

Approved:

ANDREW D. GOLDSTEIN/LEE RENZIN  
Assistant United States Attorneys

COPY

Before:

HONORABLE LISA MARGARET SMITH  
United States Magistrate Judge  
Southern District of New York

14 MJ 145

----- x

COMPLAINT

UNITED STATES OF AMERICA :

-v.- :

BRIAN FANELLI, :

Defendant. :

Violation of 18 U.S.C.  
§§ 2252A(a) (5) (B),  
(b) (2) & 2

COUNTY OF OFFENSE:  
PUTNAM

----- x

SOUTHERN DISTRICT OF NEW YORK, ss.:

JASON SAMUELS, being duly sworn, deposes and says that he is a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("DHS/HSI"), and charges as follows:

COUNT ONE

From at least in or about October 2013, through in or about January 2014, in the Southern District of New York and elsewhere, BRIAN FANELLI, the defendant, knowingly possessed, and accessed with intent to view, a book, magazine, periodical, film, videotape, computer disk, and other material that contained an image of child pornography that had been mailed, shipped and transported using a means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, to wit, FANELLI possessed in his residence in Putnam County, New York images of child pornography that he had downloaded from the Internet.

(Title 18, United States Code, Sections 2252A(a) (5) (B)  
and (b) (2).)

The bases for my knowledge and for the foregoing charge is, in part, as follows:

1. I have been employed as a Special Agent with DHS/HSI for approximately 12 years. I am currently assigned to the New York Office, Child Exploitation Group ("CEG"). I have participated in numerous investigations of the sexual exploitation of children in violation of federal law. I have gained expertise in the conduct of such investigations through, among other things, training in seminars, classes, and everyday work related to conducting these types of investigations. I have conducted or participated in the execution of search warrants; interviews of informants, cooperating witnesses, and other witnesses; and reviews of business and other records. In part through my training, education, and experience, I have become familiar with the manner in which acts of sexual exploitation of children are committed. I also have received training in the investigation and enforcement of federal child pornography laws and offenses in which computers are used as the means for receiving, transmitting, and storing child pornography, and I have participated in the execution of search warrants involving electronic evidence.

2. I have been personally involved in the investigation of this matter. This affidavit is based upon my conversations with other law enforcement officers and agents and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all of the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

#### DEFINITIONS

3. The following terms have the indicated meanings in this Complaint:

a. "Child Pornography," as used herein, means any visual depiction, the production of which involved the use of a minor engaged in sexually explicit conduct. See 18 U.S.C. §§ 2252, 2256(2), and 2256(8).

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

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

d. "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 persons. See 18 U.S.C. § 2256(2).

e. "Computer" 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. See 18 U.S.C. § 1030(e)(1).

#### TECHNICAL BACKGROUND

4. Based on my training, experience, and information related to me by other law enforcement agents, I know the following:

a. IP Address. An Internet Protocol ("IP") address is a unique numeric address used to identify a particular computer connected to the Internet. An IP address looks like a series of four numbers, each in the range of 0 to 255, separated by periods (e.g., 123.45.67.890). Every computer connected to the Internet must be assigned an IP address so that communications from or directed to that computer are routed properly.

b. The Internet. The Internet is a global network of computers and other devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when devices communicating with each other are in the same state.

c. Peer-to-Peer ("P2P") File Sharing. One form of Internet use is peer-to-peer file-sharing or "P2P," which allows users to collect and share large numbers of files containing music, text, graphics, images and movies, including child pornography. The use of P2P file sharing software is a standard mechanism for transferring files from one computer system to another while connected to the Internet. P2P file sharing software allows groups of computers using the same file

sharing network to connect directly with each other and to share files from one another's computer systems. The P2P network used by BRIAN FANELLI, the defendant, is referred to herein as the "P2P Network."

d. Upon enabling a P2P network on a computer, the software allows a user to search the P2P network for pictures, videos, and other digital files by entering text as search terms. For example, an individual looking for music files by a specific artist may enter a search term such as "Sinatra," and will receive nearly instantaneously a list of other P2P Network users that have music titles relating to Frank Sinatra on their hard drives that they have chosen to make available for sharing.

e. Because of their relative ease of use and perceived anonymity, many P2P networks provide readily available access to child pornography. I know from using P2P file sharing software that the search results presented to a user allow the user to select a file and then receive that file from other users around the world. I am aware that these users can receive the selected file from numerous sources at once.

f. On a P2P network, different copies of the same file may have different file names. However, each file has a corresponding hashed algorithm value ("hash value") which uniquely identifies it on the network. The hash value is often referred to as a digital signature, which is akin to a fingerprint. P2P software uses these hash values to determine whether files hosted on different computers with different names are, in fact, the same file.

g. By querying P2P networks, law enforcement personnel can compare the offered hash values with hash values that belong to videos or images of known child pornography. These known videos or images of child pornography have been compiled by law enforcement agencies during the course of separate and unrelated Internet child sexual exploitation investigations into a database readily accessible for law enforcement use.

h. One method employed by law enforcement agents to investigate crimes involving child pornography is the use of a tool known as "Investigative Software." Such software is designed by and for law enforcement and is only available to law enforcement officers who have attended the appropriate training and received a license to obtain and operate the software.

i. Investigative Software designed for the P2P Network can be used by law enforcement agents to obtain the IP addresses of computers that have the P2P Network file sharing software installed, and that have individual files available for download with hash values that correspond to files of known child pornography.

j. The Investigative Software designed for the P2P Network also can be used by law enforcement to download files from one specific user of the P2P Network. This is different from the consumer version of the P2P Network, which typically draws files from multiple users at one time, as noted above.

#### THE INVESTIGATION

5. From my training and experience, I know that the National Center for Missing and Exploited Children ("NCMEC") maintains a registry listing of, among other things, the hash values of computer files containing images believed to be child pornography. NCMEC also maintains a list of those files for which law enforcement has been able to specifically identify the minors depicted.

6. On or about November 9, 2013, law enforcement agents using the Investigative Software identified a computer at IP address 71.167.52.95 ("the Subject IP Address") as possibly being used to share child pornography files over the Internet using the P2P Network. On that date, law enforcement agents using the Investigative Software for the P2P network were able to determine that the computer with the Subject IP Address was using the P2P Network, under a particular "nickname" or user name ("Nickname 1"). Between approximately 12:32 p.m. and 1:04 p.m. on November 9, 2013, law enforcement agents downloaded a file with file name "yo jovencita 14.avi" directly from the computer with the Subject IP Address. In attempting to view the downloaded file ("File-1"), law enforcement agents were able to view only the initial screen image (depicting a person's neck and shoulder), after which the file stalled. However, the hash value of File-1 matched the hash value of a file located and maintained by DHS/HSI through other investigations of child exploitation offenses. The hash value of File-1 was also listed on the NCMEC registry of files containing images believed to be child pornography. In addition, law enforcement agents viewed the uncorrupted file in the possession of DHS/HSI and determined, based on their training and experience, that File-1 is a video of child pornography, depicting a female that appears

to be under the age of 18 undressing and inserting an object into her vagina.

7. On or about January 3, 2014, law enforcement agents using the Investigative Software for the P2P Network were able to determine that the computer with the Subject IP Address was using the P2P Network, this time under the nickname of "Nickname 2." Between approximately 11:49 a.m. and 12:27 p.m., law enforcement agents successfully completed a download of a file with file name "! new ! (pthc)veronika pthc 2007 nuevo 2 nenas 1.wmv" directly from the computer with the Subject IP Address. Agents viewed this file ("File-2") and determined, based on their training and experience, that File-2 is a video of child pornography, depicting two prepubescent female children, one who appears to be under the age of ten and the other approximately the age of twelve; the younger child is holding a cylindrical object that is inserted in the other child's vagina. The hash value of File-2 is listed on the NCMEC registry of images believed to be child pornography.

8. Also on or about January 3, 2014, between approximately 11:49 a.m. and 12:27 p.m., law enforcement agents completed a partial download of a file with file name "(((kingpass))) 10y touch pussy webcam 3.avi" directly from the computer with the Subject IP Address. In attempting to view the downloaded file ("File-3"), law enforcement agents were able to view only part of the file, depicting what appeared to be a prepubescent female beginning to remove her underwear, and then, after the file stalled, depicting what appears to be the female's vagina. As with File-1, the hash value of File-3 matched the hash value of a file located and maintained by DHS/HSI through other investigations of child exploitation offenses. The hash value of File-3 is also listed on the NCMEC registry of images believed to be child pornography. Law enforcement agents viewed the uncorrupted file in the possession of DHS/HSI and determined, based on their training and experience, that the file is a video of child pornography, depicting a female who is approximately 11-13 years old exposing her breasts and vagina to a webcam.

9. Using the Investigative Software for the P2P Network, law enforcement agents were able to determine that between on or about October 26, 2013 and on or about December 30, 2013, the computer with the Subject IP Address had downloaded from other P2P Network users, and made available to other P2P Network users through the computer's "shared folder"

on the P2P Network program, a total of at least 126 files and associated hash values (the "Shared Files").<sup>1</sup>

10. On or about January 7, 2014, I submitted the hash values of the 126 Shared Files to NCMEC for comparison against their registries. NCMEC advised that of the 126 Shared Files, 114 have hash values that were recognized as containing images believed to be child pornography; 11 of the Shared Files were recognized as having hash values of known identified child victims; and one file was not on any NCMEC registry.

11. In addition, I observed that many of the Shared Files have file names that by their title indicate an apparent connection to child pornography, including, among others, "(((kingpass))) 10y touch pussy webcam 3.avi"; "boy gay sexo infantil porno (37)(2).jpg"; "pthc - capb (little boy slowly fucks little girl).mpg"; "11 years old masha masturbate.avi"; "bibcam webcam ultimate 12 best boy suck & fuck(2).avi"; "13 and 12 year old brothers enjoy playing and sucking off each others dick.mpg"; "17 yo boy fuck 7 yo girl kdv.avi"; and "homemade (pthc) father with daughter 13y anal (inzest).wmv."

12. I have reviewed records obtained from Verizon, which list the account associated with the Subject IP Address as active, and identify the subscriber to the Subject IP Address as "Brian Fanelli." The address on the account is a residence in Mahopac, New York (the "Fanelli Residence"). An AOL email address (the "Email Address"), is listed as an associated email address on the account.

13. I know that the "Brian Fanelli" listed as the subscriber to the Subject IP Address is BRIAN FANELLI, the defendant, based on the following, among other sources of information:

a. I have reviewed a copy of the passport application for a Brian Fanelli, with the same Fanelli Residence address. The passport application lists "Police Officer" as the applicant's occupation and "Town of Mount Pleasant" as the

---

<sup>1</sup> I know from speaking with law enforcement agents that a P2P Network user's shared folder, which makes files accessible to other P2P Network users, can be populated either by downloading files from other P2P Network users - such downloaded files are automatically stored in a user's shared folder unless and until the user removes them from that folder - or by dragging files from another location on the user's computer into the shared folder.

applicant's employer. The application also lists the Email Address.

b. I have reviewed the Town of Mount Pleasant's website, which identifies BRIAN FANELLI, the defendant, as the Police Chief of Mount Pleasant.

c. I have reviewed records obtained from AOL pertaining to the Email Address, which reflect that the Subject IP Address is among the IP addresses used by the Email Address to access the Internet.

d. On or about January 15, 2014, law enforcement agents using a device to identify and detect the status of wireless network ("WIFI") connections in a given area were able to determine that the Fanelli Residence maintains a secure, password-protected WIFI connection, under the name "Fanelli."

14. On January 17, 2014, based in part on the information set forth above, I obtained a search warrant for the Fanelli Residence issued by United States Magistrate Judge Paul E. Davison.

15. On January 23, 2014, I, working with other law enforcement agents, executed the search warrant on the Fanelli Residence, where we encountered BRIAN FANELLI, the defendant. While executing the search warrant, I and other law enforcement agents located three computers inside the Fanelli Residence.

16. On January 23, 2014, at or about the same time that the search warrant on the Fanelli Residence was being executed, law enforcement agents working with DHS/HSI conducted an interview of the wife of BRIAN FANELLI, the defendant. FANELLI's wife told the agents, in substance and in part, that only she and FANELLI live at the Fanelli Residence, and that there are three computers inside the Fanelli Residence: a small laptop computer that she uses and two computers that are exclusively used by FANELLI.



17. On January 23, 2014, during the execution of the search warrant, I and other law enforcement agents conducted an interview of BRIAN FANELLI, the defendant. After being advised of his Miranda rights, FANELLI stated the following, in substance and in part:

a. FANELLI is the Chief of Police of the Mount Pleasant Police Department.

b. For more than one year, FANELLI has taught sexual abuse awareness classes to elementary and middle school-age students.<sup>2</sup>

c. Approximately one year ago, FANELLI began viewing child pornography using the P2P Network. FANELLI stated that at first, he viewed child pornography as research for the classes he was teaching, but shortly thereafter began viewing child pornography for personal interest.<sup>3</sup>

d. FANELLI identified certain search terms that he used to locate child pornography on the P2P Network; those terms are familiar to me, based on my training and experience, as search terms commonly used to locate child pornography on the Internet.

e. FANELLI admitted that after viewing images and/or videos of child pornography using the P2P Network, he would attempt to delete the images and/or videos from his computer and also employed software designed to delete from his computer any evidence of his use of the P2P Network.

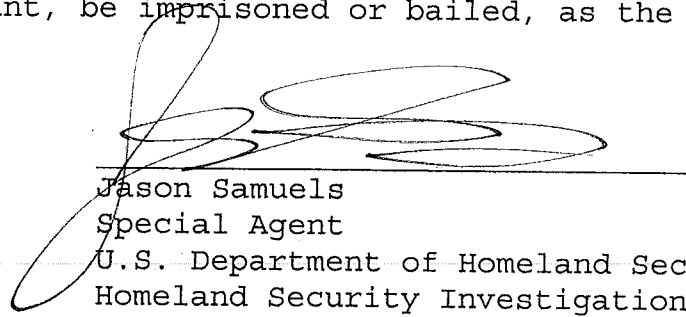
f. FANELLI identified the computer that he used to view child pornography using the P2P Network, which was not the small laptop computer that his wife told agents that she used.

---

<sup>2</sup> During the course of the investigation, I learned that FANELLI taught both sexual abuse awareness education and religious education classes to elementary and middle school students at a school in Westchester County.

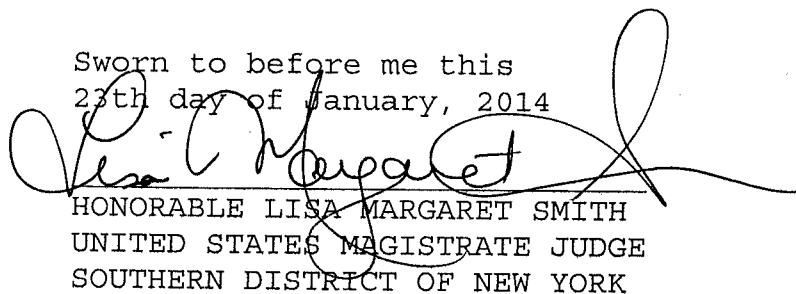
<sup>3</sup> I have spoken with an individual who was a designer of the Investigative Software used by law enforcement agents, and based on that interview, I know that the version of the P2P Network used by FANELLI is not the Investigative Software.

WHEREFORE, deponent respectfully requests that BRIAN FANELLI, the defendant, be imprisoned or bailed, as the case may be.



Jason Samuels  
Special Agent  
U.S. Department of Homeland Security,  
Homeland Security Investigations

Sworn to before me this  
23th day of January, 2014



HONORABLE LISA MARGARET SMITH  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK