys. On April 12, 2012, "Administrator" posted messages to the board that included digital photos depicting minor boys engaging in oral sex with adult males. On February 13, 2011, "Administrator" posted messages to the board that included digital photos depicting minor boys exposing their genitals and engaging in anal sex with adult males.

17. "Administator" also provided advice to other users about how to avoid law enforcement detection. For example, on April 16, 2011, "Administrator" posted a reply message on a posting thread titled "What do you do to ensure safety doing what you do?" In that post, "Administrator" stated:

> I recommend running all your on-topic activities from a virtual machine with an encrypted system drive. Also not a bad idea to store the vm files withing [sic] an encrypted container on the host system. And of course, if you are able to piggyback of [sic] somebody else's internet connection, go with that.

In my training and experience, "on-topic" refers to the topic of child pornography. Also in my training and experience and in consultation with computer forensic professionals, a "virtual machine" is a software program that emulates characteristics of a real physical computer including graphics, computer processing, memory, and disk storage. A 'virtual machine' executes programs like a real, physical computer – essentially a virtual computer-within-a-computer. Virtual machines can be used to mask one's activity online and conceal computer programs and files.

18. "Administrator" also shared some personal information through postings to the site. On January 15, 2009, "Administrator" posted a message in response to a posting thread titled "How old is everyone here?" In that post, "Administrator" stated: "25 here, though I've been into this since I was like maybe 14 or 15 I think." Aaron McGrath was 25 years-old on January 15, 2009. On January 16, 2009, "Administrator" posted a reply message in response to another message that asked whether anyone "had any hot true pedo stories to share." In that post, "Administrator" described how "a couple years ago" he had fondled the breasts and vagina of a then nine-year-old cousin while that cousin was sleeping. He stated that the female cousin was 15 years old at the time of his post.

Prior Identification and Seizure of Data Associated With "Bulletin Board A"

19. In August of 2011, the National High Tech Crime Unit (NHTCU) of the National Police Services Agency (KLPD) of the Netherlands initiated an independent investigation into large volumes of child pornography being hosted and distributed via "hidden services" within the Tor network. Prior to initiating its investigation, the United States, along with other countries, was made

aware of the investigation, but the United States was not involved in its execution. In order to identify potential "hidden services" involved in the distribution of child pornography, the NHTCU activated a web crawler to search available "hidden services" within the Tor-network. A web crawler is a software program that can be used to automatically search for websites, identify any hyperlinks contained on those websites, and follow those hyperlinks to additional websites. The NHTCU configured the web crawler to search for "hidden services" ending in ".onion" within the Tor network. Several hundred "hidden services" were identified and documented by the NHTCU. Each of these "hidden services" was then manually reviewed by the NHTCU to determine whether it contained child pornography. After determining which "hidden services" contained child pornography, the NHTCU obtained a search warrant from the Court of Rotterdam as ordered by the Public Prosecutor at the Rotterdam National Prosecutor's Office to obtain evidence in regards to these "hidden services," including the physical location of the server(s) hosting them.

20. On or about August 15, 2011, the NHTCU identified the "hidden service" hereinafter referred to as "Hidden Service B" as containing numerous images of child pornography, including images of minors engaged in oral, vaginal and/or anal sex with either adults or other minors. The actual name of "Hidden Service B" contains a reference to the sexual exploitation of children. Pursuant to the aforementioned search warrant, the NHTCU accessed "Hidden Service B" from August 15, 2011 through August 18, 2011. After accessing the hidden service, the NHTCU accessed the administrative account that had complete access to the hidden service. Upon accessing the administrative account, the NHTCU determined the account was not password protected. Pursuant to the search warrant, the NHTCU logged into the administrative account, granting them administrative access to "Hidden Service B." The NHTCU then copied the entire contents of

"Hidden Service B" onto a server operated by the NHTCU in The Netherlands. After copying the contents of "Hidden Service B," the NHTCU gained access and control of the server hosting "Hidden Service B." Once the NHTCU gained control of the server hosting "Hidden Service B," it located multiple IP addresses assigned to that server. The NHTCU found four IP addresses that were associated with the server hosting "Hidden Service B," including: 70.34.32.235, 70.34.32.112, 70.34.32.1, and 70.34.32.3. A search of publicly available data revealed that these IP addresses appeared to resolve to locations within the United States. As described further below, it was later discovered that those IP addresses belonged to computers located at Power DNN in Bellevue, Nebraska, a company affiliated with the employer of Aaron McGrath. Accordingly, as of August of 2011, "Hidden Service B" was being hosted on computers located at Power DNN in Bellevue, Nebraska.

21. After obtaining those IP addresses, the NHTCU executed a series of additional commands and searches within the server hosting "Hidden Service B." Among other things, the NHTCU identified all programs present on the server and all active programs on the server at the time the NHTCU controlled the server, and created a list of each. One of the active programs was identified as TrueCrypt, which is an open source, publicly available encryption program, the functionality of which is more particularly described below. The NHTCU also copied all files contained in the server directory file. Due to the nature of the Tor anonymous network hiding the physical location of the server, the likelihood that their presence on the server would be known to its operator, and the subsequent likelihood and concern that the evidence would be easily deleted by the operator, Dutch authorities secured the evidence they encountered by copying it from the servers prior to completing their search warrant. The NHTCU then identified a Tor-network configuration

file on the server, which revealed two additional hidden services being hosted on that server hereinafter referred to as "Hidden Service C;" and "Hidden Service D." The actual name of "Hidden Service C" contains a reference to minors. The actual name of "Hidden Service D" contains a reference to images. The NHTCU then found, accessed and copied the contents of a Mozilla Firefox Internet web browser profile that was also located on the server hosting "Hidden Service B." A search of this profile by the NHTCU revealed that numerous websites believed to contain child pornography had been browsed by the user of that computer using a Mozilla Firefox browser.

22. A further search of the above described Tor-network configuration file revealed an additional hidden service, "Bulletin Board A." That hidden service was previously known to the NHTCU as a Tor hidden service which contained child pornography, including images of minors engaged in oral, vaginal, and/or anal sex with either adults or other minors. The NHTCU then copied the contents of "Bulletin Board A" using multiple software programs. After copying the contents of "Bulletin Board A," the NHTCU gained access to the server hosting "Bulletin Board A." The NHTCU identified the directory in which the hidden service application was found. The NHTCU then successfully accessed the "hidden services" database and gained access to the server. After gaining access to the server, the NHTCU identified the IP address of the server as 98.161.25.30. A search of publicly available data revealed that this IP address appeared to resolve to a location within the United States. As described below, that IP address belonged to Cox Communications and was in August of 2011 assigned to the home Internet account at the address of Aaron McGrath. Accordingly, as of August of 2011, "Bulletin Board A" was being hosted at the home of Aaron McGrath.

23. The NHTCU then searched various directories within the "Bulletin Board A" server

and identified a directory containing approximately 24,951 digital image files. The NHTCU reviewed these files and determined that the majority of them constituted child pornography, including images of minors engaged in oral, vaginal, and/or anal sex with either adults or other prepubescent minors. The contents of this directory were then copied to a server operated by the NHTCU in The Netherlands. The NHTCU located several other directories within the server that directly related to the operation of the server, including the possible identity of the operator, as well as the server contents. They copied these directories as well. As with the first server encountered, due to the nature of the Tor anonymous network hiding the physical location of the server, the likelihood that their presence on the server would be known to its operator, and the subsequent likelihood and concern that the evidence would be easily deleted by the operator, Dutch authorities secured the evidence they encountered by copying it from the servers prior to concluding their search warrant.

24. In August of 2011, due to the aforementioned IP addresses appearing to resolve to the United States, the NHTCU notified the FBI and the United States Department of Justice (DOJ) of evidence obtained from the respective servers. A search of publicly available records determined that the four IP addresses associated with "Hidden Service B": 70.34.32.235, 70.34.32.112, 70.34.32.3, and 70.34.32.1; were assigned to Power DNN in Bellevue, Nebraska. Power DNN, according to its website, provides data hosting services to the public. Data hosting services refers to computer servers that can host data, including web servers. Such a facility is sometimes referred to colloquially as a "server farm." In August of 2011, FBI issued an administrative subpoena to Power DNN for information regarding those servers. The response to that administrative subpoena indicated that the servers were not at that time assigned to any Power DNN customer. Accordingly,

use of the servers to host a website could have been achieved by someone with physical access to Power DNN servers - such as an employee of the company.

25. On August 29, 2011, the United States Department of Justice issued a request for assistance from the appropriate authorities in the Netherlands pursuant to the 2004 U.S. - Netherlands Mutual Legal Assistance Agreement and its Annex and the Council of Europe Convention on Cybercrime in regards to evidence seized by the NHTCU, KLPD, as part of their investigation. In October of 2011, pursuant to the above request, the NHTCU provided a computer hard drive containing evidence seized by the NHTCU in regards to the aforementioned servers hosting "hidden services" containing child pornography within the United States. After obtaining a search warrant from a U.S. federal magistrate, FBI agents and DOJ computer forensic personnel reviewed the contents of that hard drive. The contents of that hard drive included the server data seized by authorities in the Netherlands described above.

Connection of Aaron McGrath of Omaha, Nebraska to "Bulletin Board A" and Related Hidden Services

26. According to a response to an administrative subpoena from Cox Communications, in August of 2011, the IP address associated with "Bulletin Board A" (98.161.25.30) was assigned to Cox Internet customer Tiffany Strasser at 510 Piedmont Dr., Omaha, NE, 68154. Public records and information received from the United States Postal Service show that Aaron McGrath and Tiffany Strasser were then and are currently the only residents listed at that address. FBI has conducted surveillance of 510 Piedmont Dr., Omaha, NE, 68154, during the past 30 days. McGrath and Strasser appear to be the only residents of the home. There is no open (i.e., not password-protected) wi-fi network accessible from within a short distance of the home, which would allow someone

outside 510 Piedmont Dr., Omaha, NE, 68154, to connect to the Internet using the Internet connection at 510 Piedmont Dr., Omaha, NE, 68154. McGrath maintains a publicly-accessible Facebook page on which he states that he works for Perigon Networks doing customer support. Surveillance reveals that Perigon Networks is located in Bellevue, Nebraska, in the same building as Power DNN - 1001 N Fort Crook Rd., Suite 145, Bellevue, Nebraska 68005. The respective websites for Power DNN and Perigon networks state that they were both founded by the same person and list the same business address - 1001 N Fort Crook Rd., Suite 145, Bellevue, Nebraska. They therefore appear to be related companies. Open-source Internet searches have determined that Aaron McGrath provides customer support for Power DNN servers. Surveillance has confirmed that McGrath does in fact work at the Power DNN facility at 1001 N Fort Crook Rd., Suite 145, Bellevue, Nebraska. A response to a subpoena sent to Facebook for subscriber information regarding McGrath's Facebook account revealed that the account was associated with the email address wytecastl@gmail.com. A response to a subpoena sent to Google, Inc. for subscriber information regarding wytecastl@gmail.com revealed that the account was registered to "Aaron McGrath" and that the user provided the alternate email address aaron.mcgrath@powerdnn.com. Upon information and belief, McGrath would therefore have access to Power DNN computer servers such as the ones described above which hosted Hidden Services B and C.

27. In reviewing data provided by NHTCU, a file folder was located that had been stored on the server with IP address 70.34.32.1123, which server belongs to Power DNN. That server had folders for "Hidden Service B" and "Hidden Service C." In another folder on that server was a folder named "privimg," which is a common abbreviation for "private images." There were two subfolders within that folder, one named "t" and one named "j." The folder "t" contained numerous

nude and sexually explicit photos of an adult female whose face was clearly visible in most photos. Agents have compared the Nebraska driver's license photo of Tiffany Strasser of 510 Piedmont Dr., Omaha, NE, 68154, to the photos, and the faces are indistinguishable. The "j" folder contained numerous photos of a minor female, most of which were clothed in either shorts or a bathing suit; however, one photo depicted her fully nude. That minor female is currently unidentified.

28. Communications and postings visible on "Bulletin Board A" demonstrate that the board remained continuously up and running between October of 2011 and April of 2012. During that time period, law enforcement continued to investigate the board as well as methods and tactics to investigate Tor-based bulletin boards and offenders using Tor. Beginning in April of 2012, a pen-trap and trace order was obtained for the home Internet account at 510 Piedmont Dr., Omaha, NE, 68154. That pen trap order has been renewed multiple times since April of 2012, and remains in effect. Data provided by Cox Communications pursuant to that order, collected between April of 2012 and the present, includes information about incoming and outgoing electronic communications. For example, the data includes the IP addresses of computer servers to which computers at the residence connect. The data also includes IP addresses of other computers that connect to that home Internet connection. Review of that data by FBI agents and computer forensic specialists has determined that an extremely large amount of Internet data requests travel into and out of that Internet connection. In analyzing that pen trap data, it is apparent that a Tor web server is not being hosted physically at the home. However, review of that data and publicly available information has disclosed other information. IP addresses of computers that form the Tor network are publicly listed. Those computers are commonly referred to as Tor "nodes." Review of the pen trap data demonstrates that the user of McGrath's home Internet account frequently accesses the Tor network.

The actual owner and location of computer servers is also publicly listed and searchable by IP address. Review of the pen trap data demonstrates that the user of McGrath's home Internet account frequently accesses numerous computer servers located at Power DNN in Bellevue, Nebraska, including computer servers with the following IP addresses: 208.88.72.99; 208.88.75.208; 208.88.77.241; 208.88.77.244; 208.88.78.230; 208.88.78.30; 208.88.78.40; and 70.34.34.106. The majority of connections between McGrath's home Internet account and Power DNN servers involves the server with IP address 208.88.77.241. McGrath's home Internet account has connected to Power DNN servers, including the server with IP address, 208.88.77.241 as recently as October 24, 2012. Between October 1, 2012, and October 24, 2012, McGrath's home Internet account connected to at least 14 different Power DNN assigned IP addresses. During that period of time, the server with IP 208.88.77.241 was the most frequently accessed. It can be determined from publicly available data and network information whether a particular IP address hosts a public website. A search of publicly available information and publicly accessible network data shows that none of the above Power DNN servers being accessed from McGrath's home are currently hosting publicly accessible websites. Accordingly, it is apparent from review of the pen trap data that "Bulletin Board A" is likely hosted on a computer or computers located at Power DNN but being accessed from a computer or computers at McGrath's home. That assessment is consistent with statements that "Administrator" made in postings to "Bulletin Board A" about having moved "Bulletin Board A" to a new hosting system after the NHTCU took action against "Bulletin Board A," as described below.

29. As of August of 2011, when NHTCU conducted their search, "Bulletin Board A" was active and operating. Shortly thereafter, "Administrator" posted a message on the board denying that law enforcement had taken action against the board but stating that he was shutting down the board

for a period of time. "Bulletin Board A" remained inactive until approximately October of 2011, when the board again became active. On October 13, 2011, "Administrator" posted a message stating that he had re-instituted the board. In that posting, "Administrator" stated that he had "take[n] the board down for awhile" and denied that the board was "hacked" or "compromised." He also stated that he had switched over to a "different hosting system." "Administrator" also stated that "Hidden Service D" would no longer be a part of the board. Before concluding the message, "Administrator" stated: "[s]orry for the interruption in your Pedo service, everybody back to fapping now." In my training and experience, "Pedo" is a reference to pedophilia, a sexual interest in prepubescent children, and "fapping" is a reference to masturbation. As of the current date, "Hidden Service B" and "Hidden Service C" do not appear to be operating on the Tor network.

30. On November 15, 2012, acting pursuant to a search warrant authorization from this Court, FBI executed a search warrant at Power DNN/Perigon Networks, 1001 N. Fort Crook Rd., Suite 145, Bellevue, NE. Upon speaking to Tony Valenti, the owner/founder of PowerDNN/Perigon Networks, agents learned that PowerDNN/Perigon Networks computer servers that begin with the IP address numbers 208 are located at the company next door, Cosentry, at 1001 N. Fort Crook Road, Suite 132. Servers that have been accessed from McGrath's home Internet connection, that begin with 208, are therefore located in that building. Mr. Valenti was able to particularly verify through an electronic lookup that the server with the IP address 208.88.77.241 (the one most frequently accessed by McGrath and which is believed to host "Bulletin Board A") is located at Consentry, 1001 N Fort Crook Road, Suite 132, Bellevue, NE. Agents have responded to Cosentry and, with the consent of Cosentry, located and secured the server with the IP address 208.88.77.241. That server is labeled "Aaron" with a labelmaker-type label. Upon issuance of a warrant to search and seize the

server with IP address 208.88.77.241, that server is being moved to a government facility where "Bulletin Board A" will continue to operate.

31. Also on November 15, 2012, agents executed a search warrant at McGrath's home at 510 Piedmont Dr., Omaha, NE. McGrath was located in his bedroom typing on a laptop computer. Upon seeing agents, McGrath immediately closed the laptop computer, which locked the computer. Agents were able to determine the password and unlock the computer. Among other things, a web browser window was open and connected to "Bulletin Board A." McGrath had been browsing a "Bulletin Board A" page titled "13 y/o girl pics," while logged in as "Administrator." Agents also noticed that the laptop computer was directly connected to the computer server with the IP address 208.88.77.241.

32. Sometimes, non-Tor-based websites have IP address logs that can be used to locate and identify the board's users. In such cases, a publicly available lookup would be performed to determine what ISP owned the target IP address, and a subpoena would be sent to that ISP to determine the user to which the IP address was assigned at a given date and time. However, in the case of "Bulletin Board A," the logs of member activity contain only the IP addresses of Tor "exit nodes" utilized by board users. A Tor "exit node" is the last computer through which the communications of a Tor user were routed before the communications reached their destination. It is not possible to trace such communications back through the Tor network to the actual user who sent the communications. Accordingly, those IP address logs cannot be used to locate and identify the users of "Bulletin Board A."

E. THE NETWORK INVESTIGATIVE TECHNIQUE

33. Based on my training and experience as a Special Agent, as well as the experience of

other law enforcement officers and computer forensic professionals involved in this investigation, and based upon all of the facts set forth herein, it is my belief that the network investigative technique applied for herein is the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity of those users of "Bulletin Board A" described in Attachment A who are engaging in the federal offenses enumerated in paragraph 4. Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," as described herein, other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

34. Based on my training, experience, and the investigation described above, I have concluded that using a network investigative technique may help FBI agents locate the users of the child pornography bulletin board "Bulletin Board A." Accordingly, I request authority to use the NIT to investigate: (1) any user who accesses any page in the "Images" section of "Bulletin Board A" and (2) any user who sends or views a private message on "Bulletin Board A" during the period of this authorization. In the normal course of operation, web sites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the web site would augment that content with some additional computer instructions. When a computer successfully downloads those instructions, the instructions are designed to cause the "activating" computer to deliver certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other

information. The NIT will not deny the user of the "activating" computer access to any data or functionality of that computer.

35. The NIT will reveal to the government environmental variables and certain registry-type information that may assist in identifying the computer, its location, and the user of the computer, as to which there is probable cause to believe they are evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and (e), Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B), Knowing Access or Attempted Access With Intent to View Child Pornography. In particular, the NIT will reveal to the government no information other than the following items, which are also described in Attachment B:

- The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
- In the ordinary course of business, "Bulletin Board A" sends a unique session identifier to the activating computer to distinguish the data from that of other "activating" computers. This unique session identifier will be collected by the NIT;
- 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).

36. Each of these categories of information described in Attachment B may constitute evidence of the crimes under investigation, including information that may help to identify the "activating" computer and its user. The actual IP address of a computer that accesses "Bulletin

Board A" can be associated with an Internet service provider ("ISP") and a particular ISP customer. The session identifier will distinguish the data from that of other "activating" computers. The type of operating system running on the computer can help to distinguish the user's computer from other computers located at the user's premises.

37. Based on my training, experience, and the investigation described herein, I know that network-level messages and information gathered directly from a sending computer can be more effective than other types of information in identifying a computer, its location and individual(s) using a computer. For instance, as described above, individual(s) using the Tor network can conceal their true originating IP address and thereby intentionally inhibit their identification. Getting IP address and other information directly from the computer being used by the subject can defeat such techniques.

38. During the thirty day period that the NIT is deployed on "Bulletin Board A," each time that any user accesses any page in the "Images" section of "Bulletin Board A" or any user sends or views a private message on "Bulletin Board A," the NIT authorized by this warrant will attempt to cause the user's computer to send the above-described information to a computer controlled by or known to the government.

F. REQUEST FOR DELAYED NOTICE

39. Rule 41(f)(3) allows for the delay of any notice required by the rule if authorized by statute. 18 U.S.C. § 3103a(b)(1) and (3) allows for any notice to be delayed if "the Court finds reasonable grounds to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in 18 U.S.C. § 2705) . . . ," or where the warrant "provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its

execution, or on a later date certain if the facts of the case justify a longer period of delay." Because there are legitimate law enforcement interests that justify the unannounced use of a NIT, I ask this Court to authorize the proposed use of the NIT without the prior announcement of its use. Announcing the use of the NIT could cause the members of "Bulletin Board A" to undertake other measures to conceal their identity, or abandon the use of "Bulletin Board A" completely, thereby defeating the purpose of the search.

40. The government submits that notice of the use of the NIT, as otherwise required by Federal Rule of Criminal Procedure 41(f), would risk destruction of, or tampering with, evidence, such as files stored on the computers of individuals accessing "Bulletin Board A." It would, therefore, seriously jeopardize the success of the investigation into this conspiracy and impede efforts to learn the identity of the individuals that participate in this conspiracy, and collect evidence of, and property used in committing, the crimes (an adverse result under 18 U.S.C. §3103a(b)(1) and 18 U.S.C. § 2705).

41. Furthermore, the investigation has not yet identified an appropriate person to whom such notice can be given. Thus, the government requests authorization, under 18 U.S.C. §3103a, to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), until 30 days after any individual accessing "Bulletin Board A" has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

42. The government further submits that, to the extent that use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no way to view the information and to use it to further the investigation. Furthermore, the NIT does

not deny the users access to "Bulletin Board A" or the possession or use of the information delivered to the computer controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

G. TIMING OF SEIZURE/REVIEW OF INFORMATION

43. Rule 41(e)(2) requires that the warrant command FBI "to execute the warrant within a specified period of time no longer than fourteen days" and to "execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time." After the server hosting "Bulletin Board A" is seized, it will remain in law enforcement custody. Accordingly, the government requests authority to employ the NIT onto "Bulletin Board A" at any time of day, within fourteen days of the Court's authorization. The NIT will be used on "Bulletin Board A" for not more than 30-days from the date of the issuance of the warrant.

44. For the reasons above and further, because users of "Bulletin Board A" communicate on the board at various hours of the day, including outside the time period between 6:00 a.m. and 10:00 p.m., and because the timing of the user's communication on the board is solely determined by when the user chooses to access the board, rather than by law enforcement, I request authority for the NIT to be employed at any time a user's computer accesses the board, even if that occurs outside the hours of 6:00 a.m. and 10:00 p.m. Further, I seek permission to review information transmitted to a computer controlled by or known to the government, as a result of the NIT, at whatever time of day or night the information is received.

45. The government does not currently know the exact configuration of the computers that may be used to access "Bulletin Board A." Variations in configuration, e.g., different operating systems, may require the government to send more than one communication in order to get the NIT

to activate properly. Accordingly, I request that this Court authorize the government to continue to send communications to the activating computers for up to 30 days after this warrant is authorized.

46. The Government may, if necessary, seek further authorization from the Court to employ the NIT on "Bulletin Board A" beyond the 30-day period authorized by this warrant.

H. SEARCH AUTHORIZATION REQUESTS

47. Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:

a. the NIT may cause an activating computer – wherever located – to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer, as described above and in Attachment B;

b. the use of multiple communications, without prior announcement, within 30 days from the date this Court issues the requested warrant;

c. that the government may receive and read, at any time of day or night, within 30 days from the date the Court authorizes of use of the NIT, the information that the NIT causes to be sent to the computer controlled by or known to the government;

d. that, pursuant to 18 U.S.C. § 3103a(b)(3), to satisfy the notification requirement of Rule 41(f)(3) of the Federal Rules of Criminal Procedure, the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an "activating" computer that accessed

"Bulletin Board A" has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

I. REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

48. I further request that this application and the related documents be filed under seal. This information to be obtained is relevant to an ongoing investigation. Premature disclosures of this application and related materials may jeopardize the success of the above-described investigation. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future. Accordingly, I request that the affidavit remain under seal until further order of the Court.

J. CONCLUSION

49. Based on the information identified above, information provided to me, and my experience and training, I have probable cause to believe there exists evidence, fruits, and instrumentalities of criminal activity related to the sexual exploitation of children on computers that access "Bulletin Board A," in violation of 18 U.S.C. §§ 2251 and 2252A.

50. Based on the information described above, there is probable cause to believe that the information described in Attachment B constitutes evidence and instrumentalities of these crimes.

51. Based on the information described above, there is probable cause to believe that employing a NIT on "Bulletin Board A," to collect information described in Attachment B, will result in the FBI obtaining the evidence and instrumentalities of the child exploitation crimes described above.

52. If necessary, your affiant requests to attest to the contents of this affidavit via telephone or other reliable electronic means pursuant to Fed. R. Crim. P. 4.1(b)(1) and (2)(A).

Sworn to under the pains and penalties of perjury.

Jeffrey Tarpinian

Jeffrey Tarpinian

Special Agent

Sworn to and subscribed before me this 15th day of November, 2012

F.A. Gossett

United States Magistrate Judge

United States District Court
District of Nebraska

ATTACHMENT A

Place to be Searched

This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.

The computer server is the server operating the Tor network child pornography bulletin board "Bulletin Board A," identified by its Tor URL of http://jkpos24pl2r3urlw.onion, which is located on a computer server at a government facility in the District of Nebraska.

The activating computers are those of: (1) any user who accesses any page in the "Images" section of "Bulletin Board A" and (2) any user who sends or views a private message on "Bulletin Board A" during the period of this authorization.

The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

- The "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
- A unique session identifier sent by "Bulletin Board A;"
- 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).

to the extent such information is evidence of violations of 18 U.S.C. § 2252A(g), Engaging in a Child Exploitation Enterprise; 18 U.S.C. §§ 2251(d)(1) and or (e), Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B), Knowing Access or Attempted Access With Intent to View Child Pornography.