Affidavit In Support Of Search Warrant

I, Eric J. Szatkowski, a Senior Special Agent with the Wisconsin Department of Justice, being duly sworn, depose and state as follows:

1. This affidavit is being submitted in support of an Application for a Search Warrant for the residence located at 10417 256th Avenue, Town of Salem (mailing address Trevor), Wisconsin, for evidence of violations of Title 18, United States Code (U.S.C.), § 2252A, entitled "Certain activities relating to material constituting or containing child pornography."

2. Based upon the information summarized in this application, I have reason to believe that evidence of such violations may be present at the residence located at 10417 256th Avenue, Town of Salem (mailing address Trevor),Wisconsin.

3. The information supplied in this affidavit is based upon my investigation, information provided by and investigation conducted by other law enforcement personnel in this matter to date. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact of this investigation.

Applicable Law

4. This investigation concerns alleged violations of United States Code, §2252A, entitled, "Certain activities relating to material constituting or containing child pornography," which provides in part:

a. any person who -

I knowingly mails or transports or ships, in interstate or foreign commerce by any means, including by computer, any child pornography;

ii. knowingly receives or distributes -

1. any child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer; or

2, any material that contains child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any mean, including by computer;

iii. knowingly -

1. re produces any child pornography for distribution through the mails, or in interstate or foreign commerce by any means, including by computer; or

2, advertises, promotes, presents, distributes, or solicits through the mails, or in interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains -

a. an obscene visual depiction of a minor engaging in sexually explicit conduct; or

b. a visual depiction of an actual minor engaging in sexually explicit conduct;

iv. . . .

v. either -

1. . . .

2. knowingly possesses any book, magazine, periodical, film videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported in 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 interstate or foreign commerce by any means, including by computer; or

vi. knowingly distributes, offers, sends, or provides to a minor any visual depiction, including any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, where such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct -

1. that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer;
2. that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer; or
3. which distribution, offer, sending, or provision is accomplished using the mails or by transmitting or causing to be transmitted any wire communication in interstate or foreign commerce, including by computer,

- for purposes of inducing or persuading a minor to participate in any activity that is illegal.

5. Per Title 18, U.S.C., § 2256(1), the term "minor" means any person under the age of eighteen years.

6. Per Title 18, U.S.C., § 2256(2), term "sexually explicit conduct" means actual or simulated:

a. sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; or
b. bestiality; or
c. masturbation; or
d. sadistic or masochistic abuse; or
e. the lascivious exhibition of the genitals or pubic area of any person.

7. Per Title 18, U.S.C., § 2256(8), the term "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated

image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where -

a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or,
c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Qualification of Affiant

8. I am a Senior Special Agent with the Wisconsin Department of Justice, Division of Criminal Investigation (DCI), and has been so employed since 1991. I have extensive experience working complex criminal investigations, including Internet crimes committed against children, death investigations, cold case homicides, murder for hire, sexual assault, fugitive apprehension, and drug trafficking. I have specialized in working in an undercover capacity in several of those areas. I have received commendations for my work from various law enforcement officials and prosecutors, as well as organizations including the National Center for Missing and Exploited Children (NCMEC) and the Wisconsin Association of Homicide Investigators.

9. Since 1999, I have been assigned to the Wisconsin Internet Crimes Against Children Task Force (ICAC), which was developed pursuant to a federal grant received from the Office of Juvenile Justice and Delinquency Prevention and NCMEC. ICAC's primary responsibility is the investigation of sexual crimes committed against children through the use of a computer and the Internet.

10. As a member of the Wisconsin ICAC Task Force, I most often pose as an underage boy or girl on the Internet, have been responsible for the arrest of approximately 150 individuals from Wisconsin and across the United States, on charges including child enticement, sexual assault and attempted sexual assault of a child, traveling interstate with intent to have sex with a minor, use of a computer to facilitate a child sex crime, possession and/or distribution of child pornography, and exposure of a child to harmful materials or narration. I have worked jointly in the area of crimes against children with federal, state, and county prosecutors, as well as federal, state, county, and local investigators.

11. I have engaged in thousands of undercover on-line communications with suspected predators of children. I have participated in interviews and interrogations of approximately 200 individuals involved or suspected in the sexual abuse and/or exploitation of children. I have also participated in the preparation and/or execution of approximately 150 search warrants and consent searches involving those same offenses. I have testified in Wisconsin as an expert on the sexual exploitation of children on the Internet, and have provided advice and opinions in that area to law enforcement officers throughout Wisconsin and the United States. My expertise has been used to assist ongoing investigations and to develop affidavits in support of search warrants and subpoenas.

12. I have also instructed on the topic of sexual predators of children on the Internet to more than 180,000 people in Wisconsin and around the country, with audiences including law enforcement officers, public officials, attorneys, judges, child welfare advocates, social workers, correctional officers, teachers, education administrators, business professionals, parents, and students. My training and/or advice has assisted numerous law enforcement agencies in starting

and conducting Internet crimes against children investigations, which have resulted in dozens of arrests.

13. During my law enforcement career, I have received more than 420 hours of training on the sexual exploitation and abuse of children from federal, state, local, and private agencies, including the Federal Bureau of Investigation, the National Center for Missing and Exploited Children, the Wisconsin Division of Criminal Investigation, Practical Homicide Investigations, Inc., the American Prosecutors Research Institute, the Kenosha County Medical Examiner's Office, the Dallas Police Department, the Wyoming Division of Criminal Investigation, and Fox Valley Technical College, Appleton, WI; I have also attended the National Internet Crimes Against Children (ICAC) Conference in Dallas in 2004, 2005, and 2006, and the National ICAC Conference in San Jose, CA in 2007 and in Columbus, Ohio in 2008. My training has included online exploitation of children; possession, collection, distribution, and manufacturing of child pornography; working undercover on child exploitation cases; basic forensic computer examination; e-mail and Internet protocol number tracing; sexual assault and abuse of children; surviving and coping with the aftermath of sexual assault and exploitation; family/non-family abduction, child homicide, interviewing and interrogations, child prostitution, child sex tourism, and human trafficking.

Background Regarding the Seizure of Computers in Child Exploitation

14. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize the computer items described above to be processed later by a qualified computer expert.

15. Computer storage devices (like hard drives, diskettes, tapes, laser disks, USB devices and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

16. In order to locate contraband images, I know that a forensic preview of a suspect hard drive or other storage device can take place at the scene of a search; however, this preliminary search does not necessarily find all evidence about the nature and scope of the crime being investigated. Searching computer systems for all obtainable evidence is a highly technical process that requires expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files.

Background Regarding The Use Of Computers In Child Exploitation

17. Based on my training and experience, I know that the Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet.

18. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102.

19. Each time an individual connects to the Internet, the computer from which that individual initiated access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. 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. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

20. I know that ISP's do not keep IP records indefinitely and that the time such information is kept can range (depending on the ISP) from several weeks to several months or even longer. I know that IP information is one of many possible investigative leads to pursue in order to identify suspects in the online exploitation of children.

21. Photographs and other images, including those of child pornography, can be used to create data that can be stored in a computer. This storage can be accomplished using a "scanner", which is an optical device that can recognize characters on paper and, by using

specialized software, convert them to digital form. Storage can also be captured from single frames of video and converted to an image file. After the photograph or other image has been scanned into the computer, the computer can store the data from the image as an individual "file". Such a file is known an image file. Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

22. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail. I also know that in addition to images, a forensic computer examination can also recover saved and/or deleted text, including chat fragments, e-mails, e-mail addresses, screen names, or other data that corroborates crimes of child pornography and/or other forms of online child exploitation.

23. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called

"downloading." The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and or print out a hard copy of the image by using a printer device (such as a laser jet or inkjet).

24. Importantly, computer files or remnants of such files, including child pornography, can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

25. I know that the deletion of images and/or files of child pornography do not mean a crime or crimes have not been committed. For example, if a child pornography suspect

knowingly downloads contraband images, uses them (e.g. for sexual gratification, trading with others, for profit, etc.) and then deletes them, he was nonetheless in direct and immediate possession of those images at one time. I know there is a chance a suspect will delete images of child pornography to try to cover his tracks and/or avoid responsibility for his actions if detected by law enforcement, employers, spouses, etc; he also knows that a suspect can also transfer images from his hard drive to other more secure storage devices, enabling him to delete images from the hard drive to avoid detection, while still keeping the images in other places. This further supports the importance of searching for deleted images and/or files, because they can be evidence of knowledge and intent. The mere possibility that a perpetrator can delete images does not change his sexual appetite for children, or his propensity to use the Internet to seek more images to satisfy that appetite.

26. Based on my training and experience, I know the primary manner in which child pornography is produced, distributed, and possessed is through the use of computers and the Internet; the Internet has given these offenders unparalleled access and opportunity to obtain these images as never before in history. The numbers of investigations and arrests involving child pornography have soared by in Wisconsin and across the United States since the late 1990's. I know the capacity of computer hard drives, the ease of access and relative anonymity afforded the computer user permits individuals with an interest in child pornography to amass large collections of such materials; he also knows that the numbers of images and videos downloaded can vary, depending on the perpetrator. The materials they download can then be saved indefinitely on various electronic storage devices, as well as transferred from one storage device to another, and/or one computer to another.

27. Furthermore, each image is a digital duplicate of the computer original; therefore, a perpetrator's child pornography stash is not diminished if he or she distributes the pornography to others via computer. Internet access also allows the computer user to locate and communicate with others of similar inclination. Once contact is established, it is then possible to send text messages, e-mails, instant messages, and graphic images to others. These communications can be quick, relatively secure, and as anonymous as desired.

28. Based on my training and experience, I know that individuals involved in child pornography will use places that they consider private and secure to receive, download, store, and/or view pornographic images or video clips available on the Internet; most often the private and secure place is the individual's residence. In the hundreds of online child exploitation cases I have worked on or assisted with, I am aware of only a handful of cases where the perpetrator did not use his residence in some capacity to engage in this kind of criminal activity; in the vast majority of my cases, the perpetrator uses his residence.

29. Based on my training and experience, I know that individuals who have a sexual appetite for children often seek out, possess and/or collect child pornography, in that those images provide them with sexual stimulation, gratification, and satisfaction. Images of child pornography allow them to fuel their fantasies and validate their behavior, which society at large finds abhorrent.

30. I also believe that someone who knowingly possesses or attempts to possess child pornography has such an appetite, because sexual arousal is the most reasonable explanation to obtain those images. I have interviewed suspects who deny sexual interest, claiming something like "curiosity;" I believe explanations like that are self-serving statements and a refusal to

accept responsibility due to embarrassment or to avoid legal consequences. I know that the excuse of "curiosity" is not a defense for knowingly possessing child pornography.

31. Based on my training and experience related to child pornography investigations, including investigations of subjects who subscribed to website offering access to child pornography, I know that individuals who subscribed to such website are individuals who have a sexual interest in children and in images of children, and who download images and videos of child pornography.

Addressing Issues of Staleness as Related to Probable Cause

32. Based on my training and experience, I know that individuals who are involved with child pornography are unlikely to ever voluntarily dispose of the images they possess, as those images are viewed as prized and valuable materials; I also know that those individuals are likely to seek out additional images to satisfy their sexual appetites, and that their ability today to seek out and obtain additional child pornography is unprecedented because of the Internet. Furthermore, I know that individuals who have an appetite for child pornography are likely to always have that desire, and that such individuals often molest children as well.

33. For example, in 2004, I investigated a Waukesha resident, David C. Kanouse, after receiving credible information from an informant that Kanouse was once involved in child pornography and child molestation. The informant in that investigation, however, had not seen or heard from Kanouse for about three or four years. I was still able to independently verify much of what the informant said about Kanouse, and that Kanouse was still using the Internet. A search warrant was obtained, which resulted in the seizure of Kanouse's computer. An examination of that computer discovered hundreds of images of child pornography, as well as

videos of the same. Kanouse was charged with possession of child pornography, and further investigation resulted in multiple charges of exposing children to harmful materials (child pornography), second degree sexual assault of a child, and repeated sexual assault of a child. Kanouse pled guilty and in April of 2005 was sentenced to 20 years in prison.

34. I note another example in my investigation of Steven Takach of La Crosse, who was suspected of having an interest in child pornography. In March of 2002, I obtained a search warrant for child pornography at Takach's residence, and seized his computer. Takach was interrogated about his interest in child pornography, which he essentially minimized or even denied. The forensic examination of Takach's computers, when finally completed, found significant evidence to the contrary. In November of 2005, more that 3 ½ years after Takach was confronted by law enforcement, I obtained an arrest warrant for Takach for the child pornography he possessed in 2002. After Takach was arrested, additional investigation showed that Takach not only obtained a new computer, but that he sought out and possessed additional images of child pornography on his new computer. When asked about his continued interest in child pornography, one of the explanations Takach offered to me was, "I have issues."

35. I note another example in a child pornography investigation of Dominic Radanovich of Milwaukee, WI, in May of 2006. I received credible information that Radanovich had child pornography on his home computer, and obtained a search warrant. Upon execution of the warrant, DCI agents found Polaroid pictures of child pornography that Radanovich took of a 16-or-17-year-old boy in 1984, or approximately 22 years prior to the execution of the search warrant. The pictures were found in the top drawer of a dresser in Radanovich's bedroom, easily accessible and not hidden or abandoned in any way. In addition to the pictures, agents found the

boy's high school ID, and unidentified clippings of hair. The victim also disclosed he was sexually assaulted as a boy by Radanovich. A plea agreement resulted in Radanovich's conviction of misdemeanor sexual assaults and a 9-month jail sentence. This example demonstrates why I am requesting items in the search warrant in addition to the computer and related storage devices; he knows that perpetrators can have developed or printed pictures, magazines, films, videotapes, souvenirs of prior child victims, notes, and other non-electronic records that are evidence of child exploitation.

36. Additionally, I worked another child pornography initiative with ICE called Operation Falcon, between 2004 and 2007. The initiative involved suspects who made one or more purchase into commercial child pornography website. In the dozens of Operation Falcon cases worked by me, the last known access of child pornography website took place between one to nearly five years prior to the execution of the search warrants. These cases offer numerous examples of how those interested in child pornography are likely to continue to use the Internet, month after month, year after year, to obtain, view, and/or save more and more images

37. I note another example in my Operation Falcon investigation of 63-year-old Newton B. Tench of Pleasant Prairie, WI. In February of 2006, a search warrant was obtained for his residence, based on one credit card purchase of a one-month membership to a child pornography site www.darkfeeling.com, in April of 2003. DCI agents found that Tench had some 50 computers in the lower level of his home, along with binders full of printed images of child pornography. In his statement to DCI agents, Tench estimated that he had one-million images of child pornography and child erotica, and that he started obtaining them in 1980, while employed as a police officer in Waukegan, Illinois. A DCI computer forensic analyst reported

that Tench had the electronic storage capacity to support his claim. Tench was subsequently arrested, charged with 20 counts of possession of child pornography, convicted and sentenced to prison.

38. I note another example in an Operation Falcon search warrant I obtained for the residence of Joseph Dillon in Hudson, WI, in December of 2005. Upon execution of the warrant, Dillon told other DCI agents that he was tipped off about the bust of a child pornography website that he visited in 2003, and that police had his name. Dillon essentially stated that he took a box of CD's he burned with images of child pornography, and hid it in the woods for months, just in case police would question him. Dillon said that once he was comfortable enough time had passed, he brought the box back into his house. Dillon also continued to use the Internet to view and obtain more child pornography. Consequently, Dillon was arrested and charged with possession of child pornography.

39. My next example involves the arrest of Robert Splittgerber of Milwaukee, WI, in August of 2008. Splittgerber was identified by NCMEC in 3 Cyber Tips as a suspected distributor of child pornography, in addition to his credit card purchase of a one-month membership to a commercial child pornography website in August of 2006. During the execution of the search warrant, agents located a significant quantity of child pornography images and videos. Splittgerber commented to DCI that he liked the images and videos of children nude or involved in sexual activity and would become aroused and would masturbate to these images and videos indicating that becoming sexually aroused was the point of having the images. He said he was a pedophile, he liked children in a sexual way, and could not be treated or counseled to change his feelings and asked a rhetorical question if a heterosexual could be

counseled to become a homosexual. Spittgerber was charged with multiple counts of possession of child pornography and later convicted.

40. My last example involves the arrest of Smedley Butler of Manitowoc County, WI in May of 2009. Butler was identified by ICE as having purchased memberships into child pornography website in 2006 and again in 2008. I prepared a search warrant for Butler's residence, resulting in the discovery of child pornography. Butler was interviewed by law enforcement, and admitted to purchasing memberships to specific child pornography website. Butler stated he downloaded child pornography files, saved them to his computer, burned them to CDs, and then deleted the files from his computer hard drive.

Additional Factors Affecting Staleness Issues

41. I also know that computer technology is always improving, and that users often upgrade their computers or purchase new ones. I believe this factor does not diminish the probable cause for this warrant, because, as stated earlier, individuals involved in child pornography will likely always have that interest, save those images as prized and valuable materials, and seek out more images. I know, based on my training and experience, that when a new computer is purchased, a user often saves the hard drive and/or data from the old computer. Additionally, I knows that suspects are very likely to use a new computer just as they used an older one to access child pornography.

42. Furthermore, I know that computers have become common items in households across the United States, much like televisions and radios. With the exception of some convicted sex offenders as a condition of their sentence, I have never personally observed or heard of a situation where someone who has a computer and Internet access later gets rid of that technology

and the convenience it offers. I know that it is common for computer users to change their Internet service provider, for example from Time Warner to America Online or MSN, but that change has no impact on their ability to use the Internet. Additionally, computers provide not only Internet access, but storage capability for personal and business records, documents, photographs, music, etc., and have become a common part of everyday life for people who have them. Even if a person cancels or discontinues Internet service, the computer will almost certainly be kept for those other uses; for a child pornographer, a computer that is not connected to the Internet can still be used to view and/or store the images he already obtained.

43. I also note that because many child pornography investigations involve a long passage of time, targets of an investigation sometimes move away from the residence where law enforcement first became aware they obtained illegal images. I do not believe this diminishes probable cause, because computers are relatively expensive items which are kept by their owners. Computers are also easily transported from one residence to the next; obviously, when a computer is moved from one location to another, the contents of that computer go along with it, as well as other electronic storage devices of the user/users. I have obtained search warrants in the past under these circumstances which have resulted in arrests, charges, and convictions. Three examples are Eric Locke, described above; *State vs. William Hoelzl* in Milwaukee County, and *State vs. Kenneth McDonald* in Waukesha County. In the Locke case, he purchased membership into the child pornography website from his college dormitory in Mequon, WI, and continued his criminal activity at his residence in Butler; in the Hoelzl case, he was found with digital child pornography in his West Allis residence after he moved from his residence in Brookfield; in the McDonald case, he admitted having digital child pornography at his residence

in Oconomowoc, after he moved from his residence in Mukwonago. McDonald got rid of the child pornography when he suspected that police were investigating him. He was later convicted of 1st degree sexual assault of a child.

44. I also know, based on my training and experience, that a suspect's lack of a prior history of child-related sex offenses is not a determining factor in the outcome of these investigations. The majority of suspects investigated by me, who were arrested, charged, and convicted, had no prior record of child sex offenses. I know that the Internet now offers an avenue of accessibility to child sex offenders, especially for child pornography and child enticement, that was not available before the Internet. I also know that many convicted child sex offenders have had multiple victims over a period of many years before being caught. Many of those offenders are skilled in gaining the trust not only of their victims, but of parents, relatives, guardians, friends and co-workers, which allows them to victimize children without raising suspicions. I also know that many of these offenders have been caught as a result of investigations that began as child pornography investigations

45. I note that the initial lead described in this affidavit was sent to the Wisconsin Department of Justice by NCMEC in January of 2009. The passage of time is due to the limited time and personnel resources available to law enforcement to investigate all ICAC-related leads generated by many different sources. I and other members of the Wisconsin ICAC Task Force have many other investigations in addition to this one that they are required to respond to in the course of their duties.

Facts Establishing Probable Cause: Background of Investigation

46. On 01/11/2009, the National Center for Missing and Exploited Children (NCMEC) forwarded Cyber Tipline Report 652675 to the Wisconsin Department of Justice Internet Crimes Against Children (ICAC) Task Force. NCMEC received the tip from cooperating citizen witness A S of Flower Mound, Texas, after she returned from a family visit to Wisconsin for the Christmas holiday.

47. A S reported that she observed pornographic images on the computer of Jeffrey S. Schroeder, DOB XX/XX/1956, at his residence, 10417 256th Avenue, Town of Salem (mailing address Trevor), Kenosha County, WI. A S said the pornographic images were of friends , who now are adults, but were minors at the time the pictures were taken. She said that some of the pornographic photos were altered so that the juvenile faces of the girls were placed on adult bodies. A S also reported that she had a copy of the photos saved to a CD.

48. The following is a transcript of the question-and-answer exchange, via e-mail, between A S and the CyberTipline. The questions were asked by a NCMEC analyst, and the responses were provided by A S

1) When did you find these images?

I was visiting ( ) and ( ) over the holidays. They live with (Jeff Schroeder) and his girlfriend) and her teenage son (because going through a divorce. Jeff and I have been on good terms for a few years and he allowed me to stay at his house so I could visit with the kids. We all got along very well and were able to enjoy as a family. On 12/27, came to me and told me

about the pornography on Jeff's computer. She was very upset and wanted to talk with me about it.

2) Where were they on the computer? (inside a folder, on the desktop, name of the files)

showed me the file folders on his computer and on a flash drive he kept in his desk. asked me not to tell Jeff that she showed me. The pictures were in two folders named '1442 A' and 'normal'.

3) Was it a shared computer, one where you both had access to it?

I had asked Jeff if I could use his computer to print things from my email while I was visiting. I had his permission to use his computer.

4) How long ago do you believe the pictures were taken? And, how old are the girls now?

The pictures of) and her friends were taken when they were in junior high school about 9 years ago. The girls are now 20 - 22 years old.

5) Do you believe your took the photographs?

and her friends took the pictures of each other. Jeff made copies of the photos and scanned them into his computer and saved them to his flash drive in the folders that contained the pornography pictures. But I don't know when he did that.

If so, how did have access to your friends and do you believe the girls knew about the images?

. I moved out and our daughters) stayed in the house with Jeff. At one point one of girlfriends moved in for a while. was a

cheerleader and she would have her fellow cheerleaders and friends stay over night sometimes. Normal teenager stuff. From the some of photos they took they were goofing around in provocative ways but again they were only 12 and 13 years old and had no supervision because I was not living there any more. Jeff allowed the girls to do many things that I would not have allowed. The girls knew about the photos but I believe they did not know that Jeff make copies, scanned them into his computer and altered some to appear as if they were engaging in sexual activity. When I found out about the photos I burned them onto a CD and took it to show

They were extremely upset and angry at Jeff. They had no idea their photos were on Jeff's computer and that he was looking at them with sexual intent. I showed these to

because it involved them. If they and their friends were not involved I would not have shown the pornography to them. is 26 yrs old and will be 22 yrs old this month.

6) Did you find any other pornographic images on his computer of females that appeared under age?

Yes I believe that some of the other photos are of under age girls. I don't know who they are or where he got the images. He may have downloaded them from the internet.

7) Could you provide any information about the girls depicted in the images (name, age, location)?

I don't remember all , friends' names or where they are now but would probably be willing to cooperate in any investigation. I think they are all of legal age now. There are photos of both of , with their friends that were take several years ago. There are also photos of his girlfriend son birthday party from many years ago. There are nude photos of me from when we were . He opened the door to the bathroom one time after I

had taken a shower. There are photos of Jeff and engaged in sex. did not know he had set up a movie camera and filmed them having sex. was very upset and humiliated when she found out. She confronted him about it and he told her he was going to tell her.

8) Have /did you ever report this to law enforcement? If yes, which department?

I did not report this to law enforcement yet. I made several calls to clergy, help lines and friends to ask what they thought I should do. All said to report it. I asked both my if it was ok to report this to the authorities and they said it was ok with them. So this is the first step in reporting it. I feel I have a responsibility to report this since it involved underage girls and girls that we knew. and I asked Jeff to get help for his addiction. We told him that he was affecting and hurting the women in his family. I told him that I had concerns about little living with him. decided to move out right away and is staying at house until she finds an apartment. has decided to stay with Jeff because he told her he would seek help. He has not apologized to us and is still angry and blaming all of this on me. He does not know it was who told me. A holiday family story we won't soon forget. I still have a CD of the photos. Please let me know what the next steps are.

49. On April 6, 2009, I contacted A , who verified the information described above. She also agreed to turn over items she took from residence, 10417 256th Avenue, Trevor, WI, on December 27, 2009. She said the items included a CD of the pornographic images made with the faces of childhood friends.

50. On April 6, 2009, I. contacted the Flower Mound, TX, Police Department, requesting assistance in picking up evidence from the A S residence, and sending it certified mail to me at the Milwaukee DCI Office.

51. On April 20, 2009, I received a package from Detective Joe Adcock of the Flower Mound Police Department. The package included several items he obtained from A S including the CD she made from the computer of Jeffrey Schroeder on December 27, 2009, negatives, and a number of 35 mm prints developed from those negatives that Schroeder scanned to his computer, in order to cut-and-paste faces of friends into pornographic scenes.

Description of Images

52. On June 1, 2009, I interviewed G S , the of Schroeder in the Milwaukee DCI Office about the contents of the CD. She reviewed the CD with me and identified images including, but not limited to, the following:

#56: A cut-out picture of the face of her friend AK, when she was about 12 or 13 years old. She said AK lived in her neighborhood on Dunbar Road, Wauconda, IL, and that her father knew her. G said she was over at her house all the time.

I observed that the face of AK was placed on the body of what appeared to be an adult female with exposed breasts, who was ejaculated on by an adult male standing next to her. The male's face is blocked out by computer-generated effects. He is holding his erect penis, with semen coming out of it.

#96: A different cut-out picture of the face of her friend AK, when she was younger, perhaps in the 6th grade.

I observed this picture to be of the same couple in Picture 56, but in an earlier scene of their sex acts. The male is lifting up the top of the female, and he is standing next to her with his erect penis just above her vagina.

qw Another picture of AK, cut-out and pasted on the body of an adult female sitting in the passenger seat of a car at night time; the woman's breasts are exposed, with her left had covering the nipple area of her left breast; her right hand is placed in her crotch area over her vagina, as she is not wearing any panties. A dressed adult male is standing next to the car door with his erect penis in his left hand.

we A close-up of AK's younger face picture cut-out above her upper lip and pasted on the face of a woman who has an erect penis inserted into her mouth.

wq A picture of AK sitting down, with G S s pet dog in the foreground; computer generated effects have been used to cut and paste an exposed vagina to replace the clothing worn by AK

'_I A picture of another one of G S s friends, KW. She said KW went to school with her at Wilmot High in Kenosha County. In this picture she said KW is somewhere between 16 and 18 years old, and her picture was cut-and-pasted from a digital picture.

I observed that in this picture, KW's head was cut and pasted into a sex scene on a couch, where a naked woman is lying on her stomach, with a naked man straddled over legs, having vaginal or anal intercourse with her. The man's face was blocked out by a computer generated effect.

001 A cut-and-pasted picture of the face of another one of G S s friends, placed on the naked body of woman; the woman is standing up with her breasts and vagina exposed, as she pulls off her panties. G S could not remember the name of the girl, but estimated that the photo was taken when she was in about the 7th grade.

hg A cut-and-pasted picture of the face of KW, placed on the naked body of a woman lying on her side on a bed; the woman's buttocks and exposed vagina are the focal points of the image.

io A cut-and-pasted picture of the face of another one of G S friends, JM, when she was in 6th - 8th grade. The picture was pasted on the body of a naked woman, standing up, exposing her breasts and vagina.

iu Three cut-and-pasted pictures of the faces of three of G S friends: AK, JM, and TL, all of whom were in middle school. The faces are pasted on the bodies of three naked females, standing together, bathing in a shower stall; the breasts and vagina are exposed on the girl in the middle; the vagina of the girl on the left is partially exposed.

lkk A cut-and-pasted picture of the face of JM, when she was in about 6th grade. The picture was pasted on the body of a naked female, perhaps in her late teens, standing on a bedroom floor, balancing on her left leg; her breasts and vagina are exposed

nb2 A cut-and-pasted picture of the face of another one of G S s friends, KF; she said KF went to a Catholic grade school in Wauconda, and she appeared to be about in the 7th grade in the picture. The picture was pasted on the body of an adult woman standing up in a hallway, with an open jacket exposing her breasts.

nb3 Another picture of KF's face, cut-and-pasted, and placed on the body of a naked woman sitting on a desk; her legs are spread apart, exposing her vagina; her breasts are also exposed.

wee Cut-and-pasted pictures of three faces of girls on the bodies of women sitting on a couch; G S could not remember the name of the girl on the left; she said the girl in the middle was KF, and the girl on the right was TL. The woman in the middle is naked, exposing

her breasts and vagina; the other two women are lifting up their tops, as if to expose their breasts in the next scene.

7 Cut-and-pasted pictures of two girl's faces, on women's bodies, having group sex with an adult male lying on his back. G S identified the girl on the right of the picture as TL; this person is naked, exposing her breasts and vagina, straddling the man's face while he performs oral sex on her. The girl on the right is not known by G S; she appears as though she is the age of a middle school girl, and is clutching the erect penis of the man, performing oral sex on it.

ee A cut-out picture of TL's face on the body of an adult woman, lying down, whose breasts are exposed; a man standing over her face has ejaculated on her left breast and towards her face as he holds his erect penis in his right hand.

er G S identified the cut-out face of this girl as TL, and the cut-out face of the man in this picture as Jeffrey Schroeder. In the picture, TL's face is on the body of an adult woman, sitting on a bed, grasping the erect penis of man sitting next to her on the bed; her right hand is on the shaft, and her left thumb appears to be touching his scrotum. Schroeder's face is on another man's body who is wearing shorts and a short-sleeved short, with his penis sticking out of his shorts.

ere TL's face is cut-out and pasted on the body of a half-naked adult woman lying on her back on a bed; her breasts are exposed, and her legs are spread apart exposing her vagina; an adult man is kneeling next to her with his erect penis just under her right breast.

nb1 TL's face is cut-out and pasted on the body of a naked adult woman, standing up against a railing, exposing her breasts and vagina; she is grasping the erect penis of an adult man standing

next to her, and guiding his penis into her vagina; the man's face is blocked with a computer generated effect.

53. G .S also identified a number of 35 mm color prints, which were sent to me by A S included in the package with the CD. G S said those pictures were taken of her and her friends when they were in middle school and high school. I observed that the cut-out faces of children that were pasted into the adult pornographic scenes described above came from these 35 mm pictures. G S said she did not know how , Jeffrey Schroeder, got those pictures.

Identification of Victims

54. On June 15, 2009, I reviewed information that positively identified all five of the children whose images were cut-and-pasted into pornographic scenesby Jeffrey Schroeder. I did this with a records search of the Wisconsin and Illinois Departments of Transportation, using the first and last names of the victims as given by G S . I obtained their current addresses, and then compared their current driver's license photos with their childhood photos used in pornographic scenes. I observed that G S 's identifications were correct. The victims are identified as follows:

1. KAW, DOB: XX/XX/1987, Kenosha, WI
2. TML, DOB: XX/XX/1987, Wauconda, IL
3. KAF, DOB: XX/XX/1987, Crystal Lake, IL
4. ALK, DOB: XX/XX/1987, Wauconda, IL
5. JMM, DOB: XX/XX/1987, Fox Lake, IL

55. Additionally, on April 28, 2009, I sent a copy of all of the pornographic images obtained by A S to NCMEC to search its database for known child victims. On June 12, 2009, S/A received a report from NCMEC, which indicated that it identified three images of one identified child victim from the "Ballet Girl" series. The image is a color picture of a naked adolescent teenage girl, balancing on her left leg in a bedroom setting. She is wearing a yellow blanket draped over her shoulders, exposing her breasts and vagina.

56. I note that this image appeared in three different places in Schroeder's collection of images: as 1) a j-peg, 2) a thumbnail, and 3) an altered j-pg. In the altered image, the girl's face is cut out and replaced with the face of one of G S girlfriends, JM, when she was in about the 6th grade.

Role of Unwitting Informant: D P

57. On June 15, 2009, I conducted a telephone interview with A S She stated that she found the pornographic pictures already described in this case file on the laptop computer of Jeffrey Schroeder. As she reported to the Cyber Tip Line, she was told about the pictures on December 27, 2008, by Schroeder's girlfriend, D P

58. A S said D P told her about the images and then showed them to her on Schroeder's laptop in his bedroom. A S said D P also gave her a CD which A S used to make a copy of the images (later sent to me). A S said she also took Schroeder's flash drive from the residence, but she later returned it to him. She explained that when Schroeder found out that she took the flash drive, he took her cell phone. She said that in order to get her cell phone back, she had to return the flash drive, which she did. A S said she deleted the images on the flash drive before returning it. She said the

images were consistent with the images she found on his laptop computer, but was not sure if they were identical or if there were more or fewer in number.

59. A S said that the 35 mm pictures and negatives she sent to me were obtained by D . P She said D P told her that she found the pictures in Schroeder's bedroom dresser. A . S suspects that he made copies of the pictures from the negatives, perhaps on the date marked on the store photo envelope (July 17, 2007) and then scanned them onto his computer in order to manufacture the pornographic images she observed.

60. Despite the fact that D P reported Schroeder's activities to A S , both A S and G S reported to me that D P married Schroeder within the past several of months.

Schroeder's Response to Discovery of Images

61. On the day she found the images on Schroeder's computer, A S said she confronted him about it. She said she told him that she was concerned about him and wanted to get him help, and that she did not feel comfortable with him being around . A S said Schroeder first expressed surprise, then anger, and left the room. A S said she left the house and has not had a conversation with him since.

62. A S said that about a month later, her daughter L H (the baby's mother) said that Schroeder asked her if she wanted the laptop computer, referring to the same computer on which A . S saw the images. She said L H told him no. A couple of months later, A S said L H changed her mind and asked Schroeder for the laptop. He told L H that she could not have it, because he had not

yet deleted the pornographic images observed by A S She said that the laptop was Schroeder's own computer, and that he also owned a desktop computer in the house.

63. On June 22, 2009, I received copies of e-mails from A S regarding her contacts with various people involved in this matter, including Jeffrey Schroeder. According to A S , the following was sent to her by Schroeder on January 4, 2009, from his e-mail address of jade_26@lycos.com :

A S ,

I allowed you into my house so you could be a part of and life. Everything in this house was available to you to use. You went through my things without permission and found some items I am not proud of. I know it was my curse to deal with. Everyday I prayed to god to release me from this curse. It was working I was there.

You had no right to drag the children into this. It should have been handled as adults. Even with all the affairs, drug use, alcohol, cigarettes, abortion and mental illness you experienced you were allowed in private to seek help. I was not given that option. In your hysteria to brand me you gave no thought or cared what this would do to the family. You made sure everybody knows what happened your hate is unchristen. I will not judge you.

You have the material, taken without my permission and I'm sure you plan to use it against me as often as possible instead of allowing the healing to begin. Do what I did get rid of the material stop hurting the children. For the rest of my life I have to live knowing my children and grand-children will think of me as less than a loving person. You have now become the sole financial and responsible person in the children and grand-children's life. I regret forever the pain I caused my family.

Only god can judge me he knows the truth. As a christen I forgive you. I will never contact you again please do the same.

64. I note that in the above e-mail, in Paragraph 3, Line 2, Schroeder writes, "Do what I did get rid of the material stop hurting the children." I do not believe Schroeder got rid of all of the contraband images for two reasons: 1) As reported in Paragraph 55, Schroeder told that she could not get his computer because he had not yet deleted the images;

according to A S. ;, this happened anywhere from 2 to 3 months after December 27, 2008; 2) as first noted in Paragraph 32, I know that it is unlikely for those with an interest in child pornography to ever voluntarily dispose of the images they possess. I believe Schroeder has such an interest, as shown by his manufacturing and storing of images taken of friends between 8 to 10 years ago; furthermore, such images were found as recently as December 27, 2008, in folders specifically created by Schroeder to be a repository for them.

65. I also know that Schroeder spent a significant amount of time using computer software to scan, transfer, and cut-and-paste images for his sexual arousal, using pictures of specific children that he knew and spent time around. I believe these images are even more prized and valuable for Schroeder than images of child pornography of unknown victims. I therefore believe it is even less likely that Schroeder permanently destroyed those images, or at the least, he would likely have transferred them to another electronic storage device before even contemplating whether to delete them from his computer.

History of Computers in Schroeder Residence

66. During his interview of G 3 on June 1, 2009, I asked her about computers she observed in the residence at 10417 256th Avenue, Town of Salem (mailing address Trevor), WI. She said the last time she saw computers there was the last time she visited, around Christmas 2008. G S : said she observed two computers in the house at the time, including a desktop in the kitchen, and a laptop downstairs. She said Schroder was also likely to have a work laptop computer somewhere in the house. G S : stated that in all of her years growing up, since Schroeder got his first computer when she was little, he has always been on the Internet and used a computer or computers regularly in the house. G

S(: said she did not know of a time when computers were not in the house in the last 8 or 9 years.

Verification of Schroeder's Residence

67. On June 29, 2009, at about 7 p.m., I conducted surveillance at 10417 256th Avenue, Town of Salem (mailing address Trevor), WI. He observed a vehicle with WI license plate number 714-FUL, which WI DOT reports as registered to Jeffrey S. Schroeder, DOB 10/16/1956, of 10417 256th Avenue, Town of Salem (mailing address Trevor), WI.

68. On August 25, 2009, I obtained utilities information for 10417 256th Avenue, Town of Salem (mailing address Trevor), WI. According to WI Energies Corporation, Jeffrey Schroeder has been the subscriber there since February of 2008.

69. On June 30, 2009, I checked whitepages.com, which reported that Jeffrey S. Schroeder is the occupant at 10417 256th Avenue, Town of Salem (mailing address Trevor), WI.

70. On June 30, 2009, I checked the Kenosha County website for information about 10417 256th Avenue in the Town of Salem (mailing address Trevor), WI. I observed the following:

Municipality: Salem

Parcel Number: 66-4-120-271-0230

Property Address: 10417 256TH AVE

Mail-To Address: Jeffrey S Schroeder
10417 256th Ave
Trevor, WI 53179

Conclusion

71. Based on his training and experience, and the totality of this investigation, I believe that evidence of the crime of possession of child pornography is likely to be found at Schroeder's residence, 10417 256th Avenue, Town of Salem (mailing addressTrevor), Kenosha County, WI. I believe Schroeder has demonstrated an ongoing interest in child pornography by scanning 35 mm pictures of childhood friends, transferring them to his computer, and cutting-and-pasting their faces into adult pornographic scenes for his sexual arousal. I believe that this took a significant amount of time, thought , and planning, based on the number of images described in this affidavit, and the number of victims (5). These are in addition to the one other victim that was identified by NCMEC amongst Schroeder's collection.

72. Furthermore, I note that these images were copied from his laptop computer by A S on December, 2008, in file folders that were specifically created by Schroeder for his handiwork. As Schroeder wrote in an e-mail to A S about one week after she confronted him, he admitted she "... found some items I am not proud of. I know it was my curse to deal with. Everyday I prayed to god to release me from this curse..."

73. Also, as I stated first in Paragraph 32, individuals who are involved in child pornography are likely to keep their images; furthermore, I believe they are likely to continue to use the Internet to obtain more images to satisfy their sexual appetite for children, and that this criminal activity is highly likely to take place in the home. Therefore, I do not believe that probable cause is diminished because A S observed the images on Schroeder's computer approximately 8 months ago.

74. Based upon the facts as stated in this affidavit, there is probable cause to believe that evidence of the stated violations is located within the residence located at 10417 256th Avenue, Town of Salem (mailing address Trevor), Wisconsin.

75. I respectfully request that this Court issue a search warrant for the items listed in "Attachment A" which is attached to this affidavit.

ATTACHMENT A - Items to be Searched and Seized

1. Images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

   a. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, MPG, MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CDs, DVDs, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography.

2. Any and all computer passwords, password files, text keys, encryption codes and other data security devices designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code.

3. Any originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C., § 2256.

4. Any motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C., § 2256.

5. Information or correspondence pertaining to the possession or attempted distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C., § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

   a. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, Internet history, establishing possession, access to, or transmission through interstate or foreign commerce, including by U.S. mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C., § 2256.

   b. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by U.S. mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C., § 2256.

6. Any and all magazines, books, periodicals, or any other types of printed material that may contain evidence of violations of Title 18, U.S.C., § 2252A, or other violations related to the sexual exploitation of children.

7. Sexual paraphernalia or objects that may be evidence of violations of Title 18, U.S.C., § 2252A, or other violations related to the sexual exploitation of children.

8. Any and all records in any form or other items or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence including, but not limited to, sales receipts, invoices, bills for Internet access, and handwritten notes.

9. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.