

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

FILED

JUL 13 2022

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

IN THE MATTER OF THE SEARCH OF:)
)
THE PERSON)
CHRISTOPHER MICHAEL TERRY,)
DOB: DOB: 4/26/XXXX, SSN: XXX-XX-5039,)
FOR ACCESS TO APPLE and)
WICKR FACIAL RECOGNITION)
("FACE ID"))

Case No. 3:22-MJ- 2121

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your affiant, Jason Stewart, a Special Agent of the Federal Bureau of Investigation (FBI) being duly sworn, deposes and states the following:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent since May of 2017. I am currently assigned to the Violent Crime Squad at the Knoxville Field Office of the FBI. As an FBI Special Agent I am authorized to investigate violations of the laws, including the criminal drug laws, of the Unites, collect evidence in investigations where the United States is or may be a party of interest, serve and execute warrants, as well as to perform other duties. Prior to serving with the FBI, I was an officer in the United States Army for eight years, and a police officer with the Knoxville Police Department in Tennessee for two years. I have investigated federal criminal violations including bank robbery, violent crime and gangs, drug trafficking organizations, criminal enterprises, and violent crimes against children. I have received formal training in investigations at the Knoxville Police Academy in Tennessee, and the FBI Academy in Quantico, Virginia. As an FBI Special Agent, I am authorized to investigate violations relating to child exploitation and child pornography, including the production, transportation, receipt, distribution, and possession of

child pornography, in violation of 18 U.S.C. §§ 2251 and 2252A, as well as the enticement and coercion of minors, in violation of 18 U.S.C. § 2422(b). I have gained experience in conducting these investigations through training and through everyday work, including executing search warrants and interviewing individuals who trade child pornography and who seek to sexually exploit children. As part of my training and experience, I have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in multiple forms of media. I have been trained by the FBI in the acquisition, imaging, extraction, and analysis of digital evidence from computers, cellular telephones, and other electronic devices. I have also been trained by the FBI in digital image and video recovery. I have attended several courses on cybersecurity and cyber investigations provided by the FBI and private industry.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) – Distribution of Child Pornography; and, 18 U.S.C. § 2252A(a)(5)(B) - Possession of Child Pornography, are located on and/or within the following:

- a. The person of **CHRISTOPHER MICHAEL TERRY (TERRY)** described as a white male, having a date of birth of April 26, XXXX, social security account number XXX-XX-5039 and

3. TERRY is located in the Eastern District of Tennessee.

4. I seek to obtain access to TERRY's biometric facial recognition data points for Apple Face ID and Wickr in order to seize evidence, fruits and instrumentalities of the foregoing criminal violations believed to be located on his cellular device, an **Apple iPhone 11, Model: A2111, IMEI:353973103887825 in a blue Buffalo Bills NFL case**, currently stored at the FBI Knoxville Division, 1501 Dowell Springs Blvd. Knoxville, Tennessee 37909. I request authority

to obtain the aforementioned biometric facial recognition of TERRY to complete the search of the content contained within the social media application Wickr located in TERRY's Apple iPhone, 11. Although TERRY'S Apple iPhone, 11 was unlocked at the time it was seized, the Wickr application was locked and protected, requiring TERRY's biometric facial recognition to gain access. Your Affiant respectfully requests access to TERRY's biometric facial recognition to search for the items specified in Attachment A, and to seize all items listed in Attachment B as evidence of the above criminal violations.

5. The statements contained in this affidavit are based in part on information provided by FBI Special Agents, written reports received by your Affiant about this investigation directly or indirectly from other law enforcement agents, information gathered from the service of administrative subpoenas, the results of physical and electronic surveillance conducted by law enforcement agents, independent investigation and analysis by FBI agents/analysts and computer forensic professionals, and my experience, training and background as a Special Agent with the FBI.

6. Because this affidavit is being submitted for the limited purpose of obtaining the requested search warrant, your Affiant has not included each and every fact known concerning this investigation. Instead, your Affiant has set forth only the facts believed to be necessary to establish probable cause for the issuance of the requested warrant.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Based on my training and experience in child exploitation investigations, I am aware that computers (to include cellular telephones), computer technology, and the Internet significantly facilitate child pornography offenses. Computers generally serve five (5) functions in connection with child exploitation offenses: production, communication, distribution, storage,

and social networking. Child pornography offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, including covert recording equipment, images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Therefore, through use of the Internet, electronic contact can be made to literally millions of computers and/or cellular devices around the world and used as an instrument to engage in criminal activity.

8. A computer's ability to store images in digital form makes the computer and/or cellular device itself an ideal repository for child pornography and content associated with the sexual exploitation of children. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown significantly within the last several years. These drives can store thousands of images at very high resolution. In addition, electronic devices such as smartphones, connected devices, e-readers, and tablets now function essentially as computers with the same abilities to store images in digital form.

9. The Internet and social media applications afford collectors of child pornography several different venues for obtaining, viewing, trading, and producing child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to request, retrieve, and store child pornography, including, but not limited to, services offered by Internet portals such as Yahoo and Google. These 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 or device with access to the Internet, and evidence of such online storage of child pornography is often found on the user's computer or device.

10. Popular social media applications such as Wickr are commonly used as platforms to sexually entice minors and produce child pornography. These applications require a user to create a username and password to access content that may be stored exclusively in the application itself. Further, some applications, if accessed with newer generations of cellular devices such as models of Apple iPhone (iPhone X and beyond), may in some cases utilize biometric information to protect not only the device itself, but applications contained on the device.

11. Even when such files containing evidence of child sexual exploitation or other criminal activity have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside on the hard drive in space that is not allocated to an active file for long periods of time before they are overwritten. A computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

12. Additionally, files that have been viewed on the Internet are automatically downloaded into a temporary Internet directory or "cache." Browsers typically maintain a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Therefore, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, and more on the user's operating system, storage capacity, and computer habits.

13. Many digital electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners,

facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

14. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Most devices offer a feature that allows the user to store a finite number of fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's fingerprint sensor. The location of the fingerprint sensor may vary depending on the model of device.

15. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

16. Per Apple Support, Face ID provides intuitive and secure authentication enabled by the state-of-the-art TrueDepth camera system with advanced technologies to accurately map the geometry of your face. With a simple glance, Face ID securely unlocks your iPhone or iPad Pro. You can use it to authorize purchases from the iTunes Store, App Store, and Book Store, payments with Apple Pay, and more. Developers can also allow you to use Face ID to sign into their apps. Apps that support Touch ID automatically support Face ID.

17. Per publicly available research, both the Apple and Wickr application support this secure method of “locking” accessibility.

18. Users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

19. As discussed in this Affidavit, your Affiant has reason to believe there may be information pertaining to the aforementioned violations of child exploitation currently located in TERRY’s Apple iPhone 11, within the Wickr application, which is currently secured and require TERRY’s biometric facial recognition to access the content. Due to the security measures put in place on these aspects of the device, law enforcement personnel may not otherwise be able to access the data contained within the applications, making the use of biometric features necessary to the execution of the search authorized by Search Warrant Case No. 3:22-MJ-2117 issued on June 29, 2022.

20. The aforementioned Wickr application was previously identified simply as “messaging platform” in paragraph 19 of the Search Warrant Application in Case No. 3:22-MJ-2117.

21. Therefore, lawful access to TERRY is requested in order to hold the communication device (TERRY’s Apple iPhone 11) in front of the face of TERRY to activate the facial recognition feature for the purpose of attempting to unlock the communication device in order to search the contents as authorized by warrant 3:22-MJ-2117.

22. The facts set forth in this affidavit establish probable cause to believe that TERRY's Apple iPhone 11, its storage devices, downloaded social media applications, and other system components were used as a means of committing offenses involving the criminal exploitation of children. Accordingly, I request access to TERRY's biometric facial recognition to search for the items specified in Attachment A, and to seize all items listed in Attachment B as evidence of the above criminal violations.

PROBABLE CAUSE

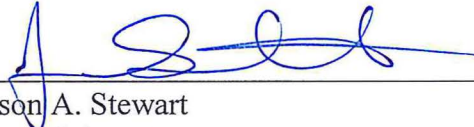
23. On July 6, 2022, TERRY was arrested by FBI Knoxville. An Apple iPhone 11, Model: A2111, IMEI:353973103887825 in a blue Buffalo Bills NFL case, (hereinafter TERRY's phone) was located on his person and seized for the purpose of searching pursuant to Search Warrant Case No. 3:22-MJ-2117 (herein incorporated and attached as Exhibit A). TERRY's phone was in an open and unlocked state when it was initially seized. However, during the initial forensic review of TERRY's phone, it became apparent that certain applications (Wickr) in TERRY's phone were locked and required biometric data to access the data necessary to complete the execution of search warrant 3:22-MJ-2117. In my training and experience, individuals may place security features on different applications, documents, or notes on their electronic devices so they (and they alone) may access them. This data may be secured with passwords, multi-factor authentication, fingerprint, or facial recognition software.

24. By the time it was made known to the FBI that facial recognition was needed to access the locked application Wickr, TERRY had asked for an attorney. Therefore, the United States seeks this additional search warrant seeking TERRY's biometric facial recognition is requested to complete the search of TERRY's Apple iPhone, 11.

CONCLUSION

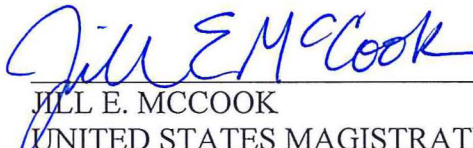
25. Based on the information set forth in this affidavit, there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of, and property designed for use in committing the violations of 18 U.S.C. § 2252A(a)(2) – Distribution of Child Pornography; 18 U.S.C. § 2252A(a)(5)(B) - Possession of Child Pornography are presently located on the **SUBJECT DEVICE**, as described in Attachment A, and the digital media therein.

26. Accordingly, I respectfully request that this Court authorize Agents to compel the **SUBJECT PERSON, CHRISTOPHER MICHAEL TERRY**, to provide the specific biometrics, namely the facial recognition feature to unlock the Wickr, so that Agents may seize the items listed in Attachment B.



Jason A. Stewart
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 7th day of July, 2022.



JILL E. MCCOOK
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The person of **CHRISTOPHER MICHAEL TERRY**, described as a white male, date of birth of April 26, XXXX, social security account number XXX-XX-5039, with specific regard to his facial recognition biometric data points.

ATTACHMENT B
Particular Things To Be Seized

Located on the **SUBJECT PERSON** to be searched, I seek to seize biometric facial recognition data points in order to obtain evidence, fruits, and instrumentalities of the aforementioned criminal violations believed to be located within the locked Wickr application and other locked messaging applications on TERRY's Apple iPhone 11, Model: A2111, IMEI:353973103887825 in a blue Buffalo Bills NFL case, which could contain CSAM.

UNITED STATES DISTRICT COURT

for the Eastern District of Tennessee



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

RESIDENTIAL PROPERTY LOCATED AT 2080 CECIL JOHNSON ROAD, APARTMENT D, KNOXVILLE, TENNESSEE 37921 AND THE PERSON CHRISTOPHER MICHEAL TERRY. Photographs and property descriptions are attached hereto as Attachment A and fully incorporated herein.

Case No. 3:22-MJ-2117

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):

RESIDENTIAL PROPERTY LOCATED AT 2080 CECIL JOHNSON ROAD, APARTMENT D, KNOXVILLE, TENNESSEE 37921 AND THE PERSON CHRISTOPHER MICHEAL TERRY. Photographs and property descriptions are attached hereto as Attachment A and fully incorporated herein.

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

PLEASE SEE ATTACHMENT B, WHICH IS ATTACHED HERETO AND FULLY INCORPORATED HEREIN.

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

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

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Rows: 18 U.S.C. § 2252A(a)(1)(2) Distribution of Child Pornography; 18 U.S.C. § 2252A(a)(5)(B) Possession of Child Pornography

The application is based on these facts:

Please see the Affidavit of Special Agent Jason Stewart which is attached hereto and incorporated herein.

- checked Continued on the attached sheet. unchecked 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.

Handwritten signature of Jason Stewart

Jason Stewart, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 6-29-22

Handwritten signature of J. M. E. McCook

Judge's signature

City and state: Knoxville, Tennessee

United States Magistrate Judge

Printed name and title

3:22-MJ-2117

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Your affiant, Jason Stewart, a Special Agent of the Federal Bureau of Investigation (FBI) being duly sworn, deposes and states the following:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent since May of 2017. I am currently assigned to the Violent Crime Squad at the Knoxville Field Office of the FBI. My primary duties and responsibilities involve the investigation of violations of federal law including violent crime as found in Title 18 of the United States Code and the Controlled Substances Act as found in Title 21 of the United States Code. Prior to serving with the FBI, I was an officer in the United States Army for eight years, and a police officer with the Knoxville Police Department in Tennessee for two years. I have investigated federal criminal violations including bank robbery, violent crime and gangs, drug trafficking organizations, criminal enterprises, and violent crimes against children. I have received formal training in investigations at the Knoxville Police Academy in Tennessee, and the FBI Academy in Quantico, Virginia. As an FBI Special Agent, I am authorized to investigate violations relating to child exploitation and child pornography, including the production, transportation, receipt, distribution, and possession of child pornography, in violation of 18 U.S.C. §§ 2251 and 2252A, as well as the enticement and coercion of minors, in violation of 18 U.S.C. § 2422(b). I have gained experience in conducting these investigations through training and through everyday work, including executing search warrants and interviewing individuals who trade child pornography and who seek to sexually exploit children. As part of my training and experience, I have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in multiple forms of media. I have been trained by the FBI in the acquisition, imaging, extraction, and analysis of digital

evidence from computers, cellular telephones, and other electronic devices. I have also been trained by the FBI in digital image and video recovery. I have attended several courses on cybersecurity and cyber investigations provided by the FBI and private industry.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of the following statutes:

- a) 18 U.S.C. § 2252A(a)(2) – Distribution of Child Pornography;
- b) 18 U.S.C. § 2252A(a)(5)(B) - Possession of Child Pornography are located on and/or within the following:
 - i. The property and premises 2080 Cecil Johnson Road, Apartment D, Knoxville, Tennessee 37921 (**SUBJECT RESIDENCE**).
 - ii. The person of CHRISTOPHER MICHAEL TERRY (TERRY) described as a white male, approximately 5’9” in height, weight 185 pounds, having blue eyes and brown hair, and having a date of birth of April 26, 1969 (**SUBJECT PERSON**).

3. I submit this application and affidavit in support of a search warrant authorizing a search of the **SUBJECT RESIDENCE** and the **SUBJECT PERSON**, as further described in Attachments A1 and A2, incorporated herein by reference. The **SUBJECT RESIDENCE** and the **SUBJECT PERSON** are located in the Eastern District of Tennessee.

4. Located within the **SUBJECT RESIDENCE** to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire **SUBJECT RESIDENCE**, including the residential dwelling and any computer, any computer media, and any communication devices including but not limited to any wireless telephones, located therein where the items specified in Attachment B1 may be found.

5. Located on the **SUBJECT PERSON** to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search those areas of the **SUBJECT PERSON** where any computer, computer media, and any communication devices including but not limited to any wireless telephones may be located for the items specified in Attachment B2, and to seize all items listed in Attachment B2 as contraband and instrumentalities, fruits, and evidence of crime.

6. The statements contained in this affidavit are based in part on information provided by FBI Special Agents, written reports received by your Affiant about this and other investigations your Affiant directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas, the results of physical and electronic surveillance conducted by law enforcement agents, independent investigation and analysis by FBI agents/analysts and computer forensic professionals, records from the Tennessee Department of Motor Vehicles (DMV), the National Crime Information Center (NCIC), and my experience, training, and background as a Special Agent with the FBI and as a law enforcement officer.

7. Because this affidavit is being submitted for the limited purpose of obtaining the requested search warrant, your Affiant has not included each and every fact known to your Affiant concerning this investigation. Instead, your Affiant has set forth only the facts believed by your Affiant to be necessary to establish probable cause for the issuance of the requested warrant.

DEFINITIONS

8. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256 apply to this affidavit and Attachment B:

- a) “Computer” refers to any electronic, magnetic, optical, electrochemical, or other high-speed data processing device capable of performing logical or storage functions and includes any data storage facility or communications facility directly related to such a device. As used herein, “computer” also incorporates digital devices that complete these same functions, such as smartphones, tablets, connected devices, and e-readers. See 18 U.S.C. § 1030(e)(1).
- b) “Computer hardware” consists of all equipment that 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).
- c) “Computer passwords and data security devices” 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 what might be termed a 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.

- d) “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 assigns a different unique number to a computer every time it accesses the Internet. IP addresses may also be static, which means the provider assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.
- e) “Mobile applications” or “mobile apps” are computer programs or software applications specifically designed to run on mobile devices (e.g., smartphones, tablets, e-readers, etc.). Mobile applications are generally downloaded from application distribution platforms operated by specific mobile operating systems, like App Store (Apple mobile devices) or Google Play Store (Android mobile devices). “Instant messaging” is a type of communication that offers real-time text transmission over the Internet. Instant messaging generally involves short messages which are transmitted between two or more parties. Various social networking, dating and gaming websites and mobile applications offer instant messaging for users to communicate amongst

themselves. More advanced features of instant messaging include push technology to provide real-time text, and the ability to send/receive digital files, clickable hyperlinks, and video chat.

- f) The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, both visually or aurally, and by any means, whether in handmade form (including, but not limited to: writings, drawings, and paintings), photographic form (including, but not limited to: microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to: phonograph records, printing, or 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 or DVD’s, Personal Digital Assistants (PDAs), Multimedia Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

9. The facts contained in this affidavit establish probable cause to believe that an individual using the Internet services at the **SUBJECT RESIDENCE** has transported and possessed child pornography, or has attempted to commit these crimes, in violation of federal law. Based on my training, experience, and numerous interviews of subjects who admitted to

having a sexual interest in children, I am aware that the following characteristics are common to individuals involved in child pornography offenses:

- a) Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity;
- b) Such individuals may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. These individuals often maintain this material for sexual arousal and gratification. Furthermore, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts;
- c) Such individuals often possess and maintain copies of child pornographic material, including but not limited to pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, in the privacy and security of their home. Prior investigations into these offenses have shown that child pornography offenders typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years;
- d) Such individuals often begin their child pornography collections by obtaining child abuse material through various free avenues afforded by the Internet, like peer-to-peer file sharing and various free websites and mobile

applications. Thereafter, these individuals may escalate their activities by producing and/or distributing child pornography, for the purpose of trading this material to add to their own child pornography collection;

- e) Such individuals often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer or surrounding area. These collections are often maintained for several years and are maintained at the individual's residence or place of employment, to afford immediate access to view the material;
- f) Such individuals may correspond with others to share information and material, and rarely destroy this correspondence. These individuals often maintain lists of names, email addresses and telephone numbers of others with whom they have been in contact regarding their shared interests in child pornography.

10. Based on my training and experience in child exploitation investigations, I am aware that collectors of child pornography prefer not to be without their child pornographic material for a prolonged period of time. This behavior has been documented by law enforcement officers involved in child pornography investigations throughout the world. Accordingly, if the offender associated with the offenses under investigation uses a mobile device to access, distribute and/or possess child pornography, it is more likely than not that evidence of this access will be found in his home at the time the requested warrant will be executed.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

11. Based on my training and experience in child exploitation investigations, I am aware that computers, computer technology, and the Internet significantly facilitate child

pornography offenses. Computers generally serve five (5) functions in connection with child exploitation offenses: production, communication, distribution, storage and social networking. Child pornography offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Therefore, through use of the Internet, electronic contact can be made to literally millions of computers around the world.

12. 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 (commonly referred to as the hard drive) used in home computers has grown significantly within the last several years. These drives can store thousands of images at very high resolution. In addition, electronic devices such as smartphones (e.g., Apple iPhones, Samsung Galaxy), connected devices (e.g., Apple Watch), e-readers, and tablets (e.g., Apple iPads, Kindle Fire) now function essentially as computers with the same abilities to store images in digital form.

13. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including, but not limited to, services offered by Internet portals such as Yahoo and Google. These 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 or device with access to the Internet, and evidence of such online storage of child pornography is often found on the user's computer or device.

14. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside on the hard drive, in space that is not allocated to an active file for long periods of time before they are overwritten. A computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

15. Additionally, files that have been viewed on the Internet are automatically downloaded into a temporary Internet directory or "cache." Browsers typically maintain a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Therefore, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed, and more on the user's operating system, storage capacity, and computer habits.

SPECIFICS REGARDING THE SEARCH AND SEIZURE OF COMPUTERS

16. Based on my training and experience, I am aware that the search of computers often requires agents to seize most of the computer items (e.g., hardware, software, and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is essential to the search for electronic evidence because of the following facts:

- a) Computer storage devices, like hard drives, diskettes, tapes, or laser disks, store the equivalent of thousands of pages of information. When the user wants to conceal electronic evidence of a crime, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all

of the stored data to determine whether it is included within the scope of warrant. This process can take weeks or months, depending on the volume of the stored data, and it would be impractical to attempt this kind of data search on-site;

- b) Searching computer systems for criminal evidence is a highly technical process that requires expert skills and a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in specific systems and applications. It is difficult to know prior to a search which expert should analyze the system and its data. The search of a computer system can be equated to a scientific procedure, which is designed to protect the integrity of the evidence while recovering hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction, both from external sources and from code embedded in the system as a “booby-trap,” the controlled environment of a laboratory is essential to its complete and accurate analysis;
- c) In order to fully retrieve data from a computer system, an analyst needs all magnetic storage devices, as well as the central processing unit (CPU). For child pornography investigations, in which the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. The analyst needs all assisting software (e.g., operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data, as well as all related instructional manuals, documentation and security devices;

d) Searching computerized information for evidence or instrumentalities of a crime often requires the seizure of the entire computer's input/output periphery devices, including related documentation, passwords and security devices, so that a qualified examiner can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored 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; therefore, it is important that the analyst be able to properly retrieve the evidence sought.

17. The facts set forth in this affidavit establish probable cause to believe that a computer (including tablets and smartphones), its storage devices, and other system components were used as a means of committing offenses involving the sexual exploitation of minors, in addition to storing evidence of said crime. Accordingly, I seek the authorization to seize and search any computers and related electronic devices located at the **SUBJECT RESIDENCE** and on the **SUBJECT PERSON**, consistent with Attachment B to the requested warrant.

18. Based on my training and experience, I am aware that members of a household may jointly use electronic devices, and that some targets will use electronic devices belonging to other family members in order to disguise their illegal activity. Accordingly, FBI personnel will conduct on-scene searches of all household members' electronic devices but will only seize devices containing or suspected to contain contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) - Distribution of Child Pornography and 2252A(a)(5)(B) - Possession of Child Pornography.

BACKGROUND OF THE INVESTIGATION

19. On November 9, 2021, an FBI Online Covert Employee (OCE) was monitoring a group chat called "[REDACTED]" on the messaging platform ¹. The OCE observed the messaging platform user "jonjay862" post a link (hereinafter, the Link) in the © [REDACTED] group chat to a cloud storage service (CSS)² that is known to the FBI. Your affiant knows through training and experience that this particular CSS is commonly used in the child sexual offender (CSO) community to share child sexual abuse material (CSAM), also known as child pornography. The CSS allows a user to share files privately to specified users, or publicly where anyone with the web address to the link can view and access the files. The OCE accessed the Link shared by jonjay862 and discovered the Link contained at least twenty-three CSAM videos. The OCE downloaded seven of the videos to preserve as evidence. The OCE and your affiant reviewed the seven preserved videos and believe, based on training and experience, they contain CSAM.

SUMMARY OF THE CHILD PORNOGRAPHY VIDEOS

20. One video, [REDACTED]

[REDACTED]

¹ The specific messaging platform is a free-to-use messaging application that allows users to send and receive text messages, share images, video, files, voice memos, and make voice calls. The specific messaging platform is end-to-end encrypted, meaning the content is generally unable to be intercepted by law enforcement.
² The cloud storage service (CSS) provides user-controlled encrypted cloud storage. The CSS allows users to store images, videos, and other files, as well as share CSS content via public and/or private links as well as through a chat feature.



IDENTIFICATION OF CHRISTOPHER MICHAEL TERRY

21. The FBI sent a request for information to a foreign law enforcement partner with access to the CSS's records. The CSS provided basic subscriber information for the user who created the Link to the foreign law enforcement partner, who in turn shared it with FBI. The CSS records revealed the user who created the Link had userhandle "g_K4jil1_Yj0", email address "christophermterry79@gmail.com", first name "Christopher", last name "Terry", and telephone number +1 865-387-8479. The CSS subscriber information for g_K4jil1_Yj0 included an outgoing contact request sent to "cinebunk79@gmail.com". The CSS subscriber information for g_K4jil1_Yj0 also listed the Link in a list of approximately ninety-five additional CSS links shared with the public that belonged to g_K4jil1_Yj0's CSS account. The g_K4jil1_Yj0 account records also included IP address history for account logins. The FBI identified some of g_K4jil1_Yj0's account's IP addresses were assigned to Comcast and Verizon. Your affiant knows based on training and experience that Comcast and Verizon usually maintain records for their subscribers. The FBI issued subpoenas to Comcast and Verizon for a few of those IPs from the g_K4jil1_Yj0 account IP logs.

22. The FBI issued an administrative subpoena to Verizon for IP addresses 174.253.128.35 on January 11, 2021, 174.250.145.25 on March 12, 2021, and 174.253.129.223 on September 23, 2021, as well as subscriber information for telephone number 865-387-8479. Verizon records showed all three IP addresses were from a NATTING ROUTER³, which

³ A NATTING ROUTER IP is an IP address that can have many users at the same time.

included 865-387-8479 as one of the assigned users of the IP addresses. Verizon records showed telephone number 865-387-8479 was assigned to the Verizon-owned pre-paid wireless carrier TracFone but was unable to provide further subscriber information, such as the name and address, for the customer. Your affiant knows based on training and experience that pre-paid wireless carriers like TracFone often do not require or verify identifying information for their customers. Of note, the FBI initially requested for records for two additional IP addresses from Verizon, however they were out of scope for Verizon's records retention time period.

23. The FBI issued an administrative subpoena to Comcast for records associated with IP address 67.187.78.162 used on July 14, 2021, October 31, 2021, and November 8, 2021, as well as IP address 2601:840:8402:58f0:5dda:19fd:619c:1ff3, June 19, 2021. Comcast records showed all IP addresses listed above were assigned to Comcast customer Christopher Terry (TERRY), address 2080 Cecil Johnson Rd Suite D, Knoxville, Tennessee 37921 (same as the **SUBJECT RESIDENCE**), telephone number 865-381-8419, and email address christophermterry79@comcast.net.

24. The FBI sent an administrative subpoena to Google requesting subscriber information for christophermterry79@gmail.com. Google records showed the account name as Christopher Terry, recovery email address cinebunk79@gmail.com, recovery telephone number +1 865-387-8479, and sign-in phone number +1 865-387-8479. Your affiant notes IP address 174.250.145.25 was also present in the IP logs of the Google account on March 12, 2021; the same date that particular IP address was present on the records of the g_K4jil1_Yj0 account.

25. Throughout this investigation records provided to the FBI by Comcast, Verizon, Google, and the CSS, as described above, have each been linked to TERRY's residence, telephone number, and/or email addresses.

26. TERRY's criminal history includes a prior conviction of Possession of Child Pornography and Use Of A Computer To Entice A Child To Engage In Sexual Activity in July 2004. TERRY's sex offender registry number is 00559046. TERRY's Tennessee Bureau of Investigation (TBI) sexual offender registry information shows his residential address as 2080 Cecil Johnson Road D, Knoxville, TN 37921 (same as **SUBJECT RESIDENCE**), his registered vehicle as a 2003 blue Chevrolet Cavalier with Tennessee tag 7G46G6⁴, his email addresses provided are cinebunk79@gmail.com and christophermterry79@gmail.com (the same email addresses associated with the g_K4jill_Yj0 account), and his telephone number as 865-387-8479 (the same Verizon/TracFone number as seen above). The sex offender registry lists TERRY's employer as a restaurant located at Bob Kirby Road in Knoxville, Tennessee. A Knoxville Police Department (KPD) Investigator contacted TERRY via text message in January 2021 when TERRY requested to update his address information for the sex offender registry. The KPD Investigator communicated with TERRY using telephone number 865-387-8479.

27. TERRY's Tennessee driver license lists his address as the **SUBJECT RESIDENCE**. Tennessee DMV records show TERRY has a 2003 blue Chevrolet Cavalier, Tennessee tag 7G46G6, registered to him at the **SUBJECT RESIDENCE**. On the afternoon of February 7 and the morning of February 8, 2022, your affiant observed TERRY's Cavalier parked outside the **SUBJECT RESIDENCE**.

28. The FBI issued an administrative subpoena to Comcast on February 10, 2022, requesting updated subscriber information for the **SUBJECT RESIDENCE**. On February 16, 2022, Comcast provided records showing TERRY is still the subscriber for the **SUBJECT RESIDENCE**. The updated Comcast records listed TERRY's telephone number as 865-387-

⁴ The registration on TERRY's vehicle has the subject's residence associated with the vehicle.

8479; a different number than the previous Comcast records, and the same Verizon/TracFone number that accessed the g_K4jil1_Yj0 account. The FBI issued two additional subpoenas to Comcast in March and April 2022, confirming TERRY was still the subscriber for the **SUBJECT RESIDENCE** as of April 22, 2022.

29. On the morning of May 19, 2022, TERRY's vehicle, described in paragraph 27, was observed parked outside the **SUBJECT RESIDENCE**.

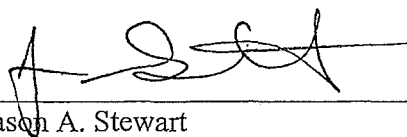
MOBILE COMMUNICATION DEVICES

30. Your Affiant knows from training and experience that modern digital devices such as cellular telephones, tablets, and other communication devices are extremely portable. With the advancements in processing power and storage capacity, many of these devices operate similar to stand alone "desktop" type computers. Application developments, communication capabilities and portability have made these devices an indispensable part of everyday life. Persons who have these devices, particularly cellular telephone type platforms, typically keep them on their persons or in other readily available locations. Your Affiant believes that the inherent portability of modern digital devices combined with evidence to believe **SUBJECT PERSON** accessed the cloud storage service and the messaging application outlined above on a mobile device from multiple locations give probable cause to believe that the items referenced in Attachment B1 for **SUBJECT RESIDENCE** could also be located on the **SUBJECT PERSON**.

CONCLUSION

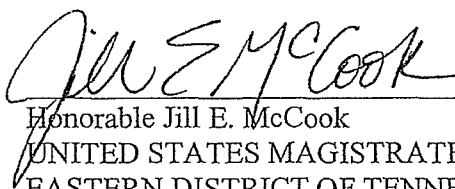
31. Based on the information set forth in this affidavit, there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of, and property designed for use in committing violations of 18 U.S.C. § 2252A(a)(2)- Distribution of Child Pornography; and 18

U.S.C. §§ 2252A(a)(5)(B) Possession Child Pornography, are presently located at the **SUBJECT RESIDENCE**, 2080 Cecil Johnson Road, Apartment D, Knoxville, Tennessee, and/or on the **SUBJECT PERSON**, Christopher Terry, as described in Attachment A1 and Attachment A2, and the digital media therein. Accordingly, I respectfully request that this Court authorize the search of this residence and person so that agents may seize the items listed in Attachment B1 and B2.



Jason A. Stewart
Special Agent
Federal Bureau of Investigation

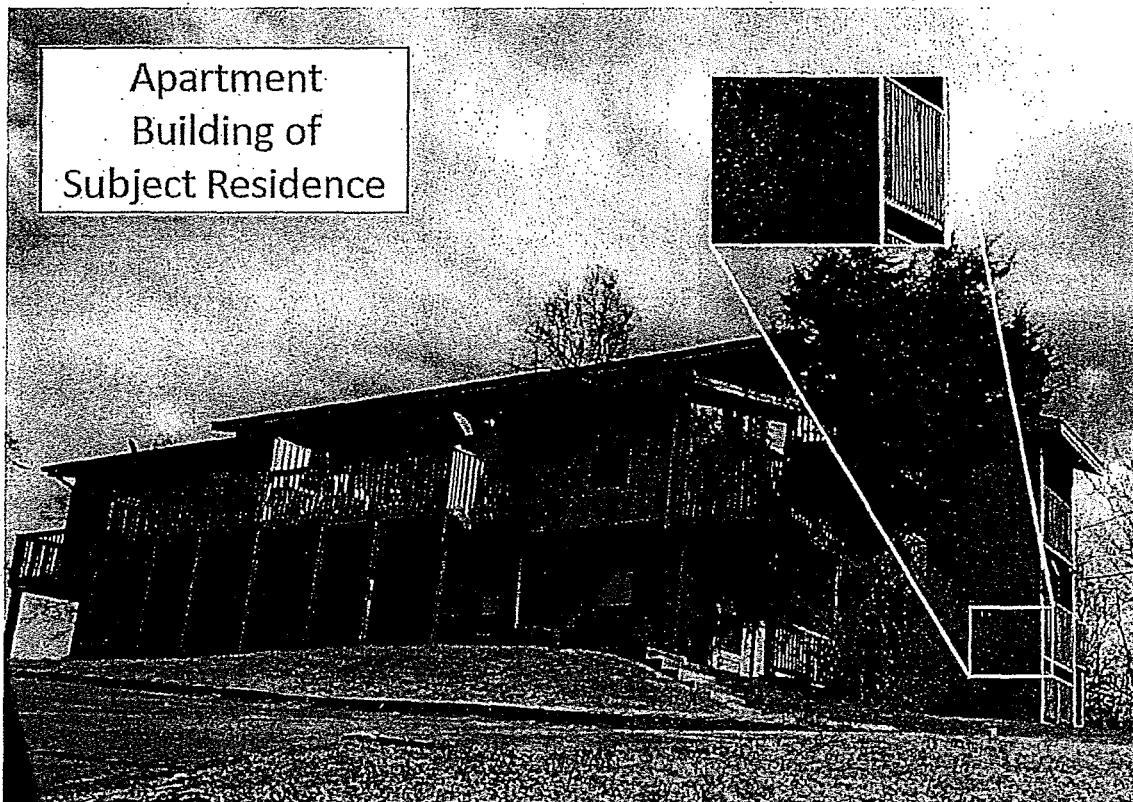
Subscribed and sworn to before me on June 29, 2022.

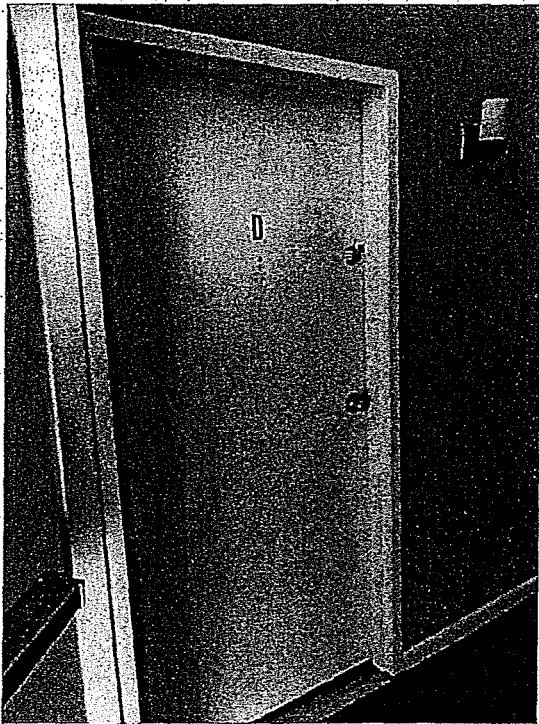
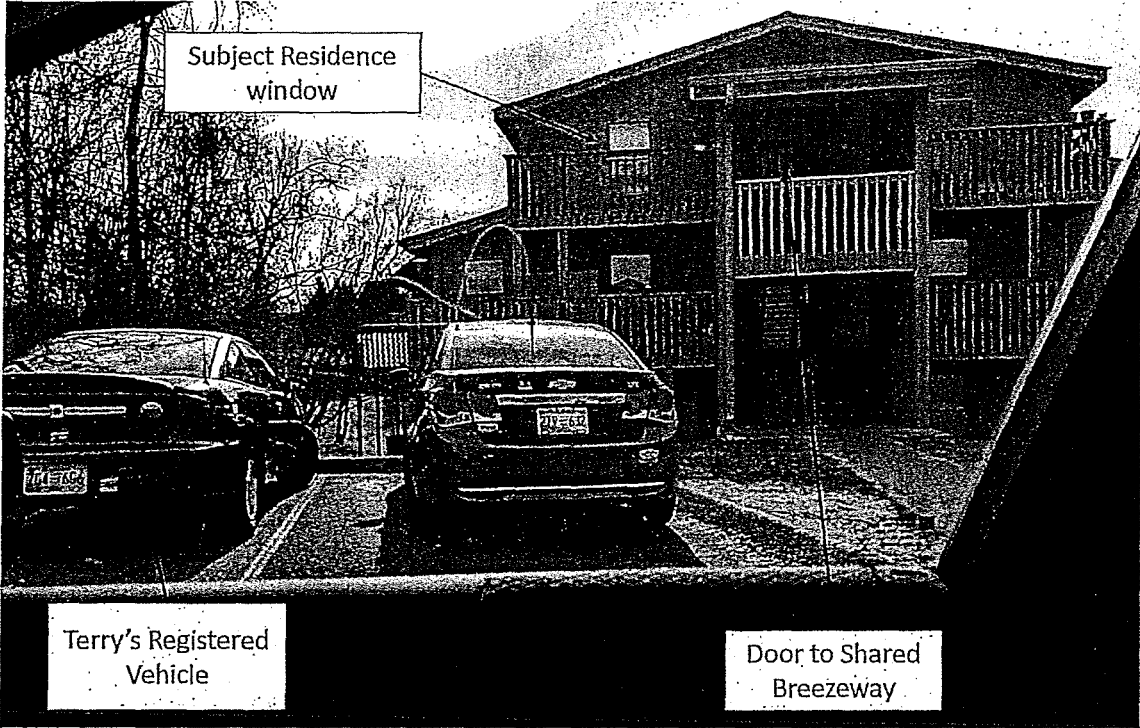


Honorable Jill E. McCook
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF TENNESSEE

ATTACHMENT A1

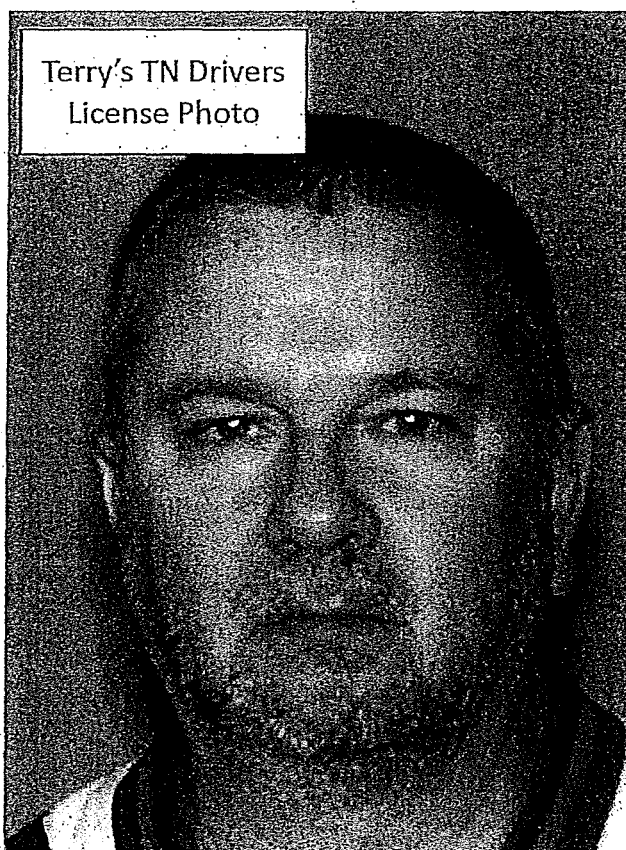
The SUBJECT RESIDENCE is located at 2080 Cecil Johnson Road, Apartment D, Knoxville, Tennessee 37921. The SUBJECT RESIDENCE is an apartment on the third story of a brown or tan colored, stand-alone building containing multiple apartments. The side of the apartment building is labeled with the numbers "2080". The SUBJECT RESIDENCE is located on the northeast corner of the apartment building. The door to the SUBJECT RESIDENCE is white, is labeled with the letter "D", and opens to a shared breezeway.





ATTACHMENT A2

The person of Christopher Michael Terry, described as a white male, approximately 5'9" in height, weight 185 pounds, having blue eyes and brown hair, and having a date of birth of April 26, 1969 (SUBJECT PERSON).



ATTACHMENT B1

Within the **SUBJECT RESIDENCE** to be searched, I seek to seize evidence, fruits, and instrumentalities of the aforementioned criminal violations. I request authority to search the entire **SUBJECT RESIDENCE**, including the residential dwelling and any computer, any computer media, and any communication devices including but not limited to any wireless telephones, and removable media that may contain evidence of Possession and Distribution of Child Pornography. **SUBJECT RESIDENCE** to include any place where child pornography material(s) could be hidden, including, but not limited to: rooms; furniture within the Premises; underneath a postage stamp (micro USB card); drawers (kitchen cabinet, bedroom furniture, etc.); suspended ceiling; attic; clothing pockets; socks; shoes; backpack; satchel; briefcase; etc.

Due to the potential for this location to have multiple parties residing on the premises, all electronic devices will be previewed on scene using forensic software. Those devices determined not to contain CSAM will be left on scene.

I request authority to search those areas of the **SUBJECT RESIDENCE** where any computer, computer media, and any communication devices including but not limited to:

1. Any wireless telephones removable media, storage media that may contain evidence of the possession and distribution of child pornography.
2. Child Pornography in any form.
3. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, Section 2256(8).
4. Any and all correspondence identifying persons transmitting, through interstate commerce including the United States mail or computers, any visual depiction of minors

engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

5. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

That could be found on the **SUBJECT RESIDENCE**.

ATTACHMENT B2

Located on the **SUBJECT PERSON** to be searched, I seek to seize evidence, fruits, and instrumentalities of the aforementioned criminal violations. I request authority to search those areas of the **SUBJECT PERSON** where any computer, computer media, and any communication devices including but not limited to:

1. Any wireless telephones, computers, removable media or storage media that may contain evidence of the possession and distribution of child pornography.
2. Child Pornography in any form.
3. Any and all correspondence identifying persons transmitting, through interstate commerce including the United States mail or computers, any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

That could be found on the **SUBJECT PERSON**.

Said electronic devices of the size that may be located on a person, to include, but not limited to, entire outside of the body, clothing, shoes and accessories thereon and/or attached thereto, all areas touching his body, excluding body cavities.

UNITED STATES DISTRICT COURT

for the Eastern District of Tennessee



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

Case No. 3:22-MJ-2117

RESIDENTIAL PROPERTY LOCATED AT 2080 CECIL JOHNSON ROAD, APARTMENT D, KNOXVILLE, TENNESSEE 37921 AND THE PERSON CHRISTOPHER MICHEAL TERRY. Photographs and property descriptions are attached hereto as Attachment A and fully incorporated herein.

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 Eastern District of Tennessee (identify the person or describe the property to be searched and give its location):

RESIDENTIAL PROPERTY LOCATED AT 2080 CECIL JOHNSON ROAD, APARTMENT D, KNOXVILLE, TENNESSEE 37921 AND THE PERSON CHRISTOPHER MICHEAL TERRY. Photographs and property descriptions are attached hereto as Attachment A and fully incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

PLEASE SEE ATTACHMENT B, WHICH IS ATTACHED HERETO AND FULLY INCORPORATED HEREIN.

YOU ARE COMMANDED to execute this warrant on or before July 13, 2022 (not to exceed 14 days) in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good 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 Jill E. McCook (United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), 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: 6-29-22 2:35pm

Jill E. McCook Judge's signature

City and state: Knoxville, Tennessee

United States Magistrate Judge Printed name and title