COPY

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS
SPRINGFIELD DIVISION

IN THE MATTER OF THE SEARCH OF "Daugherty Devices" Further Described in Attachment A, currently located at 900 E. Linton Ave, Springfield, IL (Federal Bureau of Investigation (FBI))	Case No. _____ **Filed Under Seal**

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Anthony Wright, being duly sworn and deposed state:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of electronic devices—herein referred to as the "Daugherty Devices"—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent for the Federal Bureau of Investigation (FBI,) and have been since May 2019. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to violent crimes against

children as well as violations involving child pornography and exploitation pursuant to violations of Title 18, United States Code, Sections 2251 and 2252. I have gained experience in conducting such investigations through work experience and in class trainings. I have been involved in multiple arrests related to child exploitation investigations. 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 courts. I have participated in the execution of multiple federal search warrants, as well as the review of electronic data seized from electronic devices.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

3. The property to be searched (hereinafter referred to as the ***Daugherty Devices***) are described as follows:

a. A Black and blue desktop hard drive, Seagate, serial number NA7DWTK4;

b. Cyperton computer tower, serial number GA-789MT-USB3;

c. 1 white USB drive, 2 black USB drives, and 1 blue USB;

d. Compaq computer, serial number CNH4520P00;

e. Gateway 7320 laptop, serial number N3451-710-03782.

These devices are currently located at the FBI Springfield Office, located at 900 E. Linton Ave, Springfield, Illinois.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. The applied-for warrant would authorize the forensic examination of the ***Daugherty Devices*** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. The ***Daugherty Devices*** are currently in the lawful possession of the FBI. The devices came into the FBI's possession in the following way: on March 21, 2018, the Taylorville Police Department seized the ***Daugherty Devices*** from Todd Eugene Daugherty based on a state search warrant related to threats of a mass shooting against Memorial Elementary School in Taylorville, Illinois made by Daugherty. The search warrant authorized the search and seizure of any and all computers, as defined in 720 ILCS 5/16D-2.

7. On April 6, 2018, Taylorville Police Department requested the FBI's assistance in analyzing digital data from the ***Daugherty Devices*** in order to further investigate the Memorial Elementary School shooting threat.

8. While reviewing the electronics for evidence related to the mass shooting threats, FBI Senior Forensic Examiner William O'Sullivan found suspected child pornography on the black and blue Seagate desktop hard drive, bearing serial number NA7DWTK4. William O'Sullivan has been a Forensic Examiner for over 10 years. O'Sullivan witnessed an obscene visual depiction of a three to five-year-old child with an adult male's penis in his mouth.

9. However, because the original search warrant did not authorize a search for child pornography, Examiner O'Sullivan halted his search so that a search warrant requesting authority to search for child pornography could be obtained. Therefore, while the FBI might already have all necessary authority to examine the ***Daugherty Devices***, I seek this additional warrant out of an abundance of caution to be certain that an examination of the devices will comply with the Fourth Amendment and other applicable laws.

10. Through my training and experience, I have seen individuals who collect, receive, distribute, transport and/or possess child pornography often maintain their collections in digital or electronic format in a safe, secure and private environment, such as a computer and/or any other electronic media that may be found in the surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to easily view the collection, which is highly valued.

11. The other electronic devices were found and seized near the black and blue Seagate Hard drive that had the suspected child pornography, thus there is a reasonable belief that depictions of child pornography would be on the other electronic devices as well.

12. The ***Daugherty Devices*** are currently in storage at 900 E. Linton Ave, Springfield, Illinois. In my training and experience, I know that the ***Daugherty Devices*** have been stored in a manner in which the devices contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of the FBI.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

13. Based upon my knowledge, experience and consultation with other Special Agents and law enforcement officers, I am aware that child pornography distributors/collectors:

a. Receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies, they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or other visual media) or from literature describing such activity.

b. Collect sexually explicit or suggestive materials (hard-core and soft-core pornography, whether of adults and/or children) in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

c. Almost always possess and maintain their material (pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, child erotica, etc.) in the privacy and security of their homes or some other secure location. Child

pornography distributors/collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years, and store their child pornography amongst other, otherwise legal, media or files.

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

e. Individuals who collect, receive, distribute, transport and/or possess child pornography often maintain their collections in digital or electronic format in a safe, secure and private environment, such as a computer and/or any other electronic media that may be found in the surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to easily view the collection, which is highly valued.

f. Individuals who collect, receive, distribute, transport and/or possess child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. There is probable cause to believe that things that were once stored on the Daugherty Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage

medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because 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 storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this

evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Daugherty Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Daugherty Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat

programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that

can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Daugherty Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a

premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. Based upon the affiant's review of information collected by the affiant and by Senior Forensic Examiner William O'Sullivan, I believe there is Probable Cause to search the electronic devices listed in this search warrant.

20. The affiant has set forth the facts that I believe are necessary to establish probable cause to believe that additional evidence of violations of Title 18 United States Code, Sections 2252 and 2252A as defined in Title 18 United States Code, Section 2256 is contained within the Daugherty Devices.

FURTHER AFFIANT SAYETH NAUGHT.

Anthony Wright
Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence on the 2nd day of March, 2020, at Springfield, Illinois.

Tom Schanzle-Haskins
United States Magistrate Judge

ATTACHMENT A

The property to be searched are the following electronic devices:

a. A Black and blue desktop hard drive, Seagate, serial number NA7DWTK4;

b. Cyperton computer tower, serial number GA-789MT-USB3;

c. 1 white USB drive, 2 black USB drives, and 1 blue USB;

d. Compaq computer, serial number CNH4520P00;

e. Gateway 7320 laptop, serial number N3451-710-03782.

The devices are currently located at 900 E. Linton Ave, Springfield, Illinois.

ATTACHMENT B

This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described below.

1. All data files, including but not limited to, graphic representations pertaining to child pornography, that is visual depictions of children under the age of 18 years engaged in sexually explicit conduct.

2. Graphic formats and/or photographs and other visual depictions of such Graphic formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG) containing matter pertaining to child pornography.

3. Electronic mail, chat logs, and electronic messages, offering to transmit through interstate or foreign commerce, including by United States mail or by computer, visual depictions of minors engaged in sexually explicit conduct.

4. Data files pertaining to the use of peer to peer file sharing software.

5. Data files indicating dominion, use and control of the storage device which contains them.

6. Records of communication (as might be found, for example, in digital data files) between individuals concerning the topic of child pornography, the existence of sites on the Internet that contain child pornography or who cater to those with an interest in child pornography, as well as evidence of membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to its members and constituents.

7. Evidence of association, by use, subscription or free membership, with online clubs, groups, services or other Internet sites that provide or otherwise make accessible child pornography.

8. Evidence of any online storage, e-mail or other remote computer storage subscription to include unique software of such subscription, user logs or archived data that show connection to such service, and user login and passwords for such service.

9. Evidence of any use of web cameras, film cameras, digital cameras, mobile cellular and digital phones, mobile computers, software, graphics software, Internet history files, movie files, user created directory and file names, electronic address books, correspondence, communications,

internet and communication setting files, Internet browser bookmark files, configuration files and password files.

10. Items on the phone concerning ownership or use of the phone, such as items indicating the name or identifying information of the person(s) using the phone.

11. Any SIM card located within the phone that aids to identify the cellular telephone number associated with that particular phone and the stored contact information, to include names, nicknames, telephone numbers and e-mail addresses.

COPY

P128

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

FILED

MAR 02 2020

CLERK OF THE COURT
U.S. DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS

for the

Central District of Illinois

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

"Daugherty Devices" further described in Attachment A, currently located at 900 E. Linton Ave, Springfield, IL (FBI)

Case No. 20-MJ- 3023

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):*

See Attachment A.

located in the Central District of Illinois, 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:

Code Section	*Offense Description*
18 U.S.C. § 2252	Possession/Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A	Possession/Receipt/Distribution 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

Anthony Wright, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 03/02/2020

Judge's signature

City and state: Springfield, IL

Tom Schanzle-Haskins, U.S. Magistrate Judge
Printed name and title