

UNITED STATES DISTRICT COURT  
for the  
District of Rhode Island

FILED

2012 SEP 27 P 1:49

United States of America )  
v. )

GERALD SILVA )

Defendant )

U.S. DISTRICT COURT  
DISTRICT OF RHODE ISLAND  
Case No.

1:12 MJ 284 A

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of \_\_\_\_\_ in the county of Kent in the \_\_\_\_\_ District of  
Rhode Island, the defendant violated 18 U. S. C. § 2252(a)(2), an offense described as follows:

That, from in or about December 2010 to in or about April 2011, within the District of Rhode Island, the defendant, GREGORY SILVA, knowingly received, visual depiction(s), using any means or facility of interstate or foreign commerce; and that had been mailed; and that had been shipped or transported in or affecting interstate or foreign commerce, by any means including by computer; and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction was of such conduct.

This criminal complaint is based on these facts:

See attached Affidavit of U.S. Postal Inspector Michael J. Connelly.

Continued on the attached sheet.

  
Complainant's signature

Michael J. Connelly, U.S. Postal Inspector  
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/27/2012

  
Judge's signature

City and state: Providence, RI

LINCOLN D. ALMOND, U.S. MAGISTRATE JUDGE  
Printed name and title

**AFFIDAVIT**

I, Michael J. Connelly, being duly deposed, sworn and say:

1. I am an Inspector with the United States Postal Inspection Service (USPIS) assigned to the Boston Division, in Boston, MA, having been so employed since 2007. As a Postal Inspector, I am responsible for the investigation of Federal offenses involving the transportation, distribution, receipt, and sale of child pornography through United States mail in violation of Title 18, United States Code, Sections 2252 and 2252A. I have completed the USPIS Basic Inspector Training (BIT) program in Potomac, MD and have conducted and assisted in numerous investigations into the violation of both state and federal laws including mail & wire fraud, identity theft, and, child pornography. I am also an affiliate member of the Rhode Island Internet Crimes Against Children (ICAC) Taskforce and routinely work with agents, troopers, and officers with dozens of years of experience investigating crimes involving the sexual exploitation of children. I have received training in the investigation of crimes involving the sexual exploitation of children by attending both seminars and courses. I have investigated child pornography cases and related sexual offenses on a full time basis since approximately May 2011.

2. This affidavit is submitted in support of an application for a criminal complaint charging GERALD SILVA, 34 Morris Street, Coventry, Rhode Island 02816, with violations of

18 U.S.C. §2252(a)(2) (Receipt of Child Pornography).

3. The statements in this Affidavit are based on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint and arrest warrant, this affidavit does not contain every fact known to me with respect to this investigation. Rather, it contains those facts I believe to be necessary to establish probable cause for issuance of a criminal complaint for SILVA charging him receipt of child pornography in violation of 18 U.S.C. §2252(a)(2).

#### STATUTORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. §2252(a)(2), relating to material involving the sexual exploitation of minors. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving a visual depiction of a minor engaging in sexually explicit conduct.

#### DEFINITIONS

5. The following definitions apply to this Affidavit

a. "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).

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a

sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "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).

d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is

engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

#### **BACKGROUND OF THE INVESTIGATION**

6. On September 26, 2012 the United States applied for and obtained a search warrant for the residence of SILVA, that is, 34

Morris Street, Coventry, Rhode Island, 02816 (case number 1:12MJ281A) regarding the receipt and possession of child pornography in violation of Title 18, United States Code, Sections 2252 and 2252A. The warrant, and its accompanying application and affidavit, are attached as Exhibit 1, and are incorporated into this affidavit.

7. On September 27, 2012, pursuant to the authorized search warrant, myself and other ICAC law enforcement personnel completed a search at 34 Morris Street, Coventry, Rhode Island. During the search, officers encountered SILVA. He was advised of his constitutional rights, and agreed to be interviewed.

8. During the search, officers found at least twenty DVDs from the Toronto Company, as well as other DVDs that appeared to contain either child pornography or child erotica. Investigators found containers which purported to contain DVDs of the three video titles described in paragraphs 23, 25, and 27 of the Search Warrant. Two of these appeared to be unopened. The third, "Cutting Room Floor: Vlaviu," and further described in paragraph 25 of the Search Warrant, had been previously opened. I personally viewed a portion of this DVD, and it appeared to be the same video, containing images of minor males lasciviously exposing their genitals, that I viewed as described in paragraph 25 of the Search Warrant. Further, I also reviewed a portion of a second DVD that was at the premises, entitled "Raw Rewind

Vol. 2 [2-disc] (2011)". This video contained child pornographic images similar to those I viewed in the "Cutting Room Floor" DVD described above.

9. During the interview on the day of the search SILVA admitted to purchasing from the Toronto Company (described in Attachment 1, paragraph 11) numerous DVDs containing movie files and/or CDs containing photographs. The defendant admitted to knowing that the disks contained images of naked minor males, but considered the images as "nudism", rather than child pornography. He further admitted that the gmail account used to receive order confirmations from the Toronto Company, gerald.silva.home@gmail.com, was his email address, and that no one else used this email address. He admitted purchasing the 22 videos from the Toronto Company in his name and with his credit card, and to receiving them at his residence on numerous occasions via the U.S. mail. SILVA told investigators that he purchased all of these videos because he was preparing a "presentation" for law enforcement and/or state youth case workers. He admitted that he had never told anyone about his plans to use the videos he had purchased to make such a "presentation."

10. During the interview, the defendant told investigators that he is employed as a Probation and Parole Officer, employed by the Rhode Island Department of Corrections. He stated that

his present duties included supervising approximately 75 probationers/parolees who were primarily sex offenders.

CONCLUSION

11. Based upon the above information and your affiant's experience, your affiant respectfully submits there is probable cause to arrest GERALD SILVA, 34 Morris Street, Coventry, RI 02816, for violations of 18 U.S.C. §2252(a)(2) (Receipt of Child Pornography).

  
\_\_\_\_\_  
Michael J. Connelly  
United States Postal Inspector

Sworn and subscribed before me this 27<sup>th</sup> day of September 2012.

  
\_\_\_\_\_  
LINCOLN D. ALMOND  
UNITED STATES MAGISTRATE JUDGE

**DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT**

BY:  INFORMATION  INDICTMENT  COMPLAINT

CASE NO. 12 MJ 284 A

Matter Sealed:  Juvenile  Other than Juvenile  
 Pre-Indictment Plea  Superseding  Defendant Added  
 Indictment  Charges/Counts Added  
 Information

USA vs.

Defendant: Gerald Silva

Name of District Court, and/or Judge/Magistrate Location (City)

UNITED STATES DISTRICT COURT RHODE ISLAND  
 DISTRICT OF RHODE ISLAND Divisional Office

Name and Office of Person Furnishing Information on THIS FORM PETER F. NERONHA  
 U.S. Atty  Other U.S. Agency  
 Phone No. (401) 709-5045

Name of Asst. U.S. Attorney (if assigned) Terrence P. Donnelly

**REDACTED**

Alien (if applicable)

**PROCEEDING**

Name of Complainant Agency, or Person (& Title, if any)

United States Postal Inspection Service

person is awaiting trial in another Federal or State Court (give name of court)

this person/proceeding transferred from another district per (circle one) FRCrP 20, 21 or 40. Show District

this is a reprosecution of charges previously dismissed which were dismissed on motion of:

U.S. Atty  Defense

SHOW DOCKET NO.

this prosecution relates to a pending case involving this same defendant. (Notice of Related Case must still be filed with the Clerk.)

MAG. JUDGE CASE NO.

prior proceedings or appearance(s) before U.S. Magistrate Judge regarding this defendant were recorded under

Issue:  Warrant  Summons

Location Status:

Arrest Date \_\_\_\_\_ or Date Transferred to Federal Custody \_\_\_\_\_

Currently in Federal Custody

Currently in State Custody

Writ Required

Currently on bond

Fugitive

Defense Counsel (if any): \_\_\_\_\_

FPD  CJA  RET'D

Appointed on Target Letter

Place of offense RHODE ISLAND County

This report amends AO 257 previously submitted

**OFFENSE CHARGED - U.S.C. CITATION - STATUTORY MAXIMUM PENALTIES - ADDITIONAL INFORMATION OR COMMENTS**

Total # of Counts 1

Set	Title & Section/Offense Level (Petty = 1 / Misdemeanor = 3 / Felony = 4)	Description of Offense Charged	Felony/Misd.
1	18 U.S.C. § 2252(a)(2)	<sup>Receipt</sup> Possession of Child Pornography	<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
Max	Pen.: 20 yrs max (5 yr mand. min.) imprison-	ment; \$250,000 fine; up to life S/R; & a \$100 assessment.	<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
		Estimated Trial Days: 3	<input type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor

# EXHIBIT 1

512-239

FILED

SEP 26 2012

U.S. DISTRICT COURT  
DISTRICT OF RHODE ISLAND

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF RHODE ISLAND

IN THE MATTER OF THE SEARCH OF )  
34 Morris Street, )  
Coventry, Rhode Island )

1:12 MJ 281 A

MOTION TO SEAL

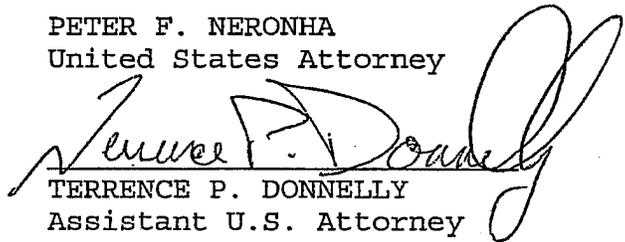
Now comes the United States of America, by and through its attorneys, Peter F. Neronha, United States Attorney, and Terrence P. Donnelly, Assistant United States Attorney, and moves that the accompanying documents (including the Application, Affidavit, Search Warrant, Attachments, and this Motion to Seal), be sealed until further Order of this Court. The United States makes this request based upon the fact that the disclosure of the above-referenced materials would potentially jeopardize the integrity of an ongoing investigation.

Respectfully submitted,

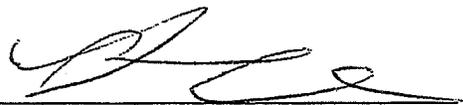
UNITED STATES OF AMERICA

By its attorneys,

PETER F. NERONHA  
United States Attorney

  
TERRENCE P. DONNELLY  
Assistant U.S. Attorney

SO ORDERED:

  
LINCOLN D. ALMOND  
UNITED STATES MAGISTRATE JUDGE

DATE: 9/26/12

AO 93 (Rev. 12/09) Search and Seizure Warrant

# UNITED STATES DISTRICT COURT

for the  
District of Rhode Island

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )  
34 Morris Street, Coventry, Rhode Island and further )  
described below )

Case No.

1-12 MJ 281A

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Rhode Island  
(Identify the person or describe the property to be searched and give its location):  
See Attachment A.

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):

See attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before \_\_\_\_\_ (not to exceed 14 days)

in the daytime 6:00 a.m. to 10 p.m.  at any time in the day or night as I find reasonable cause has been established.

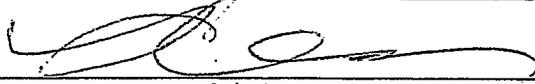
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge LINCOLN D. ALMOND  
(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)  for \_\_\_\_\_ days (not to exceed 30).

until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: 9/26/12 11:30 AM

  
\_\_\_\_\_  
Judge's signature

City and state: Providence, Rhode Island

LINCOLN D. ALMOND, U.S. MAGISTRATE JUDGE  
Printed name and title

UNITED STATES DISTRICT COURT

for the District of Rhode Island

REDACTED

In the Matter of the Search of )
(Briefly describe the property to be searched )
or identify the person by name and address) )
34 Morris Street, Coventry, Rhode Island and further )
described below )

Case No. 1:12 MJ 281A

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the District of Rhode Island (identify the person or describe property to be searched and give its location): 34 Morris Street, Coventry, Rhode Island, and further described in Attachment A, which is incorporated by reference.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): See Attachment B, which is incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- [x] evidence of a crime;
[x] contraband, fruits of crime, or other items illegally possessed;
[x] property designed for use, intended for use, or used in committing a crime;
[] a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 17 U.S.C. § 506, and the application is based on these facts:

See attached Affidavit of Postal Inspector Michael J. Connelly of the U.S. Postal Inspection Service.

- [x] Continued on the attached sheet.
[] Delayed notice of days (give exact ending date if more than 30 days: ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Michael J. Connelly
Applicant's signature

MICHAEL J. CONNELLY, POSTAL INSPECTOR
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/26/12

Lincoln D. Almond
Judge's signature

City and state: Providence, Rhode Island

LINCOLN D. ALMOND, U.S. MAGISTRATE JUDGE
Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Michael J. Connelly, being first duly sworn, hereby depose and state as follows:

1. I am an Inspector with the United States Postal Inspection Service (USPIS) assigned to the Boston Division, in Boston, MA, having been so employed since 2007. As a Postal Inspector, I am responsible for the investigation of Federal offenses involving the transportation, distribution, receipt, and sale of child pornography through United States mail in violation of Title 18, United States Code, Sections 2252 and 2252A. I have completed the USPIS Basic Inspector Training (BIT) program in Potomac, MD and have conducted and assisted in numerous investigations into the violation of both state and federal laws including mail & wire fraud, identity theft, and, child pornography. I am also an affiliate member of the Rhode Island Internet Crimes Against Children (ICAC) Taskforce and routinely work with agents, troopers, and officers with dozens of years of experience investigating crimes involving the sexual exploitation of children. I have received training in the investigation of crimes involving the sexual exploitation of children by attending both seminars and courses. I have investigated child pornography cases and related sexual offenses on a full time basis since approximately May 2011.
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. I have conducted and assisted in multiple investigations relating to the possession, receipt, transportation, distribution, and production of child pornography and obscene visual representations of the sexual abuse of children over the Internet and the US Mail. I have received training in investigations relating to the sexual exploitation and physical sexual abuse of minors. I have reviewed hundreds of images and videos of actual and suspected child pornography, child erotica, and obscene visual representations of the sexual abuse of children.
4. This affidavit is submitted in support of an Application for a Search Warrant authorizing a search of the entire residence located at **34 Morris Street, Coventry, RI 02816**, the "SUBJECT PREMISES", more particularly described in Attachment A, incorporated herein by reference, which is located in Rhode Island. The purpose of this application is to seize and search evidence, more particularly described in Attachment B, incorporated herein by reference, as evidence, fruits, and instrumentalities of criminal activity.
5. I have probable cause to believe that evidence, fruits, and instrumentalities of violations of 2252(a)(2) & 2252A(a)(2) (receipt of child pornography), and 2252(a)(4)(B) & 2252A(a)(5)(B) (possession of child pornography), are located within the SUBJECT PREMISES. I am requesting authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer(s) and digital media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of criminal activity.

6. The statements contained in this affidavit are based upon my personal observations, training and experience, and review of relevant records related to this investigation, as well as information provided to me by other law enforcement officers involved in this investigation to include Postal Inspector Brian Bone.
7. Postal Inspector Bone has been employed by USPIS since February 2007 and he is currently assigned to the U.S. Department of Justice's Child Exploitation and Obscenity Section in Washington, D.C. Postal Inspector Bone has participated in numerous investigations and search warrant executions involving child exploitation offenses. Postal Inspector Bone has received extensive training in computer forensics and digital investigations from the Treasury Computer Forensic Training Program, National White Collar Crime Center, and the International Association of Computer Investigative Specialists ("IACIS"), including specialized training on digital data recovery, and the investigation and analysis of e-mail communications and Internet activities, such as "Instant Messaging" programs, newsgroups, and forums. Postal Inspector Bone also has received training on the use of specialized forensic software programs, including I-Look, Encase by Guidance Software, and Forensic Tool Kit by Access Data. Prior to becoming a Postal Inspector, he worked as a sworn law enforcement officer within the State of Illinois for over 8 years and was employed during that time by the Office of the State's Attorney, Lake County, Illinois, and the Office of the Sheriff, Lake County, Illinois. In this position, he was assigned to the Cyber Crimes Division and the Child Exploitation Unit, which investigated child exploitation related offenses and various computer related crimes.
8. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2), 2252A(a)(2), 2252(a)(4)(B), and 2252A(a)(5)(b), are present in the SUBJECT PREMISES. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

#### RELEVANT STATUTES

9. This investigation concerns alleged violations of 18 U.S.C. §§ 2252(a)(2), 2252A(a)(2), 2252(a)(4)(B), and 2252A(a)(5)(b), relating to the sexual exploitation of minors.
  - a. Title 18 U.S.C. §§ 2252(a)(2) & 2252A(a)(2) prohibit a person from knowingly receiving or distributing any visual depiction involving the use of a minor engaging in sexually explicit conduct (child pornography) or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

- b. Title 18 U.S.C. §§ 2252(a)(4)(B) & 2252A(a)(5)(B) prohibit a person from knowingly possessing or knowingly accessing with intent to view any material that contains any visual depiction involving the use of a minor engaging in sexually explicit conduct, or an image of child pornography as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

### APPLICABLE DEFINITIONS

10. The following definitions apply to this Affidavit and its Attachments:
  - a. "Child" means "minor," as defined by 18 U.S.C. § 2256(1) (any person under the age of eighteen years).
  - b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
  - c. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
  - d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."
  - e. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
  - f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not

limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, cameras, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- j. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- k. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a

computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

- l. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
- m. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).
- n. "Producing," as used herein, is defined by 18 U.S.C. § 2256(3) (producing, directing, manufacturing, issuing, publishing, or advertising).
- o. A "record" means any communication, representation, information, or data. A "record" may be comprised of letters, numbers, pictures, sounds, or symbols.
- p. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).
- q. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- r. "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).

### **PROBABLE CAUSE**

#### **INVESTIGATION OF "Toronto Company"<sup>1</sup>**

11. In October of 2010, USPIS and the Toronto Police Service (TPS) began an investigation into a movie production company that operated a website offering DVDs and streaming videos (collectively "films") for sale. The majority of these films feature young boys and were marketed as "naturist films from around the world." TPS and USPIS determined that this production company, "Toronto Company", was located in Toronto, Canada and

---

<sup>1</sup> For purposes of the confidentiality and integrity of the investigations involved in this matter, specific names and other identifying factors have been replaced with generic terms.

was the subject of more than 20 complaints to the National Center for Missing and Exploited Children's Cyber TipLine regarding the sale of child pornography.

12. In October 2010, USPIS Inspectors accessed the Toronto Company's website ("www.[torontocompany].com") and were able to review film previews, website movie summaries, and customer ordering information. On six occasions between February and April, 2011, USPIS Inspectors from Brentwood, Tennessee conducted controlled purchases of DVDs via the Toronto Company's online ordering system. By way of example, one of the videos purchased from the Toronto Company via an undercover purchase was titled "Cutting Room Floor – Vlaviu." Toronto Company's website described this film as follows:

“we sweep up the cutting room floor to bring you tow action-packed discs of ooey-goey slippery goodness with Vlaviu and his friends, Lore and Luci! Like our original . . . this is all the footage that didn't make the cut over the last 2-years from our Boy Fights series! This two disc set features Vlaviu and his buddies going commando in a very unique way. They're sweet enough, but that didn't stop them from breaking out the sugary cupcakes and giving you a whole new perspective on nudist food fighting! One this is for sure . . . there's no laundry to do tonight!”<sup>2</sup>

13. The video depicts minor boys seen naked in an apartment living room setting eating desserts and other food. There are several close-ups of the minors' genitals and pubic area as they eat desserts and towards the end of the film several of the boys are seen sitting naked on the desserts and placing the remnants in their anuses.
14. Law enforcement determined that the Toronto Company has a shipping facility located in North Tonawanda, New York and that the undercover online orders were transferred from the Toronto Company to this New York based shipping facility for fulfillment. These undercover orders were then shipped from North Tonawanda, New York via USPS Priority Mail to a post office box in Nolensville, Tennessee.
15. TPS executed a search warrant on the Toronto Company's business premises on May 1, 2011 and seized hundreds of DVD movies, photo DVDs, computers, and business records, including customer shipping labels and customer order histories. Many of the DVD movies included the exhibition of the genitals of nude minors. Law enforcement determined that these films were being shipped to customers worldwide, including hundreds of individuals residing in the United States. Law enforcement also determined that for those orders placed from the United States, the Toronto Company would fill those orders via USPS Priority Mail.
16. The Toronto Company, as well as its two operating principals were subsequently charged and are being prosecuted in Canada for child exploitation offenses, including the production and distribution of child pornography.

---

<sup>2</sup> The Toronto Company's website is quoted verbatim.

### IDENTIFICATION OF GERALD SILVA

17. Law enforcement conducted a review of certain records contained in the "Toronto Company's" customer database and located one customer, Gerald SILVA, (SILVA,) with an address of 34 Morris Street, Coventry, RI 02816 and determined that on multiple occasions, SILVA purchased child pornography from this company's website.
18. Law enforcement extracted the customer invoices and purchase summary from the database, which details the purchase transactions made by SILVA. A summary review of the transactions showed that between October 2010 and April 2011, SILVA purchased 75 different titles in 22 separate orders via the "Toronto Company's" website, totaling \$1,589.00 in United States currency.
19. Each of the 22 transactions reviewed by USPIS employees related to this individual showed a billing and shipping address of 34 Morris Street, Coventry, RI 02816 and a telephone number of [REDACTED].
20. The customer records related to SILVA show that the purchaser used the email address of gerald.silva.home@gmail.com for receipt of confirmation in the transactions.
21. In addition to the contact information discussed above, the business records associated with each customer transaction also captured the date an order was placed and the specific video or DVD requested, each of which contained a corresponding product identification number. Of the titles which were offered for sale, some contained a single video file and others contained multiple video or image files.
22. Below is a summary of three of the orders derived from the "Toronto Company"; I have personally reviewed the DVDs described in paragraphs 23, 25, and 27:

ORDER NUMBER	98406
DATE	December 18, 2010
NAME	Gerald Silva
BILLING DETAILS	34 Morris Street Coventry, RI 02816-5971
PHONE	[REDACTED]
EMAIL	gerald.silva.home@gmail.com
AUTH CODE	Capture Card
Product ID	90008, 70247, 90006, 70032, 90009
Product Name	Before the Storm (Fore Stormen) (2000) DVD BF v2.0: Black Sea 2.0 [3-disc] (2010) DVD Growing Up: Boys (2002) DVD Angler, The (1993) DVD Kes (1969) DVD
Grand Total Price	\$85.56

23. The following is a description of the movie files of "BF v2.0: Black Sea 2.0"<sup>3</sup>

(a) 70247-1.avi

This movie file contains two minor males under the age of 18 years. The first minor male removes all of his clothes and enters the shower and starts to wash himself exposing his genitals. The second minor then removes all of his clothes and enters the shower and starts to wash himself exposing his genitals. The two minor males proceed to the bed, and while they are both naked, they begin to begin to wrestle and play around on the bed. During this period the genitals and sometimes the anuses of the minor males are lascivious displayed. The movie file ends with the minor males at a fair with friends. (1:14:00)

(b) 70247-2.avi

This movie file contains three minor males under the age of 18 years. The minor males are in various stages of undress on a bed. After a short period, the minor males all become fully undressed. At this time the three minor males are naked on the bed and start to have a pillow fight and are playing. During this playing, the minor males have their legs apart exposing their genitals. The movie file ends with numerous minors playing in the ocean clothed. (1:17:16)

(c) 70247-3.avi

This movie file starts with numerous males under the age of 18 years swimming in the ocean. The movie then shows two minor males under the age of 18 years on a bed naked with their legs apart exposing their genitals. (28:54)

24. Below is information on a second order by SILVA:

ORDER NUMBER	104258
DATE	February 15, 2011
NAME	Gerald Silva
BILLING DETAILS	34 Morris Street Coventry, RI 02816-5971
PHONE	[REDACTED]
EMAIL	<a href="mailto:gerald.silva.home@gmail.com">gerald.silva.home@gmail.com</a>
IP Address	68.229.81.106
AUTH CODE	Capture Card
ORDER STATUS	Shipped 2/16/2011 15:43
Product ID	70249, 70290, 70123, 70148
Product Name	Cutting Room Floor: Vlaviu [2-disc] (2011) DVD Zhenya 2 for 1 [2-disc] (2011) DVD Boy Fights XVIII: Commando Squared (2008) DVD

<sup>3</sup> Films 90008, 90006, and 90009 were not recovered in the TPS search warrant of the "Toronto Company" (see paragraph 15.) Film 70032 was recovered.

Grand Total Price                      Boy Fights XXVII: Commando Knights (2009) DVD  
\$97.96

25. The following is a description of the movie files of “Cutting Room Floor: Vlaviu”:<sup>4</sup>

(a) 70249-1.avi

This movie file contains three minor males under the age of 18 who enter what appears to be an apartment kitchen carrying food. All three children are nude and eat seated on the floor. One of the children sits on a cupcake, causing pieces of it to become stuck to his buttocks and genital area. This same process is repeated over and over with the same male child sitting on numerous cupcakes which have been placed on a basketball, a bicycle seat, and on a mattress until he is covered in chocolate with numerous lascivious displays of the child’s genitals. One of the boys in the above mentioned scene enters the camera view in a kitchen, removes all of his clothes, and sits down on a basketball, exposing his genitals. He then proceeds to eat what appears to be chicken and repeatedly sits on pieces of meat on top of the basketball. At multiple points the child’s genitals are lasciviously displayed. (1:30:16)

(b) 70249-2.avi

This movie file contains one of the three minor males seen in *70249-1.avi* who enters what appears to be the same kitchen and removes all of his clothes. The child then places pieces of meat and more chocolate cupcakes on the basketball before sitting on them, forcing pieces of food to become stuck to his buttocks and anus. At multiple points the child’s genitals are lasciviously displayed. (1:06:48)

26. Below is information on a third order by SILVA:

ORDER NUMBER	108703
DATE	April 05, 2011
NAME	Gerald Silva
BILLING DETAILS	34 Morris Street Coventry, RI 02816-5971
PHONE	[REDACTED]
EMAIL	gerald.silva.home@gmail.com
AUTH CODE	Capture Card
Product ID	70198, 70212, 70201
Product Name	<b>FKK Brasov (2009) DVD</b> FKK Wiggly Wonders (2010) DVD FKK Wilderness (2010) DVD
Grand Total Price	\$70.26

<sup>4</sup> Films 70290, 70123, and 70148 were recovered in the TPS search warrant of the “Toronto Company” (see paragraph 15,) and are available upon request.

27. The following is a description of the movie files of **FKK Brasov**:<sup>5</sup>  
70198vid.avi  
This movie file contains three minor males under the age of 18 years. The minor males walk around rural area and end up in the woods. All three undress and run around in the woods and one takes pictures of the other two children. The movie cuts to a separate indoor location with all three children sitting naked on a sofa bed. The boys play cards and then start to have a pillow fight. They then exercise naked in front of each other and end with two of the boys wrestling in the bed and floor. At numerous points during this sequence, the minor males have their legs apart exposing their genitals and two of the children expose their anuses as well. (1:34:57)
28. The DVD files described in paragraphs 23, 25, and 27 will be made available with this affidavit for the court's review.
29. Based on your affiant's review of the order information related to SILVA, as well as my review of the videos purchased by SILVA, I have probable cause to believe that SILVA purchased child pornography via the Toronto Company's website multiple times and that target received this child pornography at the SUBJECT PREMISES.

#### VERIFICATION OF TARGET AND SUBJECT PREMISES

30. A query of the Rhode Island Division of Motor Vehicles records on or about September 13, 2012 revealed that an individual named Gerald J Silva with a date of birth of [REDACTED] 1954 resides at the SUBJECT PREMISES.
31. Your affiant confirmed that as of September 18, 2012 SILVA is currently receiving mail at 34 Morris Street, Coventry, RI 02816.
32. Physical surveillance of the SUBJECT PREMISES on September 12 and September 18, 2012 revealed that a tan Chevy Malibu sedan bearing RI license HU158 was parked next to the driveway of the SUBJECT PREMESIS.
33. A check of the RI registry of motor vehicles for HU158 lists the plate as actively registered to Gerald Silva with a residential address of 34 Morris Street, Coventry, RI.
34. A query using publicly available search tools was conducted for SILVA with the date of birth of [REDACTED] 1954. These public records indicated that SILVA's current address is 34 Morris Street, Coventry, RI 02816.
35. On September 21, 2012, while on surveillance in the area of 34 Morris Street, your affiant observed a white male, approximately 50 years old, with white hair and a white

---

<sup>5</sup> Films 70201 and 70212 were recovered in the TPS search warrant of the "Toronto Company" (see paragraph 15,) and are available upon request.

beard in the driveway of the residence. Based on a review of the Rhode Island Division of Motor Vehicles (DMV) digital license image of SILVA, your affiant confirmed that the individual was in fact SILVA.

36. On or about June 21, 2011 the United States Department of Justice Criminal Division, Child Exploitation and Obscenity Section (CEOS) issued an administrative subpoena to Google Inc. for email address [gerald.silva.home@gmail.com](mailto:gerald.silva.home@gmail.com) which is information from the customer database related to SILVA's transactions. On or about July 26, 2011, Google provided the following relevant information:

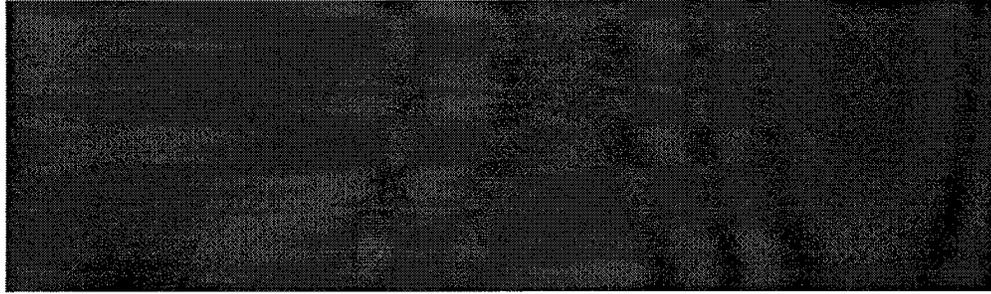
Name:	Gerald Silva
E-Mail address:	<a href="mailto:geraldsilvahome@gmail.com">geraldsilvahome@gmail.com</a>
Other usernames:	<a href="mailto:gerald.silva.home@gmail.com">gerald.silva.home@gmail.com</a>
Created on:	8/7/2010
Creation IP address:	24.177.253.205 <sup>6</sup>

37. Google's response to the above mentioned subpoena also included an IP log. On June 24, 2011 the [gerald.silva.home@gmail.com](mailto:gerald.silva.home@gmail.com) email account was accessed from IP address 12.157.80.162. A query of 12.157.80.162 using publicly available search tools identified the IP address as registered to Panera Bread.
38. On or about January 25, 2012 CEOS issued another administrative subpoena to Google Inc. for email address [gerald.silva.home@gmail.com](mailto:gerald.silva.home@gmail.com). On or about March 20, 2012, Google provided the same subscriber information as mentioned in paragraph 34 as well as an updated IP log. On January 7, 2012 the [gerald.silva.home@gmail.com](mailto:gerald.silva.home@gmail.com) email account was again accessed from IP address 12.157.80.162.
39. On September 18, 2012, your affiant went to the Panera Bread restaurant located at 1000 Division Street, East Greenwich, RI 02818. While in a vehicle within approximately 25 feet of the restaurant, using a laptop computer with a Windows operating system, I opened the wireless network connections function and refreshed the network list. This function displays the available wireless internet networks available within range of the computer. The computer detected the presence a wireless networks identified as Panera. I logged into Panera's wireless internet and opened internet explorer web browser, navigating to [www.whatismyipaddress.com](http://www.whatismyipaddress.com), a free commercial website which can identify the IP address of the given computer which is used to access the internet. The website identified a static IP address of 12.157.80.162, with internet service provided by AT&T on behalf of Panera Bread.
40. The Panera Bread restaurant located at 1000 Division Street, East Greenwich, RI 02818 is the closest Panera Bread franchise to the SUBJECT PREMESIS, located only approximately 6 miles away.
41. As discussed above, child pornography was delivered to the SUBJECT PREMISES on multiple occasions. On or about June 30, 2011, CEOS issued an administrative subpoena

---

<sup>6</sup> The IP listed was outside of the provider's retention period at the time of the subpoenas issuance.

to Cox Communications for IP address 68.229.81.106 on 2/15/2011 at 23:03 EST which was the IP address captured in the 2/15/2011 order detailed in paragraph 24 above. On or about July 15, 2011, Cox Communications provided the following relevant information:



42. [REDACTED] is located on [REDACTED]

[REDACTED] On September 18, 2012, while in a vehicle in the immediate area of both [REDACTED] and 34 Morris Street, using a laptop with a windows operating system I opened the wireless network connections function and refreshed the network list at several points. This function displays the available wireless internet networks available within range of the computer. The computer detected the presence of numerous unidentified, wireless networks in the area around the SUBJECT PREMISES. All of those networks are secured, i.e., password-protected. Given the distance between the two residences, if someone inside of the SUBJECT PREMISES had the password to their neighbor's wireless internet router, that individual would be able to access their neighbor's network from the SUBJECT PREMISES. It is therefore possible that while inside of SUBJECT PREMISES, an individual could make it appear as if their internet activity was originating in a neighbor's house in an attempt to avoid detection.

43. A check of open source information from the Internet regarding SILVA revealed that from 2/22/1995 through 5/1/2003, SILVA held a license as a clinical social worker in the state of RI. Additionally, from 3/5/2002 through the present Silva has held a license as an independent clinical social worker from the state of RI.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE RECEIPT AND ATTEMPTED RECEIPT OF CHILD PORNOGRAPHY**

44. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in the receipt and attempted receipt of child pornography:

- a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in

sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

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

c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

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

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

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

45. Your affiant participated in the execution of federal search warrants for receipt and possession of child pornography in the District of Massachusetts on September 13, 20, and 24, 2012. The three warrants were for three separate residences of three unrelated individuals, all of whom had been customers of the same Toronto Company during a similar time frame as SILVA. All three search warrants resulted in the seizure of hundreds of images and videos of child pornography including materials which were

directly purchased from the same Toronto Company by the individuals under investigation.

46. Based on SILVA's purchase of 75 different titles in 22 separate orders between October 2010 and June 2011 via the "Toronto Company's" website, totaling \$1,589.00 in United States currency I believe that SILVA likely displays characteristics common to individuals involved in the receipt or attempted receipt of child pornography.

#### **BACKGROUND ON COMPUTERS, DIGITAL CAMERAS, AND CHILD PORNOGRAPHY**

47. Computers and digital technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.
48. The development of computers and digital cameras has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
49. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 4 gigabytes of data, which provides enough space to store over 1000 high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.
50. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service,

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

51. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. 500 gigabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them.)
52. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
53. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.
54. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. When a DVD or CD is played in the optical disc drive of a computer, evidence regarding this activity often can be recovered from the computer's media player software, Windows Registry, and recent "link" files. Such information is often maintained indefinitely until overwritten by other data.

### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND OTHER MEDIA**

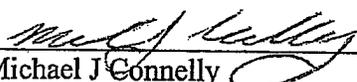
55. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:
- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.
  - b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.
  - c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers.
  - d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can

conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

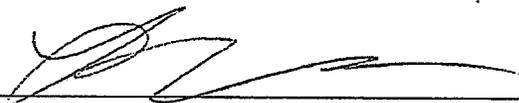
56. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:
  - a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and
  - b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.
57. Child pornography can be stored and hidden within videotapes, VHS tapes, DVDs, CDs, and similar media in various ways. For example, videotapes, VHS tapes, DVDs, and CDs containing child pornography may be stored within outer containers and boxes that inaccurately or misleadingly describe the contents of the videotapes, VHS tapes, DVDs, and CDs. Further, child pornography may be spliced or merged into the latter portion of a videotape, VHS tape, DVD, or CD that contains seemingly innocuous subject matter on its initial portions. In order to conduct a thorough examination of the content of videotapes, VHS tapes, DVDs and CDs reasonably believed to contain child pornography, it is respectfully requested that law enforcement be granted authority to remove all videotapes, VHS tapes, DVDs, and CDs located in the aforementioned premises during the execution of the search warrant for further examination.

**CONCLUSION**

58. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the residence described in Attachment A, in violation of 18 U.S.C. Sections 2252 and 2252A.
59. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

  
\_\_\_\_\_  
Michael J. Connelly  
United States Postal Inspector

SUBSCRIBED and SWORN  
before me this 26<sup>th</sup> day of September 2012

  
\_\_\_\_\_  
LINCOLN D. ALMOND  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**DESCRIPTION OF PREMISES TO BE SEARCHED**

The premises to be searched, (SUBJECT PREMISES,) is 34 Morris Street, in the town of Coventry, County of Kent, State of Rhode Island, more fully described as a single family one-story dwelling. The residence is located on Morris Street near the intersection of Morris Street and Coventry Drive. The residence has white siding with a light brown roof and dark colored shutters. The number "34" is located to the left of the front door. There are several steps leading to the front door from the front walk. On the right side of the house is a driveway leading to a one-car garage. To the left of the garage door is a second dark colored front door with a mail box on the wall adjacent to the door.

## ATTACHMENT B

### ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252 and 2252A including but not limited to:

1. All records and tangible objects concerning: "Toronto Company"; "www.[torontocompany].com"; and email addresses "gerald.silva.home@gmail.com" and "geraldsilvahome@gmail.com".
2. Computer(s), computer hardware, computer software, computer-related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, digital video disc (DVD) players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
3. All originals, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), and child erotica, in any format or medium (including, but not limited to, computer or digital data files, photographs, magazines, photocopies, DVDs, compact discs (CDs), VHS tapes, videotapes, and photographic and motion picture film).
4. All visual depictions of minors.
5. All DVDs, CDs, VHS tapes, and videotapes.
6. All cameras, film, and other photographic equipment.
7. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) pertaining to the possession, receipt, distribution, transportation, or sale of child pornography as defined in 18 U.S.C. § 2256(8), or to the possession, receipt, distribution, transportation, or sale of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

8. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) identifying individuals or companies distributing, transporting, selling, or receiving child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), through interstate or foreign commerce by any means (including, but not limited to, by United States mail or computer).

9. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records), identifying individuals or companies possessing child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

10. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records), concerning communications between individuals or companies about child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

11. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) concerning subscriptions to or memberships in groups, clubs, or services that provide or make child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), accessible to subscribers or members.

12. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) identifying individuals or companies that may have contacted SILVA, or have been contacted by SILVA, by any means for the purpose of receiving, distributing, transporting, or selling child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

13. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, mailing lists, supplier lists, mailing address labels, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) pertaining to the preparation, purchase, or acquisition of names of individuals or companies, or lists of names of individuals or companies, to be used in connection with the receipt, distribution,

transportation, or sale of child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), through interstate or foreign commerce by any means (including, but not limited to, by United States mail or computer).

14. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) reflecting a sexual interest in minors, or personal contact or activities with minors.

15. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) containing or listing names and addresses of minors who are visually depicted while engaged in sexually explicit conduct, as defined by 18 U.S.C. § 2256.

16. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, invoices, billing statements, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) that concern any accounts with an Internet Service Provider.

17. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, invoices, billing statements, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records), that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

18. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, invoices, billing statements, envelopes, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) that evidence ownership, use, or control of any computer(s) and all related computer and/or video equipment found in the premises listed and described in Attachment A.

19. All notes, documents, records, correspondence, diaries, and address books, in any format or medium (including, but not limited to, computer or digital data files, envelopes, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, addressed correspondence, letters, papers, handwritten notes, and electronic messages, chat logs and electronic records) pertaining to occupancy or ownership of the premises listed and described in Attachment A.