

AFFIDAVIT IN SUPPORT OF APPLICATION UNDER THE ALL WRITS ACT FOR COMPELLED DECRYPTION

I, Brett E. Banner, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been employed with the FBI since November 1999 and I am currently assigned to the Milwaukee Division Child Exploitation Task Force (CETF). I am charged with conducting investigations of violations of Federal Law including the receipt, possession, distribution, and production of child pornography; coercion and enticement of a minor to engage in sexual contact; and, the sexual exploitation and sexual abuse of minors. I have gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with law enforcement partners in local, state and federal law enforcement agencies. Prior to my assignment with Milwaukee I was assigned to the Detroit Division where I was the administrator for the Mid-Michigan Area Computer Crimes Task Force from June 2004 to September 2009. This task force primarily investigated crimes against children matters. I have also been employed in the State of Wisconsin as a certified law enforcement officer from 1993 to 1999.
2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.
3. This affidavit is being submitted in support of an Application for an order compelling Jeffrey Feldman to provide the decrypted contents of the seized storage media and to allow law enforcement access to the encrypted contents of his personal data storage system in order to effectuate a search warrant ordered by this Court, 13-M-421 (hereinafter "Warrant.")
4. The Application for the Warrant and supporting affidavit are restated as part of this Affidavit and, to my knowledge, nothing from the original showing of probable cause has been disproven by the subsequent investigation.
5. The Warrant was issued authorizing the FBI to search the residence of Jeffrey Feldman (hereinafter "Feldman") at 2051 South 102nd Street, Apartment E, West Allis, Wisconsin

(hereinafter "Premises"), for evidence of violations of Title 18, United States Code (USC) 2252A, entitled "Certain activities relating to material constituting or containing child pornography."

6. Based upon the information summarized in this affidavit, I have reason to believe that evidence of such violations may be present in the storage media recovered from the search of the Premises.
7. The information supplied in this affidavit is based upon my investigation and information provided 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 an order for compelled decryption of currently-encrypted contents, I have not set forth every fact related to or otherwise the product of this investigation.

DEFINITION OF TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:
 - a. Data Storage System: A data storage system is a collection of all of the different storage devices one uses to contain and access one's personal information. A data storage system may contain numerous devices that store data in a variety of media. The defining characteristic of a data storage system is that data is shared, copied and transferred between the different devices included in the system. Because the different devices of a data storage system are interconnected, whether a specific piece of data (a document, picture, video, etc.) is stored on one device or another is largely a result of the organizational preferences of the owner or administrator of that system.
 - b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.
 - c. Peer-to-Peer Network (P2P): A P2P network allows users to trade digital files through a worldwide network formed by linking computers together via special software. Typically, users perform a keyword search to locate files, and the files can then be downloaded from any users in possession of those files. Users cannot send or receive files without consent.
 - d. Encryption: Encryption is the process by which data is encoded, and thus hidden or obscured from view by those not privy to the encryption key. Encryption can be as

simple as replacing each letter with a corresponding number (thus “a” would be rendered as “1” and “b” as “2”) but can be incredibly complex. Modern electronic encryption measures can render entire data storage systems impossible to view unless the correct password or biometric signature is input into the system. “Breaking” digital encryption, while possible, is extremely time consuming and resource intensive. Inexpensive, or even free, encryption software is widely available over the internet, is extremely effective and is becoming more and more commonplace on average consumer computers.

- e. Password: A password is usually some combination of letters and numbers that, when correctly entered into the encryption program, will run a program which will decrypt the contents of encrypted storage media. The input of other, non-alphanumeric data can be used as a password including biometric data, though such programs are still relatively rare. At present, most passwords are short words or phrases and numbers. Usually, these phrases and numbers are random or have little more than mnemonic value. Once a password is chosen by a user, it is recorded into the base code of the encryption program where it is then itself encrypted.

EXECUTING THE SEARCH WARRANT AS ORDERED BY THE COURT

- 9. On January 22, 2013, a warrant was issued which ordered the FBI to enter and search the Premises for evidence of violations of Title 18, United States Code (USC) Section 2252A, entitled “Certain activities relating to material constituting or containing child pornography.”
- 10. In accordance with that warrant, law enforcement entered the Premises on January 24, 2013 and began a search for, *inter alia*, records, computers and electronic storage devices containing child pornography.
- 11. During that search your affiant conducted an abbreviated interview with Feldman before he invoked his right to counsel and indicated he did not wish to speak to law enforcement anymore. I have been advised that Feldman has since retained counsel.
- 12. Because evidence of violations of 18 USC § 2252A is often stored in data storage systems, and because the seizure of electronic storage media was authorized by the Warrant, law enforcement seized a number of electronic devices together constituting a data storage system. A list of the pertinent storage devices include the following:
 - a. A Dell Inspiron 530, serial number HYX4VF1, located in Feldman’s living room.

- b. Western Digital My Book Essential, serial number WMC1T0358400, connected to a Dell Inspiron 530 located in Feldman's living room.
 - c. Western Digital My Book, serial number WMAZA0052668, located in Feldman's living room.
 - d. Western Digital My Book, serial number WCANU1155143, located in Feldman's bedroom.
 - e. Western Digital My Book, serial number WCAVY0868325, located in Feldman's bedroom.
 - f. Western Digital My Book, serial number WCASJ0087391, located in Feldman's bedroom.
 - g. Western Digital My Book, serial number WCASJ0854891, located in Feldman's bedroom.
 - h. MadDog External USB Drive, serial number 3JT4B7LH, located in Feldman's bedroom.
 - i. Western Digital My Book, serial number WCAZA0078782T, located in Feldman's bedroom.
 - j. Western Digital My Book, serial number WCAZA0078878T, located in Feldman's bedroom.
 - k. Western Digital My Book, serial number WCAPW4354447, located in Feldman's bedroom.
 - l. Western Digital My Book, serial number WCASJ1003049, located in Feldman's bedroom.
 - m. Western Digital My Book, serial number WCAPW0572841, located in Feldman's bedroom.
 - n. Western Digital My Book, serial number WMC1T0276658, located in Feldman's living room.
 - o. Maxtor Black Armor External Hard Drive, serial number 2HC04653, located in the pocket of a jacket in Feldman's closet.
 - p. Maxtor Black Armor External Hard Drive, serial number 2HC0491M, located in the pocket of a jacket in Feldman's closet.
13. Five of the recovered storage devices (d, f, g, h and l, above) have been wiped and all traces of electronic data on them are irretrievable.
14. Two of the storage devices (a and k, above) were not encrypted.

15. A forensic analysis of the remaining nine storage devices (b, c, e, i, j, m, n, o and p, above) shows that they contain data but the data is inaccessible due to encryption.
16. Additionally, agents recovered other passwords that have been used by Feldman. These passwords tend to be some combination of letters from his first name, letters from his last name and arbitrary number values. The use of this combination of letters and numbers makes it difficult for law enforcement to crack the encryption.
17. The encryption protocols used by Feldman to encrypt his data appear to be of the sort that will lock or damage the information contained therein if too many incorrect password guesses are made. For example, the user manual for the My Book Essential external hard drives contains the following statement, which in the original text is both highlighted and bold, "CAUTION! The WD SmartWare software uses your password to electronically lock and unlock your drive. If you forget your password, you will not be able to access the data that is on your drive or write new data to it. You will have to erase the drive before you can use it again."

ENCRYPTION HAS IMPEDED THE FBI'S ABILITY TO CARRY OUT THE COURT-ORDERED WARRANT

18. The Warrant ordered law enforcement to search for records containing child pornography. Based on my knowledge and experience, I know that individuals who receive and distribute child pornography usually maintain their illegal files on electronic data storage systems.
19. The Storage System is encrypted, making it difficult or impractical to access the files and information that the court has ordered law enforcement to recover.
- a. Feldman's data storage system has a capacity of approximately 19.56 terabytes.
 - b. Of those 19.56 terabytes, approximately 15.64 terabytes (or approximately 80%) are encrypted.
 - c. One terabyte of data storage can contain approximately 220 million pages of text at 5,000 characters per page. For comparison, the United States Library of Congress printed collection is equivalent to 10 terabytes of information.

20. Law Enforcement has already spent a great deal of time and resources attempting to recover the files and information as directed by the court.

- a. Examiners and agents assigned to the FBI -Milwaukee 's Computer Analysis Response Team (hereinafter "CART") have spent over ten weeks working on decrypting Feldman's storage devices. Their efforts, thus far, have been unsuccessful.
- b. Additionally, FBI – Milwaukee enlisted the assistance of the FBI's Cryptologic and Electronic Analysis Unit in an effort to decrypt Feldman's storage devices. Despite working on decrypting Feldman's storage devices for approximately eight weeks, their efforts have also been unsuccessful.

21. Attempts to break encryption on computer systems can put at risk the data that is being decrypted and the hardware on which that data exists.

- a. Some encryption programs are set up such that if more than a certain number of incorrect guesses are entered as to the password, the device locks up, deletes its contents or even self-destructs.
- b. In the event information cannot be extracted via software means, a more invasive procedure would be to remove the micro-processor chips from the device, thus destroying the hardware while attempting to recover the password for the device.
- c. Loss of data incidental to the decryption process could be severely detrimental to an FBI investigation, because the lost data might have been useful, probative evidence.
- d. Potential damage to the hardware and the potential loss of data could lead to significant financial hardships for the owner of said devices because storage media itself can be expensive, as can be the data one stores on such media.

22. The FBI uses evidence of child pornography to track down victims and to stop their further abuse. If the FBI is not given the passwords to the Storage System, the decryption process may take a great deal of time and may slow the FBI's efforts to stop the further abuse of children.

THE INVESTIGATION HAS REVEALED EVIDENCE OF CHILD PORNOGRAPHY ON THE SEIZED STORAGE SYSTEM

23. A forensic analysis of the nine encrypted drives (b, c, e, i, j, m, n, o and p, above) shows that they contain data.

24. Analysis of the unencrypted portions of the storage system (a and k, above) revealed links to the encrypted portions that strongly indicate the presence of child pornography.
25. During the search of Feldman's Dell brand desktop computer, model Inspiron 530 (a, above), FBI – Milwaukee's CART examiners found a Peer-to-Peer software program called eMule. Within the eMule program, log files indicated that 1009 files were received, distributed or stored using eMule. These files had titles mainly indicative of child pornography. A representative sample of the file names is as follows:
- a. Pthc - !!!New Fucking 7 Yo Little Girl Hard Weekend3.mpg
 - b. Childlover Pedo Rape 11Yo Nude Video Angels Pthc R@Ygold 13YoLolitas R@Ygold Orgy 1Hr Film Webcam Pedo 15Yo Teen.avi
 - c. BoyLove – cute little 3Yo Toddler Boy with man 4 yo with sound rbv hmv gay boys young kiddie golden bibcam.mpg
 - d. (Pthc) Open – f06 – Daughter (12 Yo) With Mum & Brother (10Yo), Spread Pussy With Dildo & Mum's Tit, Fisting Mum, Fucked By Brother, & Peeing.mpg
 - e. Yoboy-Man-10Yo-Blonde-Boy-Sucks-And-Is-Anal-Fucked-15m35S.avi
 - f. Tara 7Yo Girl-Eat Cum-Pthc.avi
 - g. Toddler 7Yo Girl 3Yo Sucking Pacifier Shows Pussy And Gets Cock Tip in Kleuterkutje.mpg
 - h. 7Yo Babyj Spread & Fucked Good By Man With Big Dick! He Cums Inside Her & On Her Belly! (Pthc preteen).avi
 - i. Pthc Pedo New Childporn Private Daughter Torpedo Ranchi Lolita – 4Yo Melinda 128276421930 Onionib.jpg
 - j. Pedo – 6Yo Boy
26. During their analysis of the Dell Computer (a, above), FBI Milwaukee's CART examiners found evidence that selected files had been downloaded to various drives connected to the Dell Computer. The eMule peer-to-peer program default download location was set to

"F:\C\eMuleDownload" and the eMule Temporary directory was set to "F:\C\eMuleTemp." A representative sample of the downloaded files is as follows:

- a. F:\C\eMuelCopy\!!((Illegal) Cute 12 Year Old Being Taught By Daddy – Fisting Incest Child Teen Preteen Lolita Young Gay Portn Beast Peep Mpeg.mkv
- b. F:\BA\A\eMuelCopy\!!RR@Ygold – Vicky, 10 Yo Boy And 9 Yo Girl Do It And Dad Joins In.mp4
- c. F:\C\stor1\!BOB! AviFiXP Vichatter Webam Pt 2011 11 Yo & 10 Yo Sisters!.avi
- d. I:\A\1-2009 Sorted \Jeffy –reviewed all pics\[boy+Man](((Pthc)))((Boylove)) Sweet Peeter Man & Boy.divx
- e. G:\testPicksXXX\Brea Bennett\GroupNew155xcsvpar2vfd003162\200606_Brea_Bennett_130.jpg

27. Your Affiant is aware through training and experience that several terms listed in the log files are routinely used as codes by those involved in child pornography to describe certain illegal depictions of child pornography. More specifically:

- a. The term "pthc" is an abbreviation for "pre-teen hard core;"
- b. The term "yo" is "years old;"
- c. The term "R@ygold" was the name of a specific set of child pornography films from the 1970's and has been attributed as a nickname for Richard Goldberg, a convicted sex offender and former fugitive on the FBI's Ten Most Wanted List;
- d. The term "lolita" is a term that has been used to describe a prepubescent or adolescent girl;
- e. Terms such as "ranchi torpedo" and "kleuterkutje" can be entered as a keyword search into the Internet Crimes Against Children website to locate individuals who distribute child pornography;
- f. "Tara" is the name of an identified child pornography series involving a minor victim from the state of Georgia.

28. Through their analysis, FBI Milwaukee's CART examiners also determined the following about the drives mentioned above:

- a. "I" drive corresponds to the Maxtor Black Armor drive with either serial number 2HC04653 (o, above) or serial number 2HCO491M (p, above). Both serial numbers are

listed in the Dell computer Registry as mounted/connected drives. Recent link files on the Dell computer, with names indicative of child pornography, also contain drive "I" with a volume name "Black Armor."

- b. "F" and "G" drives may correspond to any of the mounted/connected drives to the Dell computer. Seven different Western Digital hard drives were listed in the Dell computer Registry as mounted/connected drives. Recent link files on the Dell computer, with names indicative of child pornography, also contain drive "F" and "G" with non-specific volume names.

29. In sum, the investigation has so far revealed that Feldman's Dell desktop computer used eMule to download child pornography, and then the child pornography was saved to the encrypted drives listed above.

FELDMAN HAS EXTENSIVE COMPUTER KNOWLEDGE AND IS THE ONLY PERSON WHO HAD CONTROL OF THE SEIZED STORAGE SYSTEM

30. Your affiant believes that Feldman is the only person who had access to his apartment, his property, and the contents of the data storage system.

- a. Feldman stated to your affiant that Feldman has lived at his current residence for the past fifteen years, and that he is the sole occupant of the residence. After he made this statement he indicated that he wished to speak with an attorney and no further questions were asked of him.
- b. Your affiant has been informed by fellow agents that they reviewed the tax records for the premises and found that Feldman is the only person who is listed as paying taxes at the Premises.
- c. Your affiant has been informed by fellow agents that they interviewed the postal carrier and were been informed that Feldman is the only person receiving mail at the Premises according to the area postal carrier.
- d. The Dell computer's login screen shows only one username, "Jeff," which indicates that Feldman was the only user of the computer.

31. Feldman has unique knowledge and abilities to work with computers and to use encryption.

- a. Feldman is a Senior Software Development Engineer at Rockwell Automation in Milwaukee, Wisconsin where he has been employed for over 22 years. A review of a sample of Feldman's performance evaluations indicate that over the years his overall work has been ranked as "high," "exceeds expectations," or "outstanding."

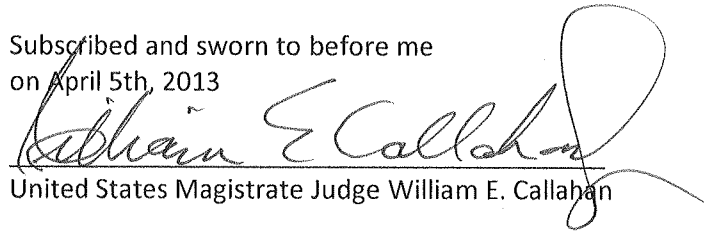
- b. On 09/29/2010, Feldman, along with co-inventors, filed for a United States patent, application number 12/893,815, publication number US 2012/0079003 A1, for a "System and Method for Interfacing with an Enterprise Resource Planning System."
- c. Feldman also graduated with a Bachelor of Science degree in computer science from the University of Wisconsin-Madison in 1990.

Respectfully submitted,



Brett E. Banner
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 5th, 2013



United States Magistrate Judge William E. Callahan