AFFIDAVIT OF SPECIAL AGENT JENNIFER L. WEIDLICH

I, Jennifer L. Weidlich, being duly sworn, hereby depose and say:

1. I am a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") assigned to the Boston Division, and have been so employed for approximately eleven (11) years. I am currently assigned to the Worcester Resident Agency of the Boston Division of the FBI. I have received specialized FBI training in the investigation of computer and computer-related crimes and crimes involving the sexual exploitation of children. My responsibilities include the investigation of various criminal offenses, including the investigation of crimes involving the sexual exploitation of children. Since my assignment to the Worcester Resident Agency, I have been assigned and have participated in numerous investigations of crimes involving the sexual exploitation of children via the Internet.

2. This affidavit is submitted in support of an application for a warrant to search the residence of SCOTT PEELER ("PEELER"), located at 28 Trinity Avenue, Worcester, Massachusetts (hereinafter, the "Subject Premises"). As described herein, there is probable cause to believe the Subject Premises contain evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and property designed for use, intended for use, or used in committing the following crimes: Attempted Production of Child Pornography, in violation of Title 18, U.S.C. § 2251; Attempted Receipt of Child Pornography, in violation of Title 18 U.S.C. § 2252A(a)(2); Attempted Coercion and Enticement of a Minor, in violation of Title 18 U.S.C. §

2422(b); and Attempted Possession of Child Pornography, in violation of Title 18 U.S.C. § 2252A(a)(5)(B) (the "Subject Offenses").[1]

3. This Affidavit is further submitted in support of a Complaint and arrest warrant charging PEELER with attempted enticement and coercion of a minor, in violation of Title 18 U.S.C. § 2422(b) and attempted receipt of child pornography in violation of Title 18 U.S.C. § 2252A(a)(2).

4. The items to be seized constitute evidence of the commission of criminal offenses, contraband, fruits of crimes and things otherwise criminally possessed, as well as property designed and intended for use, and that has been used, as a means of committing the Subject Offenses. A more specific list of items to be seized may be found in Attachment B, attached hereto.

5. The evidence described in Attachment B includes evidence maintained in electronic format on any computer (or other device capable of storing data) within the Subject

[1] I am informed that several Circuit Courts have concluded that the communications directed toward persuading a minor to engage in unlawful sexual conduct may occur through third parties. *See United States v. Olvera*, 687 F.3d 645, 647 (5th Cir. 2012); *United States v. Berk*, 652 F.3d 132, 140 (1st Cir. 2011); *United States v. Douglas*, 626 F.3d 161 (2d Cir. 2010); *United States v. Nestor*, 574 F.3d 159, 160–62 (3d Cir. 2009); *United States v. Spurlock*, 495 F.3d 1011, 1013–14 (8th Cir. 2007); *United States v. Murrell*, 368 F.3d 1283, 1287 (11th Cir. 2004). I am further informed that, federal courts have concluded that even if the statute required direct communication with children (which it does not) an individual who arranged through an intermediary to persuade a child to engage in unlawful sexual conduct would still be guilty of attempted enticement, because that individual had, with the specific intent to commit the crime, taken a substantial step toward its completion. *Nestor*, 574 F.3d at 161-162. I am also informed that the two federal courts of appeals to have considered whether 18 U.S.C. § 2251 prohibits producing child pornography through an adult intermediary have answered in the affirmative. *See United States v. Pavulak*, 700 F.3d 651 (3d Cir. 2012); *United States v. Lee*, 603 F.3d 904 (11th Cir. 2010).

Premises. The methods by which the electronic information will be searched are more fully set forth in the "Computer Evidence" section of this affidavit.

6. The information set forth in this affidavit is based on an investigation conducted by law enforcement agents, including myself. This affidavit does not contain every fact known to me with respect to this investigation. Rather, it contains those facts that I believe to be necessary to establish probable cause for issuance of the requested warrant to search the Subject Premises and for the issuance of an arrest warrant for, and a criminal complaint against, PEELER.

RELEVANT STATUTES

7. Generally, Title 18, United States Code, Section 2251 prohibits any person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or who has a minor assist any other person to engage in, any sexually explicit conduct outside of the United States, its territories or possessions, for the purpose of producing any visual depiction of such conduct, where (A) the person intends such visual depiction to be transported to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail; or (B) the person transports such visual depiction to the United States, its territories or possessions, by any means, including by using any means or facility of interstate of foreign commerce or mail.

8. Generally, Title 18, United States Code Sections 2252A(a)(2) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in Title 18, United States Code Section 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.

9. Generally, Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 USC § 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.

10. Generally, Title 18, United States Code, Section 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce, including by computer, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempting to do so.

11. "Child Pornography," as used herein, is defined in Title 18 United States Code, Section 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

12. For purposes of this affidavit, any individual below the age of 18 will be referred to as a "child" or "minor."

13. Pursuant to Title 18, United States Code, Section 2256(2), "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.

THE SUBJECT PREMISES

14. The Subject Premises, as described in Attachment A, hereto, is located at 28 Trinity Avenue, Worcester, Massachusetts. Twenty Eight Trinity Avenue, Worcester, Massachusetts is specifically described as a multi-family residence with light yellow-colored siding, white trim, and yellow front door. The residence has a small covered front porch with white trim surrounding the entrance. The number "28" is displayed on the white trim located on the right side of the entrance to the front porch. Two last names, including that of "Peeler" appear on the black mail box located on the left side of the entrance to the front porch.

15. A public records database query identified PEELER as the owner of the residence at 28 Trinity Avenue, Worcester, Massachusetts and identified the land use as a duplex. The United States Postal Inspection Service identified three current recipients of mail at 28 Trinity Avenue, Worcester, Massachusetts with no apartment designation. Two of the recipients of mail have the last name of Peeler, one of whom is Scott Peeler. Based upon the #2 designation in the

records received from Charter Communications detailed in Paragraph 53 below,[2] agents believe that the property may be subdivided in some fashion and may, as a result, be the residence of more than one individual. Agents believe that PEELER occupies, at a minimum, the first floor of the 28 Trinity Avenue residence and that the portion occupied by PEELER is accessible by the side door on the left of the home as one views it from the street. (Photos of the property are attached at Attachment A, hereto.[3]) Agents believe the portion of the residence accessible through this door to be occupied by PEELER because on October 9, 2014, an officer of the Worcester Police Department responded to the Subject Premises in response to a claim of custodial interference relating to PEELER's three year old child. The officer noted that he walked in the side door on the left of the home as it is viewed from the street (the door indicated by the red arrow). Inside, the officer spoke with PEELER. The officer believes that the location where the officer spoke to PEELER was PEELER's apartment. The Officer was able to observe a kitchen, and a bedroom where the child was found after walking through the kitchen. The officer did not see the second floor. PEELER was alone and to the officer's observation, there was no other person living in the home. The warrant seeks only the authority to search the first floor of the premises accessible through the door on the left side of the home which is believed to be PEELER's residence based upon the foregoing.

[2] Those records reflected an address of "Scott PEELER, 28 Trinity Ave, #2, Worcester, Massachusetts."

[3] A red arrow appears on Attachment A-2 and A-3 showing the specific location of the identified door. The photographs of the premises, including the photographs identifying the door in question, are further attached as an Exhibit to the requested warrant.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

a. The following definitions apply to this Affidavit: "Electronic Communication Service Provider ("ESP"), as used herein, is defined in 18 U.S.C. § 2510(15) as any service which provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

b. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. Regardless of whether an IP address is dynamically or statically assigned, only one device can be assigned a particular IP address at any one time.

c. "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.

d. "Remote Computing Service" ("RCS"), as used herein, is defined in 18 U.S.C. § 2711(2) as the provision to the public of computer storage or processing services by means of an electronic communications system.

e. "Short Message Service" ("SMS"), as used herein, is defined as a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

f. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

g. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and

includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

h. The term "web cache," as used herein, refers to is a mechanism for the temporary storage (caching) of web documents.

i. The term "webcam," as used herein, refers to a front-facing video camera that attaches to a computer or that is built into a laptop or desktop screen. It is widely used for video calling as well as to continuously monitor an activity and send it to a Web server for public or private viewing. Webcams generally have a microphone built into the unit or use the computer's microphone for audio.

BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE[4]

16. The National Center for Missing and Exploited Children ("NCMEC") is located in Alexandria, Virginia and is the leading nonprofit organization in the U.S. working with law enforcement, families, and the professionals who serve them on issues related to missing and sexually exploited children. As part of its Congressional authorization, NCMEC has created a unique public and private partnership to build a coordinated, national response to the problem of missing and sexually exploited children, establish a missing children hotline, and serve as the national clearinghouse for information related to these issues.

17. One of the services administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children. Launched in 1998, the CyberTipline is operated in partnership with the FBI, HSI, the U.S. Postal Inspection Service, the U.S. Secret Service, the Military Criminal Investigative Organizations, the Internet Crimes Against Children Task Forces, the U.S. Department of Justice's Child Exploitation and Obscenity Section, as well as other state and local law enforcement agencies.

[4] This description is taken from NCMEC's website at http://www.missingkids.com.

18. Reports are made by members of the general public and by U.S. ESPs, which are required by U.S. federal law (18 U.S.C. §2258A) to report "apparent child pornography" to NCMEC via the CyberTipline if they become aware of the content on their servers. Leads are reviewed by specially-trained analysts, who examine and evaluate the reported content, add related information that may be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

19. The CyberTipline receives reports, known as CyberTip reports, on the following type of criminal conduct: possession, manufacture and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

20. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. However, the reports will include any known information: (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. *See* 18

U.S.C. § 2258A(b). Also, as will be illustrated below, CyberTip reports can be supplemented and made in connection with other CyberTip reports.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND EMAIL

21. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. The four functions are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols ("FTP") to anyone with access to a computer and modem.[5] Because of the proliferation

[5] The File Transfer Protocol ("FTP") is a protocol that defines how to transfer files from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

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

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

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

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

ONLINE SEXUAL EXPLOITATION OF CHILDREN VIA WEBCAM AND THE INTERNET

22. Based on my training and experience, I know one way in which individuals currently exploit children online is through the use of webcams and live streaming of the sexual abuse of children over the Internet. This is a practice that is often utilized in the Philippines and other South East Asian countries. This practice is commonly used by individuals residing outside of the Philippines who use the Internet to make contact with child sex traffickers within the Philippines. Based on my training and conversations with other agents who have experience working child exploitation investigations with ties to the Philippines, I have learned that people outside of the Philippines will use a computer, e-mail, instant messaging chat services, and/or a webcam to arrange for the sexual exploitation of minors in the Philippines. The requesting individual creates the opportunity by sending payment (through an international money transfer service such as Xoom, Western Union, or PayPal) to a third party such as a family member, guardian, or a pimp in the Philippines, who can facilitate a live show via webcam in which the child disrobes and/or performs sexually explicit acts in front of a webcam in the Philippines that is broadcast live over the Internet to the individual abroad.

23. Individuals who send money to the Philippines in exchange for a sexually explicit webcam show use various means of communicating with the minor victim or a third party over the Internet - such as e-mail and Instant Messenger programs (like Yahoo! mail and Yahoo! Messenger) - in order to facilitate the shows. E-mail and Instant Messenger programs are often used to groom the minor victim and/or to negotiate and plan the webcam shows.

24. I also know that the purchasing individuals often find ways to capture the sexual abuse and exploitation, either by recording the live shows onto their computers or taking still shots of the abuse, which can also be stored on the individual's computer or an electronic storage device.

TECHNICAL INFORMATION REGARDING YAHOO!

Yahoo! E-mail

25. In my training and experience, I have learned that Yahoo! Inc. provides a variety of on-line services, including e-mail access, to the general public. Yahoo! Inc. allows subscribers to obtain email accounts at the domain name yahoo.com. Subscribers obtain an account by registering with Yahoo! Inc. During the registration process, Yahoo! Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo! Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Yahoo! Inc. subscribers) and information concerning subscribers and their use of Yahoo! Inc. services, such as account access information, e-mail transaction information, and account application information.

26. In general, an e-mail that is sent to a Yahoo! Inc. subscriber is stored in the subscriber's "mail box" on Yahoo! Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo! Inc.'s servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Yahoo! and other ISPs have provided their users with larger storage capabilities associated with the user's e-mail account. Yahoo! and other ISPs have allowed users to store up to one (1) terabyte of information associated with the account on ISP servers. Based on

conversations with other law enforcement officers with experience in executing and reviewing search warrants of e-mail accounts, I have learned that search warrants for e-mail accounts and computer systems have revealed stored e-mails sent and/or received many years prior to the date of the search.

27. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Yahoo! Inc.'s servers, and then transmitted to its end destination. Yahoo! Inc. typically saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo! Inc. server, the e-mail can remain on the system indefinitely.

28. A sent or received e-mail typically includes the content of the message (including attachments), source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Yahoo! Inc. but may not include all of these categories of data.

29. A Yahoo! Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Yahoo! Inc. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

30. Many subscribers to Yahoo! Inc. do not store copies of the e-mails stored in their Yahoo! Inc. account on their home computers. This is particularly true because they access their Yahoo! Inc. account through the Internet, and thus it is not necessary to copy e-mails to a home

computer to use the service. Moreover, an individual may not wish to maintain particular e-mails or files in their residence to ensure others with access to the computer cannot access the e-mails.

31. In my training and experience, generally, e-mail providers like Yahoo! Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers (usually a mobile number) and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provides clues to their identity, location or illicit activities.

32. The mobile number and alternate e-mail information provided to Yahoo! Inc., by the user are particularly useful in instances where a user needs to recover his/her account in the event of a lost password or account compromise. With these, Yahoo! Inc. can send a "reset password" link to the alternate e-mail address, or an SMS message to the mobile number. Upon receiving the "reset password" link to an SMS mobile number affiliated with that account, the user can then reset the password in order to continue to utilize that particular account. Because both a mobile device number and alternate e-mail address are used to recover access to an account, they both tend to be closely associated with the user of the account. It is important to note that though Yahoo! attempts to validate the personal identifying information provided by

subscribers, the validation requires additional voluntary input from users. As this additional input is voluntary, Yahoo! is not always successful in validating a user's personal identifying information.

33. When creating an account at Yahoo! Inc., the user is provided the opportunity to create a display name and an associated "Profile." Yahoo! Inc. allows a user to personalize their Profile by "adding an image that represents you." The display name and display image a user provides for their Profile is public and can be seen by anyone, even if the user chooses to keep the rest of their Profile hidden from other users. [6]

34. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo! Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

35. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such

[6] This information regarding Yahoo Profiles is listed on Yahoo! Inc. information pages located at https://help.yahoo.com/kb/answers/SLN4197.html?impressions=true and https://info.yahoo.com/privacy/us/yahoo/profile/details.html.

as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

36. In my training and experience, e-mail users often use e-mail accounts for everyday transactions because it is fast, low cost, and simple to use. People use e-mail to communicate with friends and family, manage accounts, pay bills, and conduct other online business. E-mail users often keep records of these transactions in their e-mail accounts, to include personal identifying information such as name and address.

37. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

38. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such

as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

Yahoo! Messenger

39. In my training and experience, I have also learned that Yahoo! Inc. provides an on-line service called Yahoo! Messenger to the general public. Yahoo! Messenger is an instant messaging client provided by Yahoo! Instant Messaging ("IM") is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. In addition to text, Yahoo's software allows users with the most current updated versions to utilize its webcam service. This option

enables users from distances all over the world to view others who have installed a webcam on their end.

40. In order to obtain a Yahoo! Messenger account, a Yahoo! e-mail account is required. The Yahoo! e-mail user must download the Yahoo! Messenger program and sign in with the same credentials used for his/her Yahoo! e-mail account. Therefore the user is issued the same Yahoo! ID for the messenger program and the e-mail account.

41. The terms of service for a Yahoo! Messenger account states that a user's Yahoo! Messenger account is tied to that same user's Yahoo! Mail account. The terms of service also notify the user that Yahoo! Messenger will allow the user and the people the user communicates with to save those conversations and other information into the user's affiliated Yahoo! Mail account. Yahoo! Messenger also allows you to exchange computer to computer voice calls with your online contacts. If you subscribe to the "Phone In" or "Phone Out" premium services, you can also use Yahoo! Messenger to make or receive calls from regular telephones.

42. You must be a registered Yahoo! user in order to use Yahoo! Messenger. Yahoo! Messenger establishes a connection to the Internet when it is active -- much like a browser does -- in order for communications to be received and transmitted.

43. You may now archive Yahoo! instant messages along with Yahoo! Mail messages and search them together (in addition to Voice Mail, SMS, call history, and more). For users that have elected to archive their messages, Yahoo! Messenger will now archive messages on Yahoo! servers to establish and maintain this archive. Messages stored on Yahoo! servers in this manner are accessible from any computer system or device able to use the latest versions of Yahoo! Messenger for computer. You can view your Yahoo! Messenger conversation history and

Yahoo! Mail archive (if they are tied to the same user ID) on Yahoo! Messenger through "Conversation History" in your settings. You can turn off this feature for instant messages at any time by selecting "Do not keep a record of my conversations." Even if you choose not to save your message history, users with whom you communicate may opt to use the functionality available in their version of Yahoo! Messenger to save the communications and your conversations may be saved on Yahoo! servers, just like e-mail. You can delete your archived messages by selecting the message, and clicking on the "Delete" button. However, this does not delete any of your conversations saved by other users. Yahoo! may analyze instant messages you elect to archive in order to provide personally relevant product features, content, and advertising, and spam and malware detection.

44. In my training and experience, evidence of the true identity of the owner of an electronic account may be found in e-mail and/or instant messages, to include personal information, pictures, and residential or work place locations and addresses.

BACKGROUND

45. On or about September 17, 2014, Xoom.com, an online international money transfer service, filed a CyberTip report with NCMEC regarding Yahoo! e-mail account hannah_sweetycole@yahoo.com. I reviewed this report, which stated in part:

> Money transfer sent using our service (xoom.com) from a sender in San Francisco to a recipient in the Philippines. The recipient's Yahoo! profile picture is suspicious and depicts a young girl in a lewd act. We believe the customer may have been paying for an online webcam show.

46. The above Xoom.com CyberTip report came to the attention of the Yahoo! Electronic Crimes Investigative Team (the "ECIT"). The ECIT focuses on identifying and

documenting instances in which Yahoo! services are used in violation of Yahoo!'s Terms of Use, which include not using Yahoo! services for criminal activity.

a. On or about September 30, 2014, the ECIT provided a supplemental report to NCMEC outlining the results of the ECIT investigation that ensued following notice of the above CyberTip report by Xoom.com. I reviewed this supplemental report and learned Yahoo! reported the following, among other things:

b. The user of the hannah_sweetycole@yahoo.com appeared to be coordinating the sale of sexually explicit shows and/or images of herself, her children, and other children with whom she had direct contact and recruited other women around her to engage in the same activity.[7] These will hereinafter be collectively referred to as "Seller Accounts." Additionally, the ECIT investigation determined the Seller Accounts had several customers to whom they sold their "product" on multiple occasions. These will hereinafter be collectively referred to as "Buyer Accounts;"

c. Seller Account cutierhea_14@yahoo.com was selling images and/or shows of minors to multiple Buyer Accounts.

d. Yahoo believed Seller Accounts hannah_sweetycole@yahoo.com and cutierhea_14@yahoo.com were connected, lived in close proximity to each other in the Philippines, and may be family members. Additionally, these two Seller Accounts were linked to each other via the same SMS phone number.

47. In addition to the ECIT's assessment that cutierhea_14@yahoo.com was utilized to sell images and/or shows of minors to multiple Buyer Accounts, on or about September 30, 2014, Yahoo! generated its own CyberTip report to NCMEC regarding cutierhea_14@yahoo.com because they viewed 75 image files sent as email attachments from

[7] Based on my training and experience, I know that "shows" refers to an emerging trend of sexual exploitation of children by individuals exploiting children in foreign countries, like the Philippines, via web cameras such that individuals remotely produce sexually explicit material of minors via webcam for another individual and transmit these videos/images through live streaming on the Internet. Additionally, the reference to the user of HANNAH_SWEETYCOLE@YAHOO.COM as a female has not been verified and confirmed by investigators at this time.

this account. I reviewed these email attachments, which were included with the CyberTip report, and discovered approximately 58 images that appeared to depict child pornography.

48. The ECIT indicated that the user(s) of the Seller Accounts used Yahoo! Messenger to negotiate, with buyers, terms of sale for images and videos of child pornography. The user(s) of the Seller Accounts negotiated with many buyers, to include buyers residing within the United States. If the buyer was interested in child pornography images, the seller would then e-mail the child pornography images to the buyer using the seller's Yahoo! e-mail account. If the buyer was interested in child pornography videos, the seller would provide the videos using the Yahoo! Messenger service.

49. Based in part on the above, a federal search warrant, authorizing the search of cutierhea_14@yahoo.com, was signed by United States Magistrate Judge Alan Kay in the District of Columbia and executed on Yahoo! November 14, 2014. On or about November 18, 2014, Yahoo! returned records pursuant to these federal search warrants.

50. The records returned by Yahoo! for cutierhea_14@yahoo.com found that this user sent several emails containing sexually explicit images of a minor to other Yahoo! users. Additionally, several Yahoo Messenger chats in which this user appeared to discuss live webcam shows involving minors were discovered:

a. In one series of Yahoo! Messenger chats, dated December 27, 2013, cutierhea_14 appears to discuss a webcam show apparently involving a 4, 10, and 17 year-old girl with Yahoo! user wolfman124. These chats read, in part:

> wolfman124(14:20:36 (UTC)):your girls there?
> cutierhea_14(14:20:57 (UTC)):yep
> wolfman124(14:21:02 (UTC)):where are they
> cutierhea_14(14:21:31 (UTC)):but u need to send me hun if u wnt our show :)

wolfman124(14:21:35 (UTC)):how many?
wolfman124(14:21:39 (UTC)):yes of course
.....
wolfman124(14:22:25 (UTC)):how many girls there with you tonite angel
.....
cutierhea_14(14:23:08 (UTC)):i have 2 friends..but can u send us frst before we do show
.....
wolfman124(14:23:18 (UTC)):2 friends?
wolfman124(14:23:24 (UTC)):both girls?
cutierhea_14(14:23:32 (UTC)):yep..
wolfman124(14:23:33 (UTC)):can you call them?
cutierhea_14(14:23:43 (UTC)):if u wnt i have 1 lil girl too hehe
wolfman124(14:23:47 (UTC)):we do wu?
cutierhea_14(14:23:52 (UTC)):yes hun
wolfman124(14:24:04 (UTC)):three girls?
cutierhea_14(14:24:18 (UTC)):yea.me and my 2friends
wolfman124(14:24:26 (UTC)):you said lil girl too
wolfman124(14:24:43 (UTC)):that makes 4
cutierhea_14(14:24:50 (UTC)):oh u wnt the lil girl too..but age is 4 :D
cutierhea_14(14:24:52 (UTC)):but shes smart lol
wolfman124(14:25:13 (UTC)):so may i meet the other girls>
cutierhea_14(14:25:51 (UTC)):when u meet them,u will send?
wolfman124(14:26:06 (UTC)):yes, how much do they want, let them tell me
cutierhea_14(14:26:54 (UTC)):100$ for all girl including me :D
wolfman124(14:27:00 (UTC)):mmmmmmmmm
wolfman124(14:27:09 (UTC)):they must be very nice
cutierhea_14(14:27:21 (UTC)):yea
wolfman124(14:27:28 (UTC)):can you call them
cutierhea_14(14:28:15 (UTC)):hun girl age is 17 and other is 10 :D
wolfman124(14:28:22 (UTC)):ok
cutierhea_14(14:28:47 (UTC)):ok..i will just show them then u will send ok
wolfman124(14:28:56 (UTC)):ok

b. In another series of chats, dated March 13, 2014, the user of the cutierhea_14 appears to be discussing webcam show apparently involving a 14-year old girl with wolfman124. These chats read, in part:

cutierhea_14(23:50:15 (UTC)):do u like a show too ?
wolfman124(23:54:27 (UTC)):yes i like
wolfman124(23:54:46 (UTC)):who is there
wolfman124(23:55:11 (UTC)):i have the mtcn
cutierhea_14(23:55:15 (UTC)):lol
cutierhea_14(23:55:29 (UTC)):i have here the 6 yrs old she will use toy
cutierhea_14(23:55:36 (UTC)):and i have 4yrs old too
.....
wolfman124(23:56:56 (UTC)):you dont have 14? 13/
cutierhea_14(23:56:58 (UTC)):with big boobs and big ass
wolfman124(23:57:10 (UTC)):i like that
wolfman124(23:57:18 (UTC)):want to invite me?
cutierhea_14(23:57:35 (UTC)):lol,u need to send for shw frst
.....
wolfman124(23:57:51 (UTC)):you dont have 13 or 14 right?
cutierhea_14(23:58:03 (UTC)):i have,i show u the pics
cutierhea_14(23:58:11 (UTC)):i have 2girls on that age
wolfman124(23:58:47 (UTC)):where are they now?
wolfman124(23:59:43 (UTC)):she is very pretty, wish she was there now
cutierhea_14(23:59:51 (UTC)):the girl with white shirt her age is 13
cutierhea_14(23:59:59 (UTC)):the yello girl age 14
wolfman124(00:00:06 (UTC)):i like the yellow
cutierhea_14(00:00:16 (UTC)):ok.
wolfman124(00:00:30 (UTC)):she is with you?
.....
cutierhea_14(00:00:33 (UTC)):i can only call her when doing show
wolfman124(00:00:39 (UTC)):why dont you invite me?
wolfman124(00:00:43 (UTC)):ohhhhhhhhhhhhhhhhhhhh
cutierhea_14(00:00:46 (UTC)):i need to fetch her i thei house
wolfman124(00:00:49 (UTC)):it is like that
wolfman124(00:00:55 (UTC)):i understand
cutierhea_14(00:01:34 (UTC)):so if u wnt her show then u need to send frst
cutierhea_14(00:01:43 (UTC)):and we will give u a naked picture too
wolfman124(00:02:41 (UTC)):i want to see her yes
cutierhea_14(00:03:19 (UTC)):u know wat the last time i show u some girl,u didnt send too

51. On January 15, 2015, the FBI issued a letter to Yahoo! Inc. pursuant to 18 U.S.C. 2703(f) requesting the preservation of Yahoo! account wolfman124. Based on my training and experience, such account preservation ensures that information relating to the account is not lost if the user closes the account or attempts to delete the account's contents.

52. On January 21, 2015, an administrative subpoena was issued to Yahoo! for subscriber and login information related to wolfman124. A review of the results, obtained on January 22, 2015, identified the following subscriber/login information:

Registration IP Address: 68.112.235.85
Account Created(reg): 10/24/2011 at 22:54:38 GMT
Recent IP Login: 68.184.40.57 on 10/27/2014 at 22:06:26 (GMT)
Account Status: Active

53. On March 20, 2015, an administrative subpoena was issued to Charter Communications in regards to the Recent Login IP address (used on October 27, 2014) described in the preceding paragraph. A review of the results obtained on March 27, 2015, identified the following account holder: Scott PEELER, 28 Trinity Ave, #2, Worcester, Massachusetts.[8]

54. A check of publicly available databases on April 8, 2015, identified PEELER as Scott W. Peeler, year of birth 1962 with a current address of 28 Trinity Avenue, Worcester, Massachusetts. A Massachusetts Registry of Motor Vehicle ("RMV") query on April 6, 2015, returned an active driver's license for Peeler with a mailing address of 28 Trinity Avenue, Worcester, Massachusetts.

[8] Charter Communication records reveal that the 68.184.40.57 IP address was assigned to the PEELER account at least from August 26, 2014 at 8:15:30 GMT through November 4, 2014 at 5:22:06 GMT. Records obtained from Yahoo! reflect that the wolfman124 account was accessed an additional eleven times from that same IP address between September 25, 2014 and October 26, 2014.

55. Based upon the information contained in paragraphs 45 to 54 above, a search warrant was obtained from this Court on April 17, 2015, and executed on the same date under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), requiring Yahoo, Inc. to disclose to the government copies of the records and other information (including the content of communications) pertaining to wolfman124@yahoo.com/Yahoo ID: wolfman124, a Yahoo! email and messenger account.

REVIEW OF YAHOO! ACCOUNT FOR WOLFMAN124

56. Based upon the aforementioned search warrant served upon Yahoo! Inc., the requested account information was received from Yahoo! on April 21, 2015. Upon reviewing the content of the wolfman124 account, several Yahoo Messenger chats were discovered in which the user appeared to discuss live webcam shows involving minors.

57. Specifically, in a chat dated July 12, 2014, wolfman124 appears to be discussing the webcam show of a 12, 15, and maybe a 10 year-old with Yahoo! user marites014. The chat reads as follows:

marites014(04:41:59 (UTC)):hello hon
wolfman124(04:42:17 (UTC)):hi sexy
marites014(04:42:19 (UTC)):u want young hon
marites014(04:42:25 (UTC)):hello hon
marites014(04:42:27 (UTC)):hru
wolfman124(04:42:46 (UTC)):who is there for me today?
wolfman124(04:42:59 (UTC)):im so fucking hard it hruts
marites014(04:43:04 (UTC)):many girsl here
marites014(04:43:16 (UTC)):but u need pay 1st
wolfman124(04:43:31 (UTC)):ok
marites014(04:44:48 (UTC)):can u pay her 1st hon
wolfman124(04:44:54 (UTC)):you havew girls there?
marites014(04:45:10 (UTC)):yes u not see hon
wolfman124(04:45:41 (UTC)):no baby, im sorry, couldnt see what you are doing

marites014(04:46:28 (UTC)):i have many girls here
marites014(04:46:41 (UTC)):u like hon
wolfman124(04:46:55 (UTC)):yes
wolfman124(04:46:59 (UTC)):how old?
marites014(04:47:24 (UTC)):5 12 10
marites014(04:47:41 (UTC)):can u send 1st
wolfman124(04:51:39 (UTC)):yes
wolfman124(04:51:44 (UTC)):i like 12
wolfman124(04:52:04 (UTC)):maybe 10 if she hss tits
marites014(04:52:36 (UTC)):15 u like hon
wolfman124(04:52:52 (UTC)):no 12?
marites014(04:53:27 (UTC)):ahhhhhhhhhhhhhhhhh
marites014(04:53:31 (UTC)):ok
marites014(04:53:43 (UTC)):i have 12 here
wolfman124(04:53:51 (UTC)):i lke her
wolfman124(04:53:54 (UTC)):12 nd 15

58. In another chat dated July 12, 2014, wolfman124 appears to be discussing the webcam show of a fourteen (14) year-old with Yahoo! user guband. The chat with subject line reads as follows:

guband(22:34:36 (UTC)):thank u
guband(22:34:40 (UTC)):pvt sac now
wolfman124(22:34:47 (UTC)):girls in denim are so ooooooooooooo sexy
guband(22:34:47 (UTC)):all here is watxh tv
guband(22:35:28 (UTC)):pvt me
wolfman124(22:35:55 (UTC)):i will be back, +
guband(22:36:00 (UTC)):ok
wolfman124(22:36:13 (UTC)):want to see if any girls want me
guband(22:36:21 (UTC)):yes
guband(22:36:38 (UTC)):pvt sac u see if u pvt i open cam here freze sac u see all here
wolfman124(22:37:09 (UTC)):some girls like to show they have friends with them
wolfman124(22:37:25 (UTC)):i will come back baby if i need your show
guband(22:37:59 (UTC)):back now ok
guband(22:38:53 (UTC)):i ahve 14 naked pic and shes her and 16
guband(22:38:55 (UTC)):u like
guband(22:39:06 (UTC)):wu is ok

wolfman124(22:39:08 (UTC)):yes
wolfman124(22:39:12 (UTC)):i like that alot
guband(22:39:16 (UTC)):wu is ok
guband(22:39:27 (UTC)):if i give 1 naked pic 14 u deal now
wolfman124(22:39:42 (UTC)):is the 14 shaved? bald?
guband(22:39:47 (UTC)):yes
wolfman124(22:39:56 (UTC)):she has movies too?
guband(22:40:17 (UTC)):after u send all u got but first see the naked pic if u like
wolfman124(22:40:22 (UTC)):ok
guband(22:44:47 (UTC)):now
guband(22:44:54 (UTC)):u want name
guband(22:44:59 (UTC)):open ur cam
guband(22:45:02 (UTC)):i on my cam
wolfman124(22:45:05 (UTC)):wow, is she really there?

59. In a chat dated April 3, 2013, wolfman124 appears to be discussing the webcam show of a ten (10) year-old with Yahoo! user twogirls.cutesmile. The chat reads as follows:

wolfman124(00:20:51 (UTC)):got hot girl for me?
twogirls.cutesmile(00:21:14 (UTC)):yess
wolfman124(00:21:17 (UTC)):small girl?
twogirls.cutesmile(00:21:18 (UTC)):pay them
twogirls.cutesmile(00:21:20 (UTC)):yess
wolfman124(00:21:24 (UTC)):invite me
twogirls.cutesmile(00:21:24 (UTC)):8 10
twogirls.cutesmile(00:21:34 (UTC)):can u give tip
wolfman124(00:21:40 (UTC)):r u guyfuck_smallgirl
twogirls.cutesmile(00:21:54 (UTC)):yess
wolfman124(00:21:57 (UTC)):great
wolfman124(00:22:02 (UTC)):does 10 have tits
wolfman124(00:22:07 (UTC)):invite me please
wolfman124(00:22:17 (UTC)):how much wu you want to fuck her hard
twogirls.cutesmile(00:22:23 (UTC)):20 tip
wolfman124(00:22:30 (UTC)):ok
wolfman124(00:22:33 (UTC)):invite me
wolfman124(00:22:56 (UTC)):thank you dear
wolfman124(00:23:17 (UTC)):20 tip and she fucks guy?
twogirls.cutesmile(00:23:27 (UTC)):yess
wolfman124(00:23:32 (UTC)):till he cums
twogirls.cutesmile(00:23:43 (UTC)):yes of course

wolfman124(00:23:50 (UTC)):show me the girl please
twogirls.cutesmile(00:23:59 (UTC)):no tips 1st
wolfman124(00:24:18 (UTC)):i aint a stupid american sorry
wolfman124(00:24:37 (UTC)):i did that before and girl changed mind
twogirls.cutesmile(00:24:39 (UTC)):no tip no show
twogirls.cutesmile(00:24:44 (UTC)):not at all
twogirls.cutesmile(00:24:48 (UTC)):im not other lol
wolfman124(00:24:51 (UTC)):watever

60. In an email dated August 19, 2012, the user of email account wolfman124@yahoo.com appears to respond to a Craigslist add with the subject line "Frisky - w4m - 24 (Worcester)" with an email that reads as follows: "6' 195 lbs brown hair green eyed prof white male in worcester, very interested if u are still available. i might be out of ur age range (44 yrs) but who knows." The email is signed, "scott."[9] In an email dated August 20, 2012, the user of email account wolfman124@yahoo.com appears to respond to a Craigslist add with the subject line "pull on my nipple rings lets talk. - w4m (Worcester)" with an email that reads as follows: "hope you are real, i am by green hill golf course, having a few whiskey and teas." The email is signed, "scott."[10]

PERSONS WHO PRODUCE, POSSESS, RECEIVE, DISTRIBUTE AND ADVERTISE CHILD PORNOGRAPHY

61. As a result of the above-mentioned training and experience, I have learned that the following characteristics are generally found to exist in varying combinations and be true in cases involving offenders who produce, possess, receive, distribute and advertise material which depicts

[9] PEELER is identified as being 6'0 and has brown hair on his Massachusetts driver's license photograph. His year of birth is 1962. As such, he would have been fifty (50) years-old in August 2012.

[10] It is noted that PEELER's residence, 28 Trinity Avenue, Worcester, Massachusetts is located less than one-half of mile from the Green Hill Golf Course.

minors engaged in sexually explicit conduct. Said material includes, but is not be limited to, photographs, negatives, slides, magazines, other printed media, motion pictures, video tapes, books, or similar items stored electronically on computers, digital devices or related digital storage media.

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from (i) contact with children; (ii) from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or (iii) from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years;

d. Likewise, such individuals often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly;

e. Such individuals also (i) may correspond with and/or meet others to share information and materials; (ii) rarely destroy correspondence from other child pornography distributors/collectors; (iii) conceal such correspondence as they do their sexually explicit material; and (iv) often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography; and

f. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

62. These offenders obtain and/or traffic in materials depicting children engaged in sexually explicit conduct through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

a. Downloading via the Internet and other computer networks. (Web sites, peer-to peer file sharing networks, newsgroups, electronic bulletin boards, chat rooms, instant message conversations, e-mail, etc.);

b. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer;

c. Trading with other persons with similar interests through shipments, deliveries and electronic transfer, including but not limited to email exchanges; and

d. Producing and manufacturing these materials during actual contact with children or manipulating children into creating such materials and providing them to the perpetrator.

63. Persons who produce, possess, receive, distribute and advertise child pornography place significant value on images and videos of child pornography (and related materials). Since child pornography is illegal, it can be risky to obtain. Thus, individuals who produce, possess, receive, distribute and advertise child pornography are very unlikely to destroy or dispose of images once they are obtained. Indeed, it is well-established that individuals who produce, possess, receive, distribute and advertise child pornography hoard their images (and related materials) for many years, rarely, if ever, destroying them. This is particularly true today, when most child pornography is obtained via the Internet and can be easily stored in digital format on a computer or other data storage device. Accordingly, if an individual saves a digital image of

child pornography on his computer, that image is likely to be present on that computer several years later. Indeed, even if the individual were to destroy the digital image (or attempt to destroy it), which is rare, it is very likely that the image would still be present on, and recoverable from, the subject's computer years later.

64. In addition to maintaining their images for long periods of time, persons who produce, possess, receive, distribute and advertise child pornography almost always maintain and possess their materials within a private location such as their home. In today's computer age, the majority of such images are likely to be maintained in digital form on a computer or other data storage device located in the subject's home. As described above, such images are likely to remain on a subject's computer or other data storage device for many years.

65. Based upon the facts described herein, there is probable cause to believe that PEELER attempted to produce child pornography, attempted to coerce or entice a minor (through a third party) and attempted to receive and possess child pornography as described herein. As described above, PEELER likely places great value on these images and maintains them on his computer or other data storage device in his home to this day. Given the propensity of individuals who produce, possess, receive, distribute and advertise child pornography to store such images and/or videos within the privacy of their own homes, there is probable cause to believe that PEELER currently maintains evidence of the Subject Offenses within the Subject Premises.

COMPUTER EVIDENCE

66. Computer hardware, other digital devices, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be

contraband, evidence, instrumentalities, or fruits of a crime; and / or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

67. In this case, the search warrant application requests permission to search and seize digital media files of child pornography, child erotica and material harmful to minors as well as items indicating illicit contact with minors, including those items that may be stored on a computer, digital device or on electronic media. The images involving sexual conduct of minors constitute both evidence of crime and contraband.

68. This affidavit also requests permission to seize the computer hardware and storage media that may contain the digital media files of child pornography if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. I believe that, in this case, the computer and digital hardware is a container for evidence, a container for contraband and also itself an instrumentality of the crime under investigation.

69. I know from training and experience that computer systems commonly consist of computer processing units (CPU's), hard disks, hard disk drives, floppy disk drives, tape drives, display screens, keyboards, printers, modems (used to communicate with other computers), electronic cables, cassette tapes, floppy disks, and other forms of magnetic and optical media contain computer information. In addition, the specific transmission of computerized imagery indicates the possible use of CD-ROM / DVD drives, compact laser disks, image scanning devices, still cameras, lighting equipment, video cameras or camcorders, VCRs, digital-analogue translation devices, and the software (computer programming) necessary to operate them.

70. I know from training and experience that such computers and magnetic and optical

media are used to store information. In addition to the above mentioned image files, that information often includes data files of other persons engaged in similar activities with minors, and lists of other exploited juveniles, as well as records of correspondence and conversations (printed or electronic) with such persons.

71. I know that information, particularly erased and deleted information, stored within computers and related digital devices can reside within the memory areas of such devices for months and occasionally years. I also know that a qualified computer expert in a laboratory or other controlled environment can recover this information in whole or part.

72. Based on my training and experience, and discussions with members of the FBI CART and members of Homeland Security Investigations (HSI) Cyber Crimes squad, I know that a qualified computer specialist is required to properly retrieve, analyze, document and authenticate electronically stored data, and to prevent the loss of data either from accidental or deliberate programmed destruction. To do this work accurately and completely requires the seizure of (1) all computer equipment and peripherals, which may be interdependent; (2) the software to operate the computer system(s); (3) the instruction manuals, which contain directions concerning the operation of the computer system(s) and software programs; and, (4) all internal and external data storage devices. Each of the seized items should be searched in a laboratory or controlled environment.

73. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a significant amount of time. Indeed, computer specialists, using exacting data search protocols, must often recover hidden, erased, compressed, password-protected, or encrypted files in order to find evidence of criminal activity. Moreover, many

commercial computer software programs save data in unique formats that are not conducive to standard data searches. This requires additional effort by specialists to review such data for evidence of a crime. Finally, many users try to conceal criminal evidence by storing files in random order with deceptive file names. This requires specialists to examine all of a user's stored data to determine which particular files are relevant and within the scope of the search warrant. This process can take a substantial amount of time depending on the volume of data stored.

74. Because computer evidence is extremely vulnerable to tampering or destruction, both from external sources or from destructive codes imbedded in the system as "booby traps," a controlled environment is essential to a complete and accurate analysis.

75. Data storage devices, including but not limited to hard drives, diskettes and compact disks ("CDs"), can store the equivalent of thousands of pages of information. The majority of computers currently sold have, at a minimum, a 40 gigabyte hard drive, or larger, with an equivalent capacity in excess of 10,000,000 pages of typewritten, double spaced text.

76. For the reasons described in Paragraphs 66 to 75 of this affidavit, it is necessary to seize all computers, data storage devices and related equipment, as described in Attachment B. It is further necessary to search such equipment in a controlled environment, off-site. Given the potential for large quantities of data, a complete forensic examination of the seized items will take longer than fourteen days.

77. To the extent practical, if persons claiming an interest in the seized computers so request, I will make available to those individuals copies of requested files (so long as those files are not considered contraband) within a reasonable time after the execution of the search

warrant. This should minimize any impact the seizures may have on the computer user's personal and/or business operations. In addition, as soon as practical, those items of hardware and software no longer required for the purpose of analysis or copying of items authorized to be seized, or for the preservation of the data and/or magnetic evidence, will be returned to the party from which they were seized, so long as such items do not constitute contraband.

78. Based on my training and experience and my discussions with members of CART and HSI Cyber Crimes squad, I know that, in most cases, a trained computer specialist can retrieve deleted image files from a computer or other data storage device, including deleted images of child pornography. Depending on the size of the computer or data storage device, deleted images can be retrieved for years after they have been deleted by the user. Thus, if a user possesses images of child pornography, evidence of those images is likely to be present on his computer or other data storage device years later, regardless of whether the user has deleted or attempted to delete the images.

CONCLUSION

79. Based upon the facts described herein, there is probable cause to believe that PEELER attempted to produce child pornography, attempted to coerce or entice a minor (through a third party) and attempted to receive and possess child pornography as described herein in April and December of 2013 and in March and July of 2014 and that he attempted to coerce or entice minors and receive those images and/or videos via the Internet using a Yahoo! based messenger service. Based on my training and experience, there is probable cause to believe that evidence of those images/videos and of the coercion and enticement of minors to produce or attempt to produce those images/videos are currently present on his computer or other

data storage devices within his home even if PEELER deleted the files.

80. Based on the foregoing, I respectfully submit that there is probable cause to believe that PEELER has committed the Subject Offenses. Based on my training and experience, I further submit that there is probable cause to believe that evidence, fruits and instrumentalities of the Subject Offenses will be found at the Subject Premises. Such evidence, fruits and instrumentalities are more fully described in Attachment B attached hereto.

WHEREFORE, your affiant requests that a warrant to search the Subject Premises for the items described in Attachment B attached hereto.

JENNIFER L. WEIDLICH
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 29th day of June 2015.

Honorable David H. Hennessy
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The Subject Premises is located at 28 Trinity Avenue, Worcester, Massachusetts. The residence at 28 Trinity Avenue is specifically described as a multi-family residence with light yellow-colored siding, white trim, and yellow front door. The residence has a small covered front porch with white trim surrounding the entrance. The number "28" is displayed on the white trim located on the right side of the entrance to the front porch. Two last names, including that of "Peeler" appear on the black mail box located on the left side of the entrance to the front porch.

The premises to be searched are particularly described as the first floor of the residence, accessible by the side door on the left of the home as one views it from the street. Photographs of the home, including a photograph specifically identifying the door through which the premises are to be entered, marked by red arrows, are attached hereto as Exhibits A-1 through A-3.

ATTACHMENT B

Items to be Seized

1. Any and all child pornography, meaning any visual depiction, including, but not limited to, any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction appears to be of a minor engaging in sexually explicit conduct.

2. Any and all computers and all related computer equipment, peripherals, hardware, software, printers, data storage devices (e.g., thumb drives, zip drives, CDs, DVDs, floppy disks, digital cameras, digital memory cards, web cameras, camera phones, cellular phones, xbox 360, other storage mediums such as Apple's IPOD line of products and Microsoft's Zune digital players, and any other technology capable of storing digital images), as well as related instructions for operating the foregoing.

3. Records evidencing occupancy and/or ownership of the Subject Premises including, but not limited to, utility and telephone bills, envelopes addressed to the Subject Premises, and photographs of PEELER with and/or without other persons.

4. Records of correspondence or other communications (including, but not limited to, chatroom messages and e-mail) pertaining to or referring to: the coercion and/or enticement of minors: knowing receipt and/or distribution of child pornography; and, production and/or attempted production of child pornography.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.