IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF COMPUTERS THAT ACCESS THE E-MAIL ACCOUNTS DESCRIBED IN ATTACHMENT A	))))	**Case No.** 13-1746 WGC

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, [redacted], being first duly sworn, hereby depose and state:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation (FBI) since [redacted] and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I currently investigate federal violations concerning child pornography and the sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information, in conjunction with criminal investigations pertaining to child pornography the sexual exploitation of children. 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 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

SC 7/23/13

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") on users of the e-mail accounts specified in Attachment A to this affidavit (hereinafter, "TARGET ACCOUNTS"), as 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/analysts and 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.

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), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receiving and Distributing/Conspiracy to Receive and Distribute Child Pornography; and 18 U.S.C. §

7/11/17

2252A(a)(5)(B) and (b)(2), 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 making, printing or publishing, or causing to be made, printed or published, or conspiring to make, print or publish, 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 receiving or 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

[redacted]
7/12/17

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.

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

[redacted] 7/22/17

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 any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

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

[redacted] 7/12/13

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).

[redacted] 7/22/13

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

[redacted] 7/22/13

the user directly to another location in a hypertext document or to some other web page.

k. 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.

l. "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

[redacted] SC
7/11/13

personal password.

m. "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.

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

o. 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,

[redacted]
7/22/13

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).

p. "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).

q. "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).

r. "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).

PROBABLE CAUSE

6. The targets of the investigation described herein are the unidentified administrators and users who regularly send and receive illegal child pornography via websites that operate as "hidden services" located on the Tor network, described herein. Those websites are dedicated to the advertisement and distribution of child pornography, the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while

sc
7/22/13

perpetrating online child sexual exploitation crimes such as those described in paragraph 4.

7. The specific targets of the investigative technique described herein are the users of the Tor Mail e-mail accounts listed in Attachment A ("TARGET ACCOUNTS"), which are e-mail accounts that were provided by registered users of the child pornography website described herein as "Website 22" in connection with their membership on Website 22.[1]

The Tor Network

8. Website 22 and the TARGET ACCOUNTS operate 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.[2]

9. 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

[1] Because this particular website is referred to in other related legal process before this court as "Website 22," that name here is being used for consistency. The actual name of Website 22 is known to law enforcement. The site remains active and disclosure of the name of the sites would potentially alert users to the fact that law enforcement action is being taken against the site, potentially provoking users to notify other users 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.

[2] Users may also access the Tor network through so-called "gateways" on the open Internet such as "onion.to" and "tor2web.org," however, use of those gateways does not provide users with the anonymizing benefits of the Tor network.

[redacted]
7/11/13

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. An exit node is the last computer through which a user's communications were routed. 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.

10. 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. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

Finding and Accessing Website 22 and the TARGET ACCOUNTS

11. Because Website 22 and TARGET ACCOUNTS are Tor hidden services, they do

[redacted] 7/22/13

not reside on the traditional or "open" Internet. A user may only access Website 22 and TARGET ACCOUNTS through the Tor network. Even after connecting to the Tor network, however, a user must know the web address of one of the websites in order to access the site. Rather than a plain language address containing the name of the website such as 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 one of the websites on Tor to obtain and click on a link to the site. 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 is available on one of the website as well as the website's 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. Website 22 is listed in that section. Accessing Website 22 therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon Website 22 without understanding its purpose and content. Accordingly, there is probable cause to believe that, for the reasons described below, any user who successfully accesses Website 22 has knowingly accessed with intent to view child pornography, or attempted to do so.

Tor Mail

12. There is probable cause to believe that the users of the TARGET ACCOUNTS have been using, are using, and will in the future use, Tor Mail in order to accomplish, to discuss, and to commit the offenses described in paragraph 4. I have learned through this

[redacted] 5/4/13

investigation and from other law enforcement personnel who are also familiar with the applicable computer and Internet technology that the TARGET ACCOUNTS operate on Tor Mail. Tor Mail is a free, anonymous e-mail service provider that operates as a "hidden service" on the Tor network. As noted below, the administrator of Tor Mail is unknown and Tor Mail does not comply with or respond to any legal process.

13. Information about Tor Mail is available on an open internet website, www.tormail.org, and on a Tor network hidden service site, at [redacted]onion/. According to the Tor Mail Internet website www.tormail.org as of July 12, 2013:

> Tor Mail is a Tor Hidden Service that allows anyone to send and receive e-mail anonymously . . . . You will need to have Tor installed on your computer to access Tor hidden services . . . . None of Tor Mail's mail systems are hosted on this server, or on any server that you can find the IP address. Siezing [sic] or shutting down this web site will have no effect on Tor Mail's services. . . . Tor Mail consists of several servers, a Tor hidden service, and an incoming and outgoing internet facing mail servers. These internet facing mail servers are relays, they relay mail in and out of the Tor network, the relays are purchased anonymously and not tracable to us.
>
> The only thing stored on the hard drive of those servers is the Exim mail server, and the Tor software. No e-mails or logs or anything important are stored on those servers, thus it doesn't matter if they are seized or shut down. We are prepared to quickly replace any relay that is taken offline for any reason. The Tor Mail hidden service and SMTP/IMAP/POP3 are on a hidden server completely seperate [sic] from the relays, the relays do not know the IP of the hidden service. Tor Mail does not co-operate with anyone attempting to identify or censor a Tor Mail user. Tor Mail's goal is to provide completely anonymous and private communications to anyone who needs it. We are anonymous and cannot be forced to reveal anything about a Tor Mail user. You can only sign up and access Tor Mail via our Tor Hidden Service, we do not ask for any identifying information such as name or address, our service is free so we do not have billing information and tor hidden services cannot see your IP so we have no way to identify any user. We have no information to give you or to respond to any subpeona's or court orders. Do not bother contacting us for information on, or to view the contents of a Tor Mail user inbox, you will be ignored.
>
> If you wish to contact us for any reason, you may send an e-mail to click here to reveal e-mail address.

[redacted] 7/22/13

The words "click here" were a hyperlink. Clicking on that hyperlink revealed that the contact information e-mail account to be admin@tormail.org.

14. Much of that information was repeated on the Tor Mail Tor network hidden service website [redacted].onion/, which stated as of July 12, 2013:

> Tor Mail is a Tor Hidden Service that allows you to send and receive e-mail anonymously, even to addresses outside Tor . . . . Tor Mail consists of several servers, this hidden service, and an incoming and outgoing internet facing mail servers. These internet facing mail servers are relays, they relay mail in and out of the Tor network, they are disposable servers purchased anonymously and not traceable to you or us. No e-mails or logs or anything important are stored on those servers, thus it doesn't matter if they are seized or shut down. We are prepared to quickly replace any relay that is taken offline for any reason. The Tor Mail hidden service and SMTP/IMAP/POP3 are on a hidden server completely separate from the relays, the relays do not know the IP of the hidden service. Tor Mail does not cooperate with anyone attempting to identify or censor a Tor Mail user. Tor Mail's goal is to provide completely anonymous and private communications to anyone who needs it. We are anonymous and cannot be forced to reveal anything about a Tor Mail user. You can only sign up and access Tor Mail via our Tor Hidden Service, we do not ask for any identifying information such as name or address, and tor hidden
> services cannot see your IP so we have no way to identify you.

Under the "Contact Us" section of the site was the following additional warning:

> Do not contact us about lost passwords, if you do not know your password, there is no way to recover it under any circumstances. You will have to create a new account if you lose your password.

15. The Tor Mail website contained a tab where a user could set up a free Tor Mail account by creating a unique log in name and password, as well as links to software programs a user could use to access and use their Tor Mail account. As clearly noted on the open Internet and Tor network home pages, Tor Mail does not respond to any legal process nor does it solicit, keep or create any records about any of its users. Accordingly, no such records are available to

[redacted]
7/12/13

law enforcement through any sort of legal process. The date of creation of the TARGET ACCOUNTS, the actual identities of the users of the TARGET ACCOUNTS and the identity of the administrator(s) of the Tor Mail e-mail system are therefore unknown.

Description of Website 22 and Its Content

16. Specific activity by the users of the TARGET ACCOUNTS has been reviewed and documented on Website 22.

17. In July of 2013, an FBI Special Agent operating in the District of Maryland connected to the Internet via the Tor Browser and accessed the Tor hidden service at the URL [redacted]onion (hereinafter referred to as "Website 22"). Website 22 is a Tor hidden service with the primary purpose to be the advertisement and distribution of files containing child exploitation material. As of 07/12/2013, the site reports that there are almost 1.4 million files that have been uploaded and are accessible by individuals who visit the hidden service. During 2012 and 2013, FBI agents and employees downloaded more than 1 million files from Website 22. Those files have been reviewed by FBI agents and employees. Nearly all of the files depict children who are engaging in sexually explicit conduct with adults or other children, posed nude and/or in such a manner as to expose their genitals, in various states of undress, or child erotica. A substantial majority of the images downloaded by the FBI depict prepubescent minor children who are fully or partially nude or engaged in sexually explicit conduct.

18. The home page of the hidden service itself is divided into sections displaying distinct categories of material. On the left side of the home page is a category for images and videos that have recently been posted by site users. On the right side of the home page is a category for image and videos that site users have recently marked as a "favorite." The exact

[redacted] 7/12/13

images visible in those sections of the home page vary from time to time, depending on what users have recently posted or marked as a favorite. Images posted to the site can be categorized or "tagged" by users based upon the image theme or characteristics. Image tags aid in searching of files posted to the site. Users may also associate an age or age range with images posted to the site. Those age ranges also aid in searching of files posted on the site. The following files were visible on the site home page when accessed by a law enforcement agent in July of 2013:

> file number [redacted].jpg, depicts a pre-pubescent male with his genital area displayed and the focal point of the image. The age range associated with the file by users was 3-5 years of age. It had been viewed 924 times.
>
> file number [redacted].jpg, depics a nude underage female sitting on a couch. The minor female is leaned back with her legs spread and exposing her genital area and anus to the camera. The age range associated with the file by users was 12-14 years of age. It had been viewed 4,987 times.
>
> file number [redacted].jpg, depicts a nude underage female sitting on a couch. Her hands are placed on either side of her vagina in such a way that the interior of her vagina is visible. The age range associated with the file by users was 12-14 years of age. It had been viewed 4,175 times.

19. At the top-right of the home page is a search box above which are clickable categories identified as "Girls," "All," and "Boys" along with subdivided age ranges including 0-2, 3-5, 6-8, 9-11, 12-14, and 15-17. There does not appear to be a clickable link for 18+. Those categories can be used in conjunction with a search box to find files associated with a particular word/age/sex. For example, a user can click on "girls," then click on "0-2," then enter a search term in the search box, to find a particular image of a female minor between 0-2 years old. The results of this type of search are provided in a thumbnail format and based on either words "tagged" onto an image by users or words located in set or filenames associated with certain groups of related files. Selecting images or sets then allows the user to download/view

[redacted] 11/1/16

individual files with an option to download all files associated with a particular result. Based upon my training and experience and in consideration of the type of content visible on the home page of Website 22, I believe that there is probably cause to believe that any user who accesses the home page of Website 22 has accessed or attempted to access with intent to view child pornography.

20. Individuals visiting the site can upload files either singularly or in groups, either as individual files or part of an archive file. Once uploaded, these files can be viewed and/or downloaded by anyone accessing the site.

21. The site's forum section, which includes 16 language specific areas, did not itself appear to contain any child exploitation material, but did provide an area for discussion on various topics such as computer security, "Morality of Pedophilia," "Website Ideas, Improvements, & Bugs" among others. There are 16 language specific areas in the forum as well.

22. It is not required to register with the site to either post/view content or participate in forum discussions. There are no pre-requisites are requirements to create a registered account. However, for the forum section of the site, by registering an account a user gains access to the site's private messaging system. An FBI agent has registered for such a member account and observed the private messaging capability. On November 6, 2012, a user posted the following message in the Website 22 forum area "Thailand 4 Boys":

> Hi Folks,
> Soon im in thailand for holiday. Did anyone know places to find young boys that he can tell me without to much trouble? Also i search for a place with young looking boys. Need some boypics to show at home ; -) any hint is welcome – pls use private message or contact-data in my profile. Bye [redacted]

[redacted] SC
7/22/13

Based on my training and experience and the review of the site by law enforcement agents, I believe that the private message function of the site is being used to communicate regarding the dissemination of child pornography and to share information among users that may assist in the identification of TARGET SUBJECTS.

Use of Tor Mail by Users of TARGET ACCOUNTS

23. Website 22 allows registered users to set up a user profile which includes personal information about the user, including an e-mail account. That information is entered by the user. Upon review of Website 22, numerous user profiles have been observed in which Website 22 users disclose a Tor Mail e-mail account as a means by which they may be contacted. Based upon my training and experience, I believe that TARGET SUBJECTS prefer using Tor Mail due to its anonymous nature and because it is not responsive to any legal process. A review of user profiles of registered users on Website 22 shows that all of the TARGET ACCOUNTS listed in attachment A were provided by registered users of Website 22 in their user profile. Based upon my training and experience, I believe that users of Website 22 use those Tor Mail e-mail accounts to communicate regarding child pornography and the sexual exploitation of children.

Identification and Seizure of the Computer Server Hosting Website 22 and the TARGET ACCOUNTS

24. Through investigation, the FBI identified a single computer server that hosts Website 22 and dozens of other illegal Tor network child pornography websites, as well as the Tor Mail e-mail server, at [redacted] Users of Website 22 and the other websites hosted on that same computer server are engaged in the rampant and ongoing sexual exploitation of

[redacted] LSC 7/22/13

children, including the production and dissemination of child pornography, to include newly produced images of child pornography indicative of the ongoing sexual abuse of children. The administrator of the single computer server that hosts those illegal child pornography websites and Tor Mail is the subject of a criminal investigation for, among other things, criminal facilitation of the illegal activity occurring on Website 22 and other child pornography websites.

[redacted] While possession of the data will provide important evidence concerning the criminal activity that has occurred on the server and Website 22, the identities of the administrators and users of Website 22 and the TARGET ACCOUNTS will remain unknown. 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 Website 22 and the TARGET ACCOUNTS, any logs of user activity will contain only the IP addresses of Tor "exit nodes" utilized by users. Those IP address logs cannot be used to locate and identify the administrators and users of Website 22 or TARGET ACCOUNTS. Accordingly, Website 22 and the Tor Mail e-mail server will remain operating at a government facility for a limited period of time in order to locate and identify the administrators and users of Website 22 and the TARGET ACCOUNTS. Separate Title III authority is being sought from this Court regarding the monitoring of communications on Website 22. Such a tactic is necessary in order to locate and apprehend offenders including users

[redacted] 7/24/13

of Website 22 and TARGET ACCOUNTS who are engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation. FBI expects to concurrently deploy a court-authorized Network Investigative Technique ("NIT"), as described below, on Website 22 in an attempt to identify the actual IP addresses and other identifying information for computers that access Website 22. Authorization for that NIT deployment on Website 22 is being sought separately from this Court.

THE NETWORK INVESTIGATIVE TECHNIQUE

25. 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, to my knowledge a network investigative technique such as the one applied for herein is the only presently 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 administrators and users of the TARGET ACCOUNTS 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.

26. 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 TARGET ACCOUNTS. Accordingly, I request authority to use the NIT, which will be

[redacted]
7/22/13

deployed on the TARGET ACCOUNTS while the TARGET ACCOUNTS operate in the District of Maryland, to investigate any user who logs into any of the TARGET ACCOUNTS by entering a username and password.

27. 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 Tor Mail web site, which will be located in [redacted] the District of Maryland, would augment that content with some additional computer instructions. When a computer successfully downloads those instructions from the website located in the District of Maryland, 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.

28. 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 the statutes cited in paragraph 4. 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;
- A unique identifier (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other "activating"

[redacted] 11/2/13

computers. That unique identifier will be sent with and 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);
- Information about whether the NIT has already been delivered to the "activating" computer;
- The "activating" computer's Host Name. A Host Name is a name that is 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;
- The "activating" computer's 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.

29. 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 the

[redacted] 7/22/13

TARGET ACCOUNTS can be associated with an Internet service provider ("ISP") and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, and the computer's MAC address can help to distinguish the user's computer from other computers located at the user's premises.

30. During the up to thirty day period that the NIT is deployed on the TARGET ACCOUNTS, which will be located in the District of Maryland, each time that any user logs into any of the TARGET ACCOUNTS by entering a username and password, 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 that is also located in the District of Maryland.

REQUEST FOR DELAYED NOTICE

31. 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 users or administrators

[redacted] 7/22/13

of the TARGET ACCOUNTS to undertake other measures to conceal their identity, or abandon the use of the TARGET ACCOUNTS completely, thereby defeating the purpose of the search.

32. 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 the TARGET ACCOUNTS. 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).

33. 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 the TARGET ACCOUNTS has been identified to a sufficient degree as to provide notice, unless the Court finds good cause for further delayed disclosure.

34. 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 other way, to my knowledge, to view the information and to use it to further the investigation. Furthermore, the NIT does not deny the users or administrators access to the TARGET ACCOUNTS or the possession or use of the information delivered to the computer

[redacted] 7/22/13

controlled by or known to the government, nor does the NIT permanently alter any software or programs on the user's computer.

TIMING OF SEIZURE/REVIEW OF INFORMATION

35. 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 the TARGET ACCOUNTS is seized, it will remain in law enforcement custody. Accordingly, the government requests authority to employ the NIT onto the TARGET ACCOUNTS at any time of day, within fourteen days of the Court's authorization. The NIT will be used on the TARGET ACCOUNTS for not more than 30-days from the date of the issuance of the warrant.

36. For the reasons above and further, because users of the TARGET ACCOUNTS communicate on the site 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 site is solely determined by when the user chooses to access the site, rather than by law enforcement, I request authority for the NIT to be employed at any time a user's computer accesses the TARGET ACCOUNTS, 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.

37. The government does not currently know the exact configuration of the computers that may be used to access the TARGET ACCOUNTS. Variations in configuration, e.g.,

[redacted]
7/22/13

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.

38. The Government may, if necessary, seek further authorization from the Court to employ the NIT on the TARGET ACCOUNTS beyond the 30-day period authorized by this warrant.

SEARCH AUTHORIZATION REQUESTS

39. 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;

[redacted] 11/2/16

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 the TARGET ACCOUNTS has been identified to a sufficient degree as to provide notice, unless notification is further delayed by court order.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

40. 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.[3]

CONCLUSION

41. 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 the TARGET ACCOUNTS, in violation of 18 U.S.C. §§ 2251 and 2252A.

[3] The United States considers this technique to be covered by law enforcement privilege. Should the Court wish to issue any written opinion regarding any aspect of this request, the United States requests notice and an opportunity to be heard with respect to the issue of law enforcement privilege.

[redacted] 7/22/13

42. 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.

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

Sworn to under the pains and penalties of perjury.

[redacted]
Special Agent

Sworn to and subscribed before me
this 22 day of July, 2013

William Connelly
HONORABLE WILLIAM CONNELLY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Locations 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 Mail e-mail accounts referred to herein as the TARGET ACCOUNTS, as identified below, which will be located at a government facility in the District of Maryland.

The activating computers are those of any user who logs into any of the TARGET ACCOUNTS by entering a username and password.

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

The TARGET ACCOUNTS, as identified by their respective account names, are:

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.gov
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.oni
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

7/22/13

[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

WC
[redacted] 7/22/13

[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.oni
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.net
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.com
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted] 7/22/13

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org
[redacted]@tormail.org

[redacted]
11/2/13

ATTACHMENT B

Information to be Seized

From any "activating" computer described in Attachment A:

1. the "activating" computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other "activating" computers, that will be sent with and collected by the NIT;
3. 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);
4. information about whether the NIT has already been delivered to the "activating" computer;
5. the "activating" computer's Host Name;
6. the "activating" computer's media access control ("MAC") address;

that 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), Advertising and Conspiracy to Advertise Child Pornography; 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt and Distribution of, and Conspiracy to Receive and Distribute Child Pornography; and/or 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Knowing Access or Attempted Access With Intent to View Child Pornography.

[redacted] 9/12/13