

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America )

v. )

Colum Patrick Moran, Jr. )

Case No. )

3:19-mj- 1098 -JBT )

Defendant(s)

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(s) of Dec. 28, 2016 - Oct. 31, 2018 in the county of Duval in the Middle District of Florida, the defendant(s) violated:

Code Section	Offense Description
18 U.S.C. §§ 2251(d)(1)(A) and (2)(B)	Solicitation and advertisement for child pornography, in violation of 18 U.S.C. §§2251(d)(1)(A) and (2)(B).

This criminal complaint is based on these facts:

See attached.

Continued on the attached sheet.



Complainant's signature

ABBIGAIL BECCACCIO, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

3/6/19

Judge's signature



City and state:

Jacksonville, Florida

JOEL B. TOOMEY, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT**

I, Abbigail Beccaccio, being duly sworn, state as follows:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2012. I am currently assigned to the Jacksonville, Florida Division of the FBI where I conduct a variety of investigations in the area of violent crimes. Prior to this assignment, I was employed as Forensics and Technology Unit Supervisor with the Orlando Police Department for approximately 8 years. I have a Bachelor's degree in Molecular Biology & Microbiology. I have received law enforcement training from the FBI Academy at Quantico, Virginia. A substantial portion of my duties are dedicated to investigating cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate child exploitation offenses. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the advertisement for, possession, collection, production, receipt, and/or transportation of images of child pornography and the solicitation and extortion of children to produce sexually explicit images of themselves. I have been involved in searches of residences pertaining to the advertisement for, possession, collection, production, and/or transportation of child pornography through either the execution of search warrants or through the subject providing written consent to permit a search to be conducted.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of 18 U.S.C. §§ 2251, 2252, 2252A, 2422, and 2423, as well as Florida state statutes that criminalize the sexual activity with minors and other methods of child sexual exploitation. In connection with such investigations, I have served as case agent, have been the affiant for several search warrants and conducted interviews of defendants and witnesses, and have served as an undercover agent in online child exploitation cases. I am a member of a local child pornography task force comprised of the FBI, U.S. Immigration and Customs Enforcement, the Florida Department of Law Enforcement, the Jacksonville Sheriff's Office, the St. Johns County Sheriff's Office, and the Clay County Sheriff's Office, among other agencies. These agencies routinely share information involving the characteristics of child sex offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. The statements contained in this affidavit are based on my personal knowledge, as well as on information provided to me by experienced Special Agents and other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of establishing probable cause for the filing of a criminal

complaint, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that COLUM PATRICK MORAN, JR. has committed violations of Title 18, United States Code, Sections 2251(d)(1)(A) and (2)(B), that is, advertisement for and solicitation of child pornography.

4. I make this affidavit in support of a criminal complaint against COLUM PATRICK MORAN, JR., charging that from on or about December 28, 2016 through on or about October 31, 2018, in the Middle District of Florida and elsewhere, COLUM PATRICK MORAN, JR. did knowingly make, print and publish, and cause to be made, printed, and published, notices and advertisements seeking and offering to receive visual depictions, the production of which visual depictions involved the use of a person whom defendant believed to be a minor engaging in sexually explicit conduct and which depictions would be of such conduct, and such notices and advertisements were transported using a means and facility of interstate commerce, that is, by computer via the internet, in violation of Title 18, United States Code, Sections 2251(d)(1)(A) and (2)(B)

5. On March 5, 2019, I applied for and obtained a federal search warrant for the residence located at 6710 Collins Road, Apartment 415, Jacksonville, Florida 32244, believed to be occupied by COLUM PATRICK MORAN, JR. I was the affiant for the affidavit in support of the application for this search warrant, and I am

familiar with the facts contained therein. A copy of the application and affidavit for this search warrant is attached as Exhibit A, and the facts and information contained therein is hereby incorporated by reference herein<sup>1</sup>. This warrant authorized the search of this residence for fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2251(d), 2252 and/2252A, that is, advertisement for and solicitation of child pornography, and receipt and attempted receipt of child pornography. This search warrant was issued by United States Magistrate Judge Joel B. Toomey in Case No. 3:19-mj-1095-JBT.

6. On March 6, 2019, at approximately 6:03 a.m., I, together with other FBI agents and law enforcement personnel, executed this search warrant at the apartment residence located at 6710 Collins Road, Apartment 415, Jacksonville, Florida 32244.

7. COLUM PATRICK MORAN, JR. was present at the residence, and was briefly detained for officer safety while the residence was cleared. MORAN was then released from this brief detention and I approached him for a possible interview.

8. I told MORAN that a search warrant was being executed at his residence, that he was not under arrest, and was free to leave. MORAN was

---

<sup>1</sup> Certain identifying information has been redacted from the affidavit in support of the application for the search warrant to protect the privacy of persons referred to therein.

advised that agents wished to speak with him and were available to answer any questions. MORAN agreed to speak with me and accompanied me, along with FBI Special Agent (SA) Jonathan MacDonald, to a nearby FBI car. MORAN entered the vehicle and sat in the front passenger seat, while I sat the driver's seat and SA MacDonald sat in the rear seat. MORAN then provided, in summary and among other things, the following information:

(a) MORAN was previously asked if he needed anything. Agents provided MORAN with pants, shirt, a hoodie and shoes.

(b) MORAN has lived in Jacksonville, Florida at this apartment approximately eight years and has Comcast internet service. The residence has secured wireless internet service and requires a password. MORAN was unaware of anyone else accessing or using his secured wireless service. MORAN lived alone and did not have a roommate or any children who live with him in the apartment.

(c) MORAN used AT&T internet services for his cellular phone service and provided telephone number 978-809-9479. MORAN was asked where the area code for his telephone number originated, and he stated "Massachusetts," where he previously resided.

(d) MORAN uses the internet for various activities to include Facebook, Instagram and online bill pay.

(e) MORAN asked about the nature of the investigating agents' visit

to his home and execution of a search warrant. MORAN was told that internet related postings were being investigated, and MORAN was read a post made by user Emilylover@aol.com to a motherhood related blog. The post stated, "I love the IG picture of the girls in their dance outfits, both of their tight little bodies are so sexy! I really like how A\_\_\_\_\_ is holding up the front of her skirt to show off her crotch, you should have her pose like that in a regular skirt and panties. Or, maybe both her and miss M\_\_\_\_\_ can pose with their skirts pulled up and nothing underneath." (I know from a previous interview that the female children referenced in this blog post, which I have probable cause to believe was posted by MORAN, have dates of birth in November 2010 and May 2015 respectively, as set forth in attached Exhibit A). After being read the post, MORAN questioned interviewing agents as to why the identity of "Emily lover" mattered. MORAN also asked if "Emily lover" was engaged in "criminal communications." MORAN then further explained that he was not a "child molester" and did not "even like kids." MORAN made numerous hypothetical comments regarding the user "Emily lover" and ultimately denied several times using the user name "Emily lover" in any capacity.

(f) MORAN agreed that the postings made by "Emily lover" to the motherhood blog sites were suspicious especially if made by someone that was not a mother with children. MORAN also agreed that it was reasonable that law enforcement would follow-up the postings.

9. At one point, I exited the vehicle and entered the search residence where I learned that during the execution of the search warrant while searching for items of evidence, FBI personnel located:

(a) A plastic storage bin containing at least 50 pairs of children's underwear (of the type and sizes worn by young female children). I saw several of these pairs of underwear, and several appeared to bear encrusted stains that were consistent with dried biological fluid.

(b) Numerous Velcro law enforcement identification patches, which were appropriately sized for placement on ballistic vests or uniforms. Also recovered was a bulletproof vest and multiple firearms, including a .357 Magnum revolver, an AR-15 rifle, a .45 caliber pistol, and a .22 caliber pistol, as well as a significant amount of ammunition.

(c) Also located within the residence were several Florida driver's licenses, credit cards and other items which were consistent with those commonly located within a person's wallet or purse. None of these items bore MORAN's name or personal identifiers.

(d) A Samsung mobile telephone that was assigned telephone number 978-809-9479 was located in the living room of the residence. A review by an FBI computer scientist on scene revealed that contained in the "Gallery" icon of the phone, were over 300 digital photos, many of which depicting minors engaged in



sexually explicit conduct, including the lascivious exhibition of their genitalia, pubic areas, and anal area. I reviewed these images and the majority depicted prepubescent female children with their vaginal and anal areas displayed prominently. Several others also contained female children's panties pulled down or over to display the vaginal/anal areas of the minors depicted in a lascivious manner. One particular photo that I reviewed was a color image that depicts a female toddler-aged minor child lying on her back. The toddler's legs are spread exposing her vaginal area as the focal point of the image, in a manner that I believe constitutes the lascivious exhibition of the child's genitalia.

10. Later, I returned to the vehicle and showed MORAN numerous images of child pornography contained on the Samsung phone that was located in the living room of his residence. MORAN stated initially, "That's not my phone." MORAN was then told that the telephone number associated with this Samsung phone was 978-809-9479, the same number that MORAN had previously confirmed was his, and he replied, "It's an old phone." A few moments later, the interview was terminated.

11. Later on the same day, FBI Supervisory Special Agent (SSA) C. J. Goodman interviewed Eric Lyons, a self-described colleague and friend who arrived at MORAN'S residence during the execution of the search warrant. Lyons told SSA Goodman, who told me, that Lyons has known MORAN for 7 years and has

known him to use the telephone number 978-809-9479. Lyons has known MORAN to use that telephone number for at least the 7 years Lyons has known MORAN and does not know MORAN to use any other telephone number.

12. Based upon my training and experience, as well as my review of all of the evidence and information set forth above and in the attached Exhibit A, I have probable cause to believe that COLUM PATRICK MORAN, JR. is the same person as the user "Emily lover" who used email address emilylover@aol.com to post the sexually explicit comments on the motherhood blogs as set forth in detail in Exhibit A.

13. After the conclusion of this interview, I contacted Assistant United States Attorney D. Rodney Brown by telephone, and he authorized me to arrest MORAN. Shortly thereafter, I placed MORAN under arrest.

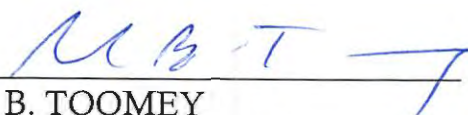
14. Based upon the foregoing facts, I have probable cause to believe that from on or about December 28, 2016 through on or about October 31, 2018, in the Middle District of Florida and elsewhere, COLUM PATRICK MORAN, JR. did knowingly make, print and publish, and cause to be made, printed, and published, notices and advertisements seeking and offering to receive visual depictions, the production of which visual depictions involved the use of a person whom defendant believed to be a minor engaging in sexually explicit conduct and which depictions would be of such conduct, and such notices and advertisements were transported

using a means and facility of interstate commerce, that is, by computer via the internet, in violation of Title 18, United States Code, Sections 2251(d)(1)(A) and (2)(B).



ABBIGAIL BECCACCIO, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this  
6 day of March, 2019, at Jacksonville, Florida.



JOEL B. TOOMEY  
United States Magistrate Judge

# UNITED STATES DISTRICT COURT

for the  
Middle District of Florida

In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*

Residence located at 6710 Collins Road, Apartment 415,  
Jacksonville, Florida 32244 more fully described in  
Attachment A

Case No. 3:19-mj- 1095-JBT

## 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 on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Residence located at 6710 Collins Road, Apartment 415, Jacksonville, Florida 32244 more fully described in Attachment A

located in the     Middle     District of     Florida    , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

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

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- 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.

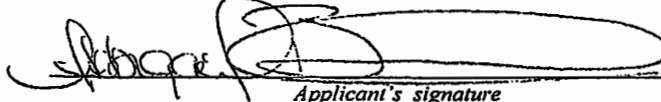
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2251(d)(1)(A) and 2(B); 18 U.S.C. §§ 2252 and 2252A	Solicitation and advertisement for child pornography; attempted receipt of child pornography.

The application is based on these facts:

See attached affidavit

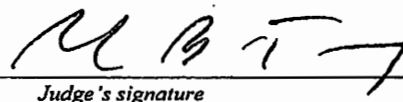
- Continued on the attached sheet.
- Delayed notice of      days (give exact ending date if more than 30 days:     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Abigail Beccaccio, Special Agent, FBI  
Printed name and title

Sworn to before me and signed in my presence.

Date:     3/5/19    

  
Judge's signature

City and state:     Jacksonville, Florida    

Joel B. Toomey, United States Magistrate Judge  
Printed name and title

# EXHIBIT A

**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

The premises to be searched is an apartment residence designated as Apartment 415 located at 6710 Collins Road, Jacksonville, Florida 32244 in the Westland Park Apartments complex. The Westland Park Apartments complex is located on the south side of Collins Road between Interstate Highway 295 and Grayfield Drive. The building containing Apartment 415 is a three-story, multi-unit structure with tan and green siding and light colored trim and marked with the number "4" on its front façade that faces east. Apartment 415 is located on the second floor at the top of the first flight of stairs toward the northeast corner of Building 4. Apartment 415 has a green door and the number "415" is posted on the outside wall the right of the front door. On February 28, 2019, there was a tan "Welcome" sign depicting a green shamrock insignia hanging on the front door. A "New England Patriots" banner was observed displayed inside a window that faced east in Apartment 415.

## **ATTACHMENT B**

### **LIST OF ITEMS TO BE SEIZED AND SEARCHED**

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, cellular telephones, "smart" phones such as an Apple iPhone, electronic tablets such as an Apple iPad, digital cameras and/or memory cards, or any other device capable of electronic storage of data and/or images) , computer-related documentation, computer passwords and data-security devices, videotapes, video-recording devices, video-recording players, and video display monitors that are or may be 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 or child erotica.

2. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs, including peer-to-peer software, 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 or child erotica.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs

and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, 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), or child erotica.

5. Any and all diaries or address books containing names or lists of names and addresses of individuals who have been contacted by use of the computer(s) or by other means for the purpose of advertising for, soliciting, distributing 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).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession 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).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet service provider.



11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including 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.

12. Any and all cameras, film, videotapes or other photographic equipment capable of being used to produce, manufacture, store and/or conceal visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. §2256(2).

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in 18 U.S.C. §2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and

electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises to be searched, including rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all diaries, notebooks, notes, logs, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the identity of any and all owners and/or users of any computers, computer media and any electronic storage devices discovered in the premises and capable of being used to produce, manufacture, store and/or conceal visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. §2256(2).

17. Any documents, records, programs or applications relating to the existence of wiping, data elimination, and/or counter-forensic programs (and associated data) that are designed to delete data from the subject computers and computer media.

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

I, Abbigail Beccaccio, being duly sworn, state as follows:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2012. I am currently assigned to the Jacksonville, Florida Division of the FBI where I conduct a variety of investigations in the area of violent crimes. Prior to this assignment, I was employed as Forensics and Technology Unit Supervisor with the Orlando Police Department for approximately 8 years. I have a Bachelor's degree in Molecular Biology & Microbiology. I have received law enforcement training from the FBI Academy at Quantico, Virginia. A substantial portion of my duties are dedicated to investigating cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate child exploitation offenses. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the advertisement for, possession, collection, production, receipt, and/or transportation of images of child pornography and the solicitation and extortion of children to produce sexually explicit images of themselves. I have been involved in searches of residences pertaining to the advertisement for, possession, collection, production, and/or transportation of child pornography through either the execution of search warrants or through the subject providing written consent to permit a search to be conducted.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422, and 2423, as well as Florida state statutes that criminalize the sexual activity with minors and other methods of child sexual exploitation. In connection with such investigations, I have served as case agent, have been the affiant for several search warrants and conducted interviews of defendants and witnesses, and have served as an undercover agent in online child exploitation cases. I am a member of a local child pornography task force comprised of the FBI, U.S. Immigration and Customs Enforcement, the Florida Department of Law Enforcement, the Jacksonville Sheriff's Office, the St. Johns County Sheriff's Office, and the Clay County Sheriff's Office, among other agencies. These agencies routinely share information involving the characteristics of child sex offenders as well as investigative techniques and leads. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. The statements contained in this affidavit are based on my personal knowledge as well as on information provided to me by other law enforcement officers. This affidavit is being submitted for the limited purpose of securing a search warrant, and I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish

probable cause to believe evidence of violations of Title 18, United States Code, Sections 2251(d), 2252, and/or 2252A, is present in the items to be searched.

4. I am requesting authority to search the residence specifically identified in Attachment A, which includes the physical structure, as well as any computer and computer media and electronic storage devices located therein. I also request to seize any and all items listed in Attachment B as instrumentalities, fruits, and/or evidence of criminal activity specified herein.

#### **STATUTORY AUTHORITY**

5. This investigation concerns potential violations of Title 18, United States Code, Sections 2251(d), 2252 and 2252A, relating to material involving the sexual exploitation of minors. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, computer forensic examiners, and federal prosecutors, I know the following:

a. 18 U.S.C. § 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing or accessing with intent to view (or attempting to do so) any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

b. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view (or attempting to do so) any

child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

c. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping (or attempting to do so) using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct. Under 18 U.S.C. § 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including by computer, any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails. Under 18 U.S.C. § 2252(a)(4), it is also a crime for a person to knowingly possess, or knowingly access with intent to view (or attempt to do so), one or more books, magazines, periodicals, films, video tapes, or other matter, which contains one or more visual depictions of minors engaged in sexually explicit conduct that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign

commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer.

d. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping (or attempting to do so) using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography 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. 18 U.S.C. § 2252A(a)(3) prohibits a person from knowingly reproducing (or attempting to do so) child pornography for distribution through the mails or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view (or attempting to do so) any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography 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 using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. §§ 2251(d)(1)(A) and (2)(B), make it a federal crime or offense for any person to knowingly make, print, or publish or caused to be made, printed or published, any notice or advertisement seeking or offering to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct, if such notice or advertisement is transported using any means or facility of interstate and foreign commerce, including by computer via the Internet.

f. The internet is a means and facility of interstate commerce and foreign commerce.

#### DEFINITIONS

6. The following definitions apply to this Affidavit:

a. "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, illegal or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (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). See 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (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," 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, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

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, 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. 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), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data

files and printouts or readouts from any magnetic, electrical or electronic storage device).

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 a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software 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 "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a unique and different 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.

k. "Wireless telephone" (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers,

enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. Many wireless telephones are minicomputers or “smart phones” with immense storage capacity.

1. A “digital camera” is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

m. A portable media player (or “MP3 Player” or iPod) is a handheld

digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

### **COMPUTERS AND CHILD PORNOGRAPHY**

7. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and significant skill to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

8. The development of computers has radically changed the way that child pornographers manufacture, obtain, distribute and store their contraband.

Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

9. Child pornographers can now convert paper photographs taken with a traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, images and videos can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. 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.

10. A 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, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

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

12. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Hotmail, and Google, among others. The online services allow a user to set up an account with a remote computing service that provides email 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. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communication 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 email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos 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). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based upon my training and experience, as well as conversations with other law enforcement officers and

computer forensic examiners, I know that these electronic “chat logs” often have great evidentiary value in child pornography investigations, as they record communication in transcript form, show the date and time of such communication, and also may show the dates and times when images of child pornography were traded over the Internet. 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 P2P software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

#### **SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

14. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, I know that searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (*e.g.*, hard drives, compact disks (“CDs”), diskettes, tapes, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching



authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system, which includes the use of data search protocols, is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased<sup>1</sup>, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

---

<sup>1</sup> Based on my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that computer forensic techniques can often recover files, including images and videos of child pornography (as well as logs of online chat conversations and other documents), that have long been "deleted" from computer media by a computer user.

### CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

15. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals who collect child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography also collect other sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not meet the legal definition of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest in children and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Many individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Many individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they

were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their sexually explicit materials as prized and valuable materials, even as commodities to be traded with other like-minded individuals over the Internet. As such, they tend to maintain or “hoard” their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. These individuals may protect their illicit materials by passwords, encryption, and other security measures; save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted; or send it to third party image storage sites via the Internet. Based on my training and experience, as well as my conversations with other experienced law enforcement officers who conduct child exploitation investigations, I know that individuals who possess, receive, and/or distribute child pornography by computer using the Internet often maintain and/or possess the items listed in Attachment B.

16. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with

law enforcement officials. For example, I am aware of an investigation by the FBI in Jacksonville in which the subject had his residence searched pursuant to a federal search warrant and his computer and digital storage media seized by the FBI. The search of his computer and other computer storage media revealed the subject knowingly possessed several thousand images of child pornography. The subject retained an attorney and both were made aware of the ongoing investigation into the subject's commission of federal child pornography offenses. Approximately two months later, the subject was arrested on federal child pornography charges. After the subject's arrest, the FBI obtained a laptop computer owned by the subject's employer but possessed and used by the subject both before and after the execution of the search warrant at his residence. Subsequent forensic examination of this computer revealed that the subject had downloaded, possessed and viewed images of child pornography numerous times *after* the execution of the search warrant and before his arrest.

17. Based on my training and experience, I also know that, with the development of faster Internet download speed and the growth of file-sharing networks and other platforms through which individuals may trade child pornography, some individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. However, as referenced above, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Furthermore, even in instances in which an

individual engages in a cycle of downloading, viewing, and deleting images, a selection of favorite images involving a particular child or act is often maintained on the device.

18. Based on my training and experience, I know that within the last several years, individuals who have a sexual interest in minor children have used the internet and internet-enabled devices with increasing frequency to make contact with and attempt to establish relationships with potential child victims and/or with individuals who are parents or guardians of potential child victims. These individuals may perceive that the internet provides some degree of anonymity and safety from prosecution. Because more and more children are using the internet and internet enabled devices, these individuals potentially expose more and more child victims to online sexual exploitation. These individuals may contact potential child victims, and/or their parents or guardians, through social networking websites such as Facebook and Twitter, or may engage in online conversations with children through text messaging and email. During these online conversations, photographic images and links to internet websites can be easily exchanged between the individual and the targeted child. Based on my training and experience, I know that when such an individual uses text messaging, email, or other websites to have online contact with children, the internet-enabled device used, whether it is a computer, a cellular telephone, a "smart" phone such as an "iPhone," or a tablet such as an "iPad," often saves and maintains evidence of such contacts. This evidence can often be extracted and examined by a trained forensic examiner.

**BACKGROUND OF INVESTIGATION AND  
FACTS ESTABLISHING PROBABLE CAUSE**

19. I make this affidavit in support of a search warrant for the apartment residence located at 6710 Collins Road, Apartment 415, Jacksonville, Florida 32244 that I believe to be currently occupied by Colum Patrick Moran, Jr. (date of birth 08/XX/1978). This affidavit is based on information provided to me both verbally and in written documentation from other law enforcement officers and personnel, including FBI SA Amy Whitman in Los Angeles and FBI Staff Operation Specialist Megan Hammerling in Jacksonville, as well as through investigation that I personally conducted as set forth herein. FBI SA Robert Schwinger of the FBI Jacksonville office has personally observed the premises and provided me with a written description of the premises, and this description is set forth in Attachment A.

20. The FBI is investigating Colum Patrick Moran, Jr. as a potential suspect for using one or more computers, smart phones, and computer media at this residence to commit violations of (i) Title 18, United States Code, Sections 2252 and 2252A, which prohibit receipt and attempted receipt in interstate or foreign commerce by any means, including by computer, any child pornography, that is, visual depictions of one or more minors engaging in sexually explicit conduct; and (ii) Section 2251(d)(1)(A) and (2)(B), which makes it a federal crime or offense for any person to knowingly make, print, or publish or cause to be made, printed or published, any notice or advertisement seeking or offering to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction, if the production of

such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct, if such notice or advertisement is transported using any means or facility of interstate and foreign commerce, including by computer via the internet.

21. FBI SA Whitman has advised me of and provided me with the following information, some of which was set forth in written documentation that I have reviewed and much of which she described to me by telephone. On March 23, 2018, SA Whitman received a complaint from a citizen, D. M. [REDACTED] regarding sexually explicit comments about minor children posted to M. [REDACTED] M. [REDACTED], an online blog<sup>2</sup> created and maintained by D. M. [REDACTED]. This online blog contains information and photos concerning motherhood and raising children. The complaint indicated that a particular online user with the username "Emily lover" and the email address [emilylover@aol.com](mailto:emilylover@aol.com) posted the sexually explicit content. M. [REDACTED] also identified and provided other online blogs that had received similar sexually explicit comments pertaining to the conduct of minors by a user with the same username "Emily lover" and email address [emilylover@aol.com](mailto:emilylover@aol.com). The comment posted by user "Emily lover" appeared to be in response to innocent and innocuous postings and

---

<sup>2</sup> Based on my training and experience, I know that a "blog" is a regularly updated online website or web page, typically run by an individual or small group, that is written in an informal or conversational style and usually addresses topics of common interest to its users/readers. A blog may contain online personal reflections and comments, and is capable of containing hyperlinks to other websites, videos, and photos provided by the host writer and/or other users. Individual users may also post comments, hyperlinks, videos and images to a particular blog using the internet.



images depicting minor children. Two of these online blogs are as follows: "A [REDACTED] L [REDACTED]" created and maintained by C. S [REDACTED] and "F [REDACTED] M [REDACTED]," created and maintained by L. C [REDACTED].

22. On August 22, 2018, C. S [REDACTED] provided SA Whitman with copies of the sexually explicit comments posted to the A [REDACTED] blog referred to above (and referred to herein as "S [REDACTED] motherhood blog") by the user "Emily lover" along with the IP addresses used by user "Emily lover." The following information was set forth in the copies of the sexually explicit comments posted to S [REDACTED] motherhood blog that were provided to SA Whitman as well as in written documentation which I have reviewed<sup>3</sup>.

23. On December 28, 2016 at 9:32 p.m. and 9:33 p.m., user "Emily lover" used email address [emilylover@aol.com](mailto:emilylover@aol.com) and IP address 107.72.164.45 to post sexually explicit comments to S [REDACTED]'s motherhood blog. Also on October 27, 2016 at 2:19 a.m., the user "Emily lover" used email address [emilylover@aol.com](mailto:emilylover@aol.com) and IP address 107.72.164.112 to post the following sexually explicit comment to S [REDACTED] motherhood blog:

---

<sup>3</sup> I have reviewed printed copies of these particular blog comments, as well as the other blog comments referenced in this affidavit. I have learned that the software used to create and maintain the blog enables the administrator of the blog to view the user name, email address, and IP address used by an individual user to post blog comments. This information is retained and captured in the printouts that I have reviewed. As set forth in more detail below, the IP addresses used by the user "Emily lover" with email address [emilylover@aol.com](mailto:emilylover@aol.com) as displayed with the comments on the blog were used during this investigation to identify the particular internet service provider and the user's ISP subscriber information.

“She did a great job with these! The next time A\_\_\_\_\_ wants to take pictures, you should suggest something fun. Have A\_\_\_\_\_ take all her clothes off and take pictures of herself in the mirror. Especially where she’s sitting in front of the mirror with her legs spread wide open so we can see her vagina. Maybe she could try spreading her vagina lips apart with her fingers, so she can get a good picture of her little pink hole. My niece loves to have her picture taken while she uses the head of her toothbrush inside her vagina. If A\_\_\_\_\_ wants to try it, my niece likes to lick the white cream from the brush when she's done, A\_\_\_\_\_ would look so cute with her tasty girl goo smeared all over her smiling mouth.”

24. On October 16, 2018, SA Whitman conducted a query of www.maxmind.com and determined that the IP addresses 107.72.164.45 and 107.72.164.112 were issued to AT&T Wireless.

25. On August 24, 2017 at 9:59 p.m. CDT, October 26, 2017 at 8:16 p.m. CDT, October 31, 2017 at 10:33 p.m. CDT, and December 17, 2017 at 9:50 p.m. CST, the user “Emily lover” used email address [emilylover@aol.com](mailto:emilylover@aol.com) and IP address 66.177.103.25 to post sexually explicit comments to S [REDACTED] motherhood blog. Two of these sexually explicit comments posted during those dates and times as well as a hyperlink to the Amazon online shopping website are set forth:

**Posted on August 24, 2017 at 9:59 p.m.:** “Great post! But the pictures I would most like to see are missing, those would be the ones of A\_\_\_\_\_ going her ‘morning stuff’. In particular, some pictures of her on the toilet would be

awesome. I'd like to see her panties around her ankles, with her legs spread wide enough to see the pee dribbling from between her vagina lips. I'd also like a couple of them to show her beautiful smiling face, and a couple good closeups of her vagina.""; and

**Posted on October 31, 2017 at 10:33 p.m.:** "Definitely more twirly dresses!

And more posting upskirt shots while she's twirling. Also, 7 is the perfect age to get her one of these for her birthday

[https://www.amazon.com/gp/aw/d/B00UZJL3LQ/ref=cm\\_cr\\_arp\\_mb\\_bd\\_crb\\_top?ie=UTF8](https://www.amazon.com/gp/aw/d/B00UZJL3LQ/ref=cm_cr_arp_mb_bd_crb_top?ie=UTF8)"

26. On November 6, 2018, I accessed the Amazon hyperlink that launched to the Amazon product referenced as, "Beginner Clit Vibrator Sex Toy Stimulator with Multi-Speed Vibrations." I observed on this Amazon webpage, among other things, six photographs depicting a pink 4.13-inch "bejeweled" vibrator. The Amazon page additionally lists, "Simple and satisfying" and "excellent beginner toy" in reference to this device.

27. On October 16, 2018, SA Whitman conducted a query of [www.maxmind.com](http://www.maxmind.com) and determined the IP address 66.177.103.25 was issued to Comcast Cable Communications in Jacksonville, Florida.

28. On January 20, 2017, at 8:06 p.m. CST and January 28, 2017 at 6:39 p.m. CST, user "Emily lover" used email address [emilylover@aol.com](mailto:emilylover@aol.com) and IP address 24.129.1.24 to post comments to S [REDACTED] motherhood blog. One of these comment posts is set forth below:

“I can’t get over how amazing A\_\_\_\_\_’s legs look in those white tights! Maybe it’s because of how much of her thighs her leotard shows off, but she looks so innocently sexy. I’d love to see more of A\_\_\_\_\_ in her dance outfits.”

29. On October 16, 2018, SA Whitman conducted a query of www.maxmind.com and determined the IP address 24.129.1.24 was issued to Comcast Cable Communications in Jacksonville, Florida.

30. On November 1, 2018, L. C. [REDACTED] provided SA Whitman with copies of the sexually explicit comments posted to the Fueling Mamahood blog, referred to herein as “C. [REDACTED] motherhood blog,” by user “Emily lover” along with the IP address used by user “Emily lover.” The following information was set forth in the copies of the sexually explicit comments posted to C. [REDACTED] motherhood blog that were provided to SA Whitman as well as in written documentation which I have reviewed.

31. Based on my review of the printed copies of these particular blog comments, user “Emily lover” used email address [emilylover@aol.com](mailto:emilylover@aol.com) and IP address 69.180.86.104 to post sexually explicit comments to C. [REDACTED] motherhood blog on May 29, 2018 at 10:59 p.m. EST, July 10, 2018 at 7:49 p.m. EST and 7:50 p.m. EST, September 20, 2018, at 12:12 a.m. EST, and October 31, 2018 at 8:26 a.m. EST. One of these sexually explicit comments is set forth as follows:

**Posted on July 10, 2018 at 7:49 and 7:50 p.m.:** “I love L\_\_\_\_\_ and P\_\_\_\_\_’s bathing suits, the ones with the ruffles around the neckline, so cute!

I was wondering, do those suits have the crotch lining that's open in the front?

I like to have cute little girls like L\_\_\_\_\_ and P\_\_\_\_\_ pull their suits down around their ankles while I kneel in front of them. I push my hard cock into that little pocket and let them watch me stroke it while I look at their smooth vaginas. When I fill the pocket with a big load of cum, I like to help them pull their suits back up. I have them bow their legs out wide, so I can work the cum soaked material deep between their vagina lips and bum cheeks. Then I give them a little pat on the bum and send them back to play. There is really nothing cuter than watching a little girl squirming around because her suit is sticking to her crotch. Obviously L\_\_\_\_\_ and P\_\_\_\_\_ would have to take turns, to let me load back up (I would hate to give the second one anything less than a full load), but I know they would both love the feeling of my warm cum squishing around against their girlie bits. Those suits do look a bit loose though the crotches, but with a little effort I think we can get them wedged in just fine"; and

**Posted on September 20, 2018 at 12:12 a.m.:** "I'm really interested in the flushable wipes you were talking about on IG! Can you please post some pictures or a video of L\_\_\_\_\_ and P\_\_\_\_\_ using them? I'm curious to see how easily their little fingers can navigate their crotches with them, and how well they clean the girl's vaginas. Thanks."

32. On November 1, 2018, SA Whitman conducted a query of [www.maxmind.com](http://www.maxmind.com) and determined the IP address 69.180.86.104 was issued to Comcast Cable Communications in Jacksonville, Florida.

33. On November 5, 2018, I submitted a request for technical assistance to the National Center for Missing & Exploited Children (NCMEC) requesting all complaints and information regarding a subject with user name "Emily lover," email address [emilylover@aol.com](mailto:emilylover@aol.com), and IP addresses 66.177.103.25, 24.129.1.34, 107.72.164.45, 107.72.164.112, and 69.180.86.104. On November 5, 2018, NCMEC responded to my request with documentation. The response referenced three CyberTipline reports<sup>4</sup> received by NCMEC that were forwarded to the Jacksonville Sheriff's Office (JSO). In each of the three CyberTipline reports, user "Emily lover," email address [emilylover@aol.com](mailto:emilylover@aol.com), and/or IP address 66.177.103.25 were referenced in regards to sexually explicit comments posted to various online blogs similar in character and content to those posted to S [REDACTED] motherhood blog and C [REDACTED] motherhood blog.

34. During my review of the information provided by NCMEC, I learned that ten CyberTipline reports pertaining to user name "Emily lover" were forwarded

---

<sup>4</sup> Based on my training and experience, I know that NCMEC routinely receives complaints and referrals through its website and telephone number from individuals who are reporting potential criminal activity involving children that they have witnessed online or elsewhere. NCMEC receives these complaints, catalogs them with a unique numbering system, and processes them as expeditiously as possible, referring them to the appropriate law enforcement agencies, including the FBI. These referrals are known as "CyberTipline" reports.

to different law enforcement agencies to include, but not limited to: FBI Virginia, Arkansas State Police, Gainesville (Florida) Police Department, and the Knoxville (Tennessee) Police Department. Fourteen CyberTipline reports pertaining to email address emilylover@aol.com were forwarded to different law enforcement agencies, including the Arkansas State Police, Gainesville Police Department, and the Knoxville Police Department. Six CyberTipline reports pertaining to IP address 66.177.103.25 were forwarded to different law enforcement agencies, including the Arkansas State Police and Gainesville Police Department. Two CyberTipline reports pertaining to IP address 24.129.1.34 were forwarded to different law enforcement agencies, including the Knoxville Police Department and the Gainesville Police Department. Two CyberTipline reports pertaining to 107.72.164.45 were forwarded to different law enforcement agencies, including the Knoxville Police Department and the Gainesville Police Department. Eight CyberTipline reports pertaining to IP address 69.180.86.104 were forwarded to different law enforcement agencies, including the Arkansas State Police and the Gainesville Police Department.

35. On November 5, 2018, I spoke to Jacksonville Sheriff's Office (JSO) Detective Kelly Vought who also provided me with copies of the three CyberTipline reports that NCMEC forwarded to JSO. The following information was set forth in the copies of the Cyber Tipline reports provided by Detective Vought. CyberTipline Report 7821138 was submitted on January 1, 2016, by J. K. [REDACTED] in regards to sexually explicit comments posted by user "Emily lover" with email address

[emilylover@aol.com](mailto:emilylover@aol.com) to an online blog created and maintained by J. K. [REDACTED]'s spouse. CyberTipline Report 222576236 was submitted on July 10, 2017 by C. P. [REDACTED] in regards to sexually explicit comments posted by user "Emily lover" with IP address 66.177.103.25 to an online blog created and maintained by P. [REDACTED]. CyberTipline Report 22332564 was submitted on July 13, 2017 by K. C. [REDACTED] in regards to sexually explicit comments posted by user "Emily lover" with email address [emilylover@aol.com](mailto:emilylover@aol.com) and IP address 66.177.103.25 to an online blog created and maintained by C. [REDACTED].

36. Detective Vought has also advised me of and provided me with the following information, some of which was set forth in written documentation that I have reviewed. On July 18, 2017, JSO Detective Brandi Merritt sent an administrative subpoena to Comcast Cable Communications requesting the subscriber information for the IP address 66.177.103.25 assigned on July 14, 2017 at 18:34:34 GMT. On July 18, 2017, Comcast Legal Response Center responded to this administrative subpoena. The subscriber information for the IP address 66.177.103.25 assigned on July 14, 2017 at 18:34:34 GMT resolved back to the Comcast account for the subscriber named Colum Moran, 6710 Collins Road, Apartment 415, Jacksonville, Florida, 32244, telephone number (978) 809-9479. On July 20, 2017, Detective Merritt conducted a query of JEA Verify (an online database available to law enforcement) and determined that Colum P. Moran, Jr. had an active account with JEA with utility service address 6710 Collins Road,



Apartment 415, mailing address 6710 Collins Road, Apartment 415, Jacksonville, Florida, 32244, and a utility service start date September 4, 2010.

37. On November 16, 2018, Detective Vought advised me of and provided me with the following information, some of which was set forth in written documentation that I have reviewed. On February 22, 2018, March 16, 2018, April 10, 2018, and May 15, 2018, Detective Vought attempted to make contact with the resident(s) of the apartment residence at 6710 Collins Road, Apartment 415, Jacksonville, Florida, 32244. On each of these four attempts, there was no answer at the front door and therefore no contact was made with Moran or any other person at the residence.

38. At my request, on November 16, 2018, FBI Operational Support Technician (OST) Kelsey Knecht prepared an administrative subpoena directed to Comcast Cable Communications requesting the subscriber information for the account associated with IP address 69.180.86.104 for the time period from May 29, 2018 to November 15, 2018.

39. On November 29, 2018, Comcast Legal Response Center responded to this administrative subpoena and I have reviewed the responsive documents. The subscriber information for the IP address 69.180.86.104 for the time period from May 29, 2018 to November 15, 2018 resolved back to the Comcast account for subscriber Colum Moran, 6710 Collins Road, Apartment 415, Jacksonville, Florida, 32244, telephone number (978) 809-9479.

40. FBI Staff Operations Specialist (SOS) Megan Hammerling has advised me of and provided me with the following information. On February 21, 2019, SOS Hammerling conducted database and social media searches for Colum Moran with the address of 6710 Collins Road, Apartment 415, Jacksonville, Florida 32244. According to the Florida Driver and Vehicle Information Database (DAVID), Colum Patrick Moran Jr. has two vehicles registered in his name, one of which is a 1998 Volkswagen 2-door vehicle that is yellow in color. An image on the Facebook page of Colum Moran (that I have reviewed) depicts a yellow 2-door Volkswagen vehicle that is consistent with and appears very similar to the vehicle listed for Colum Moran according to DAVID. Open source queries revealed that the email address [emilylover@aol.com](mailto:emilylover@aol.com) is associated with Apple, Spotify, Myspace, and Gaia Online<sup>5</sup> accounts.

41. A criminal history query for Colum Moran revealed the following arrests. On April 26, 2006, Moran was arrested by the Lawrence Police Department in Massachusetts, for carrying a folding knife and stainless steel billy club in violation of city ordinances which prohibit the carrying of dangerous weapons. On February 6, 2015, Moran was arrested by the Clay County Sheriff's Office due to an outstanding warrant for failure to appear for a traffic offense.

42. On January 9, 2019, I conducted a telephonic interview of D. M. [REDACTED] regarding the sexually explicit comments posted to her online blog referenced above

---

<sup>5</sup> SOS Hammerling has advised me that Gaia Online is an English-language, anime-themed social networking and forums-based website.

herein. I verified the information provided by SA Whitman and learned M [REDACTED] has operated and maintained her blog for approximately seven years and focuses on family, fitness and recipes, among other things. M [REDACTED] has two minor children (one male and one female) who are routinely depicted in images on the blog, and the children are always clothed and pictured engaged in innocent and age-appropriate activities. M [REDACTED] stated in substance that the sexually explicit comments and request for sexually graphic images of genitalia by the user "Emily lover" were always in relation to references to and images of her minor female child, J \_\_\_\_\_, whose date of birth is August XX, 2015.

43. On January 10, 2019, I conducted a telephonic interview of C. S [REDACTED] regarding the sexually explicit comments posted to her online blog referenced above herein. I verified the information provided by SA Whitman and learned she has operated and maintained her blog since February 2012, which focuses on motherhood, style, and family, among other things. C. S [REDACTED] has three children (one male and two females) who are routinely depicted in images on the blog, and the children are always clothed and pictured engaged in innocent and age-appropriate activities. C. S [REDACTED] stated in substance that the sexually explicit comments and requests for sexually graphic images by the user "Emily lover" were always in relation to references to and images of her minor female children, A \_\_\_\_\_ and M \_\_\_\_\_, whose dates of birth are November XX, 2010 and May XX, 2015.

44. On January 11, 2019, I conducted a telephonic interview of L. C [REDACTED] regarding the sexually explicit comments posted to her online blog referenced above

herein. I verified the information provided by SA Whitman and learned she has operated and maintained her blog for approximately three years which focuses on motherhood, infertility, and family, among other things. L. C. [REDACTED] has three children (one male and two females) who are routinely depicted in images on the blog, and the children are always clothed and pictured engaged in innocent and age-appropriate activities. L. C. [REDACTED] stated in substance that the sexually explicit comments and requests for sexually graphic images were always in relation to references to and images of her minor female children, L. [REDACTED] and P. [REDACTED], whose dates of birth are the same day, that is, May XX, 2015.

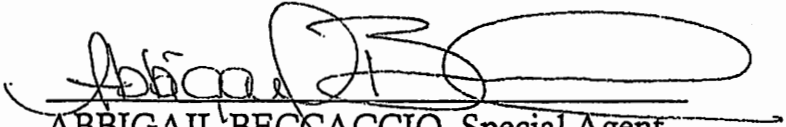
45. On February 27, 2019 and at my request, FBI SOS Megan Hammerling conducted a query of JEA Verify (an online database available to law enforcement) and determined that Colum P. Moran, Jr. has an active account for utility service with the Jacksonville Electric Authority (JEA) with service address 6710 Collins Road, Apartment 415, mailing address 6710 Collins Road, Apartment 415, Jacksonville, Florida, 32244, and utility service start date September 4, 2010. JEA records indicate the account is active, with a next payment due February 25, 2019.

46. At my request, on February 28, 2019, FBI SA Robert Schwinger conducted physical surveillance at the close proximity of the apartment residence located at 6710 Collins Road, Apartment 415, Jacksonville, Florida, 32244. SA Schwinger has advised me, both by oral and written report, that the subject premises appears as set forth in Attachment A to this affidavit, which is incorporated by reference herein.

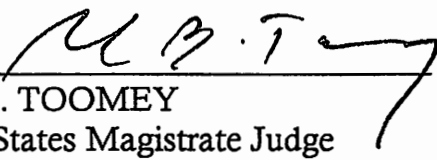
### CONCLUSION

47. Based on the foregoing, I have probable cause to believe that one or more individuals has used and is using one or more computers and/or electronic storage media located in the apartment residence located at 6710 Collins Road, Apartment 415, Jacksonville, Florida, 32244, more fully described in Attachment A to this affidavit, to, among other things, solicit and advertise for child pornography, and attempt to receive child pornography. Therefore, I have probable cause to believe that one or more individuals, using the residence described above has violated 18 U.S.C. §§ 2251(d), 2252, and/or 2252A. Additionally, I have probable cause to believe that fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2251(d), 2252, and/or 2252A, including at least one computer, smart phone, and/or other electronic storage media containing images and/or video depicting child pornography, and the items more fully described in Attachment B to this affidavit (which is incorporated by reference herein), will be located in this residence.

48. Accordingly, I respectfully request a search warrant be issued by this Court authorizing the search and seizure of the items listed in Attachment B.

  
\_\_\_\_\_  
ABBIGAIL BECCACCIO, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this  
5 day of March, 2019 at Jacksonville, Florida.

  
\_\_\_\_\_  
JOEL B. TOOMEY  
United States Magistrate Judge