UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA v. JARON WOODSLEY	CASE NUMBER: 25 CR 444 ~~UNDER SEAL~~

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 September 20, 2024, at Chicago, in the Northern District of Illinois, Eastern Division, the defendant(s) violated:

Code Section	*Offense Description*
Title 18, United States Code, Sections 2252A(a)(2)(A)	Receipt and distribution of child pornography

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

Meghan Crooks by MV

MEGHAN CROOKS
Special Agent, Federal Bureau of Investigation (FBI)

Pursuant to Fed. R. Crim. P. 4.1, this Complaint is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the Complaint and Affidavit by telephone.

Date: July 31, 2025

Maria Valdez

Judge's signature

City and state: Chicago, Illinois

MARIA VALDEZ, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Meghan Crooks, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed for nine years.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in multiple forms of media, including computer media. I also have participated in the execution of multiple federal search warrants, many of which have involved child exploitation and/or child pornography offenses. I have participated in the execution of multiple federal search warrants.

3. This affidavit is made in support of:

a. a criminal complaint alleging that Jaron Woodsley (WOODSLEY) has violated Title 18, United States Code, Section 2252A(a)(2)(A); and

b. an application for warrants to search the apartment located at [redacted] Oakwood Blvd, [redacted] Chicago, Illinois, described further in Attachment A-1 (the "**Subject Premises**") *and* WOODSLEY's person for evidence, instrumentalities,

fruits, and contraband described further in Attachments B-1 and B-2, concerning possession, receipt, and distribution of child pornography offenses, in violation of Title 18, United States Code, Sections 2252 and 2252A (the "Subject Offenses").

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant and an arrest warrant, I have not included every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence, instrumentalities, fruits, and contraband of violations of Title 18, United States Code, Sections 2252 and 2252A, are located at [redacted] Oakwood Blvd, [redacted] Chicago, Illinois, the **Subject Premises**, and probable cause that WOODSLEY has committed the Subject Offenses.

I. BACKGROUND INFORMATION ON TELEGRAM

5. As described by Telegram on their public-facing website, as well as based on my training and experience, I am aware that Telegram is a mobile and desktop messaging application. It can be used on smartphones, such as Apple iOS and Google Android devices, and on desktop computers by users to send messages and media to each other.

6. To sign up for a Telegram account, a user must provide a phone number. Telegram users can select a username, but they are not required to do so. Usernames are unique, meaning only one Telegram user can have a particular username.

Telegram users can find other users by searching for the username or by using the known phone number of a user. Users can also select a display name, such as a first and last name. Display names are not unique. Telegram offers a variety of communication methods for its users, including one-on-one chats, group chats, channels, and secret chats.

7. The companies that control Telegram are not based in the United States. Until approximately September 2024, Telegram refused to respond to legal process from the United States. Starting in approximately September 2024, Telegram updated its privacy policy and began to respond to law enforcement requests for subscriber information, typically consisting of a user's phone number and the Internet Protocol (IP) address of the user's most recent login. Telegram, however, still does not provide the contents of communications in response to any legal process. This is in part because of the encryption properties of Telegram communications.

8. According to Telegram's privacy policy, encrypted data can only be accessed through the device on which the Telegram application is installed. As of December 9, 2024, the Telegram website states that it has never disclosed user information to governments, making it an ideal platform for individuals engaged in the receipt, and distribution of child pornography.

II. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

9. In summary, and as described more fully below, JARON WOODSLEY, a 27-year-old male who resides at the **Subject Premises**, used the social media application Telegram to communicate online with an individual for the purpose of

distributing and receiving child pornography. Specifically, as outlined below, WOODSLEY used Telegram account "[redacted]" to distribute and receive child pornography.

10. As described more fully below, on or about September 20, 2024, WOODSLEY distributed at least thirteen videos of child sexual abuse material ("CSAM") and received six videos of CSAM from the subject of an FBI investigation who was indicted out of district on [redacted] for multiple counts of child exploitation.

A. Background of Investigation

11. This investigation stems from an FBI investigation in Colorado in [redacted] regarding Subject 1.

12. On [redacted], a federal search warrant was executed at the residence of Subject 1 in Colorado. During the execution of the search warrant, a cell phone belonging to Subject 1 was seized. The cell phone contained several chats with users in the Telegram app, to include a chat with Telegram user [redacted]

13. From approximately September 20, 2024, to September 24, 2024, Subject 1 and [redacted] (later identified as WOODSLEY) direct messaged through Telegram. The following is a summary of the chats and the CSAM sent and received in the chats, as reviewed by the law enforcement

[redacted]: "Got any boys?"
few hbu"
[redacted]: "Same. Wanna trade?"
ends three videos depicting CSAM]
[redacted]: [Sends four videos depicting CSAM]

[redacted]: "Got more?"
eah"
ends two videos of CSAM]
[redacted]: "Fuck"
hey're the hottest"
[redacted]: [Sends eight videos depicting CSAM.]
he eighth video sent by [redacted] was subsequently identified as a CSAM video that captured Subject 1 sexually abusing an approximately 3-year old child who Subject 1 had access to (hereinafter Minor 1).

o fucking way my videos are getting around"
[redacted]: "Huh?"
: "Which is you?"
ast one"
amn wasn't expecting that"
[redacted]: "Thats you and [Minor 1] in the tub? [3
] hot"
Subject 1: "Can't wait to fuck him when I get my own
nth"
[redacted]: "Got more pics of him?"
: "Damn. I wanna watch [devil emoji]"
ends one video of CSAM produced by Subject
inor 1]
[redacted]: "Damn. You're so lucky lol"
How'd you get that video? It's kinda hot
ng around"
[redacted]: "Someone on here sent it to me"
: "I'll definitely be down to join you if
haring haha. Where are you from?"
Subject 1: "I want to share him so bad I'm in Colorado"
nd what was the username"
[redacted]: [redacted]
: "Damn. Illinois here"
: "You ever share face? Maybe we can share
or somewhere else"
Subject 1: "Still a little safe about that but once I
get comfortable yeah"

14. Subject 1 was arrested under the authority of a federal complaint and indicted in the District of Colorado [redacted], for four counts of Production of Child Pornography, one count of Distribution of Child Pornography, and one count of Possession of Child Pornography.

B. The Identification of WOODSLEY Who Resides at the Subject Premises

15. As detailed below, there is probable cause that WOODSLEY is the user of the Telegram account [redacted]

16. According to Telegram return information, Telegram account [redacted] has a user [redacted], username [redacted], and display name [redacted] The phone number associated with the account is (815) XXX-4625, and had a log-in IP of [redacted].[1]

17. According to T-Mobile records, the phone number associated with the [redacted] Telegram account has WOODSLEY listed as the customer with Individual A listed as the subscriber, and both a billing and service address on [redacted] W. Glenlake Avenue, Chicago, Illinois. According to T-Mobile, service was started on or about January 8, 2023, and remained active through at least July 29, 2025. T-Mobile records indicated the IMEI of the phone active on this account on September 20, 2024, was [redacted], and remains the IMEI of the phone active on July 29, 2025.

18. Open sources and public social media indicate that WOODSLEY and Individual A are spouses.

19. According to a database that, in my experience, analyzes numerous records from various data sources, including financial and governmental institutions,

[1] T-Mobile was unable to provide any subscriber information, alternate email addresses or IP address history for [redacted] due to it being an IPV4.

to provide accurate identifying information regarding individuals (the "Records Database"), WOODSLEY and Individual A resided at the Glenlake Avenue address until 2023 or 2024. According to the Records Database, in approximately October or November 2023, WOODSLEY and Individual A purchased a residence at [redacted] Oakwood Blvd, [redacted] Chicago, Illinois, the **Subject Premises**. According to the Cook County Clerk's Office, a publicly registered deed for the **Subject Premises** shows that it was purchased in November 2023 by both WOODSLEY and Individual A.

20. A search of Illinois Secretary of State's records show an active and valid Illinois Driver's License for WOODSLEY issued in July 2024, that lists his birthdate in October 1997, and his address as the **Subject Premises**. A photograph of WOODSLEY's driver's license image is depicted below:

21. According to records maintained by the Department of Homeland Security, WOODSLEY is a citizen of Trinadad and Tobago and is a lawful permanent resident in the United States as of July 2024.

22. Public social media accounts additionally tie WOODSLEY to the [redacted] account:

a. A WhatsApp account linked to phone number (815) XXX-4625 was located. The profile picture for this account depicts a black male facing away from the camera, on a cliff side overlooking a city.

b. Law enforcement located an Instagram account with WOODLSEY's first and last name ("jaronwoodsley") that, based on the information below, appears to be controlled by WOODSLEY. Specifically, the account includes a photo posted on January 1, 2020, that, based on law enforcement comparison, is the same photo as the WhatsApp photo referenced above. The bio on this account is "Trinidad and Tobago" (WOODSLEY's nation of origin) and based on law enforcement's comparison to Illinois driver's license photographs for WOODSLEY and Individual A (who is Caucasian), the Instagram account includes posted photos containing both WOODSLEY and Individual A, as well as individual photos of WOODSLEY. Additionally, the phone number subscribed to the jaronwoodsley Instagram account is (815) XXX-4625, the same number subscribed to the Telegram account [redacted] Further, the birthdate subscribed to the account is October 1997, which is WOODSLEY's birthday listed on his Illinois driver's license.

c. A Snapchat account with username [redacted] was also located. The display name is "[redacted]" alongside a Trinadad and Tobago flag and a United States flag. The publicly-available bitmoji, or personal avatar photograph,

depicts a black male with a goatee, which is similar to the appearance of WOODSLEY.

23. A publicly available search for Telegram account [redacted] showed it remained active online as of July 29, 2025.

24. According to Chicago Public School's website, WOODSLEY is a Chicago Public School teacher at Elementary School A. According to publicly available data, WOODSLEY also is a staff member at the Chicago Youth Symphony Orchestra. Based on my training and experience, both positions put WOODSLEY in a position of trust with children and provide him frequent access to children.

25. On or about July 30, 2025, law enforcement observed WOODSLEY and Individual A exit the **Subject Premises** at approximately 7:45 a.m. They departed the residence in a white Mercedez-Benz SUV, registered to Individual A, who was driving the vehicle. The vehicle drove to the area of [redacted] Michigan Avenue, which is the location of the Chicago Youth Symphony Orchestra, where WOODSLEY departed the vehicle and entered the building.

C. WOODSLEY's Distribution of Child Pornography

26. Based on my review of the initial Telegram chat from Subject 1's cell phone, WOODSLEY used Telegram username [redacted] to distribute and receive child pornography to and from Subject 1 on September 20, 2024.

27. During a preliminary review of the chat, FBI agents observed video files of prepubescent male children that, in my training and experience, constitutes child pornography as defined in Title 18, United States Code, Section 2256(8)(A).

Specifically, FBI agents observed video file, sent from [redacted] to Subject 1 at timestamp 9:37 pm in the chat on September 20, 2024, that is approximately four minutes and twelve seconds in length, and depicts a dark-haired, fully nude, prepubescent-aged male, sitting on what appears to be a bed up against a wall. The prepubescent-aged male initially has his penis manually manipulated by a clothed male appearing to be a pubescent-aged minor sitting next to him and then the pre-pubescent male is depicted masturbating.

28. FBI agents observed a video file sent from [redacted] to Subject 1 at timestamp 9:44 pm in the chat on September 20, 2024, that is approximately six seconds in length, and depicts a dark-haired, clothed, prepubescent male orally penetrated by the penis of an adult or pubescent male that appears to be sitting on a bed, while the older male holds the younger male's head on the penis. This video was followed by [redacted] saying "Sending the rest I have now," and followed by five additional videos appearing to depict child pornography of prepubescent males.

29. FBI agents observed the video file sent from [redacted] to Subject 1 at timestamp 9:45 pm in the chat on September 20, 2024, that is approximately forty-five seconds in length, and depicts a blonde, fully nude, prepubescent male bathing in a bathtub while an adult male masturbates with an exposed penis. As noted in paragraph 13, this is the video that Subject 1 identified as a video that Subject 1 produced that involved Minor 1, a child Subject 1 had access to and exploited.

30. In total, [redacted] sent at least thirteen video files that, in my training and experience, that depict apparent child pornography to Subject 1 on September 20, 2024.

D. WOODSLEY's Possession and Receipt of Child Pornography

31. Based on FBI agents' review of Subject 1's cell phone, FBI agents observed a video file, sent from Subject 1 to [redacted] at timestamp 9:33pm in the chat on September 20, 2024, that is approximately one minute in length, and depicts the genitals of prepubescent-aged male, anally penetrated by an adult penis, while an adult hand manually manipulates the genitals of the prepubescent male. [redacted] responded to this video with four videos of his own and then asked, "Got more?"

32. FBI agents observed a video file, sent from Subject 1 to [redacted] at timestamp 9:39 pm in the chat on September 20, 2024, that is approximately one minute and ten seconds in length, and depicts a dark-haired prepubescent-aged male clothed in a shirt, orally penetrated by an adult penis as the adult lies on what appears to be a bed. [redacted] responded "Fuck" at timestamp 9:43 pm.

33. FBI agents observed a video file, sent from Subject 1 to [redacted] at timestamp 9:48 pm in the chat on September 20, 2024, that is approximately one minute and fifteen seconds in length, and depicts a blonde prepubescent clothed male sitting on a chair at a table, touching a standing adult male's exposed, erect penis, being orally penetrated by it, and having the penis rubbed on the prepubescent male's face. This video was preceded by [redacted] asking "Got more pics of him?" Based

on the investigation to date, this video was produced by Subject 1 and depicts Subject 1 and Minor 1.

34. In total, [redacted] received six video files depicting apparent child pornography from Subject 1 on September 20, 2024.

III. BACKGROUND INFORMATION CONCERNING CHILD PORNOGRAPHY

35. Based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers affect the methods used by people who possess, receive, distribute, and transport child pornography in these ways:

36. Those who create child pornography can produce both still and moving images directly from a common video or digital camera, and other devices that create video and still images, including most cellular telephones. Images from such devices can be transferred to a computer by attaching the device to the computer using a cable, or by uploading images from the device's memory card directly onto the computer or into a storage account accessible from any computer with the capability of accessing the internet (sometimes referred to as a "cloud" account). Once on the computer, images can then be stored, manipulated, transferred, or printed. This includes transfer to some of the same types of devices that are commonly used to create child pornography, such as cellular telephones, as well as other computers. As

a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography.

37. The Internet allows any computer to connect to another computer. Electronic contact can be made to millions of computers around the world. The Internet allows users, while still maintaining anonymity, to locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. They can also distribute and collect child pornography with peer-to-peer ("P2P") file sharing, which uses software to link computers together through the Internet to form a network that allows for the sharing of digital files among users on the network. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet.

38. The computer's capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high

resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise, optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child pornography search warrants often find electronic, optical, and/or electromagnetic storage media containing child pornography in the same location as or near the computer that was used to obtain, access, and/or store child pornography.

39. My training and experience, and the training and experience of other agents whom I have consulted, have shown the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or other images, as well as literature describing sexually explicit activity involving children. Such individuals frequently store their child pornography on multiple electronic, optical, and/or electromagnetic storage media, including not only their computer, but also on external hard drives, CD-ROMs, DVDs, memory sticks, thumb drives, cell phones, and other such media. Many of these individuals also

collect child erotica, which consist of items that may not rise to the level of child pornography but which nonetheless serve a sexual purpose involving children.

b. Individuals who possess, transport, receive, and/or distribute 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. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, Internet Relay Chat, newsgroups, instant messaging, and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute child pornography often collect, read, copy, or maintain names, addresses (including e-mail 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 address books or notebooks, on computer storage devices, or merely on scraps of paper.

d. The majority of individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. These individuals almost always

maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including filing cabinets, safes, or lockboxes. These individuals may also maintain their collections in password-protected or encrypted electronic media. They may keep these passwords, and other information concerning their use of the computer, on handwritten or printed notes that they store in personal areas and around the computer.

e. Possessors, traders and distributors of child pornography sometimes store their illegal images and videos online in remote storage accounts. Therefore, any records, documents, invoices and materials in any format or medium that concern online storage or other remote computer storage could indicate that a person at the **Subject Premises** is storing illegal material in an online storage account.

f. Files, logs, and records relating to P2P files can contain the names of files sent through the P2P service, as well as the date and time the files were transferred. These records could help identify the individual who transferred the child pornography images at the **Subject Premises**. Additionally, these records can provide historical information about the trading of child pornography by individuals at the Subject Premises.

IV. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

40. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) 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. Electronic storage media 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 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.

b. Searching electronic storage media 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 an electronic storage media system is an exacting scientific procedure which is designed

to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media 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.

41. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

42. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251 through 2256, and are subject to seizure as such if they contain contraband or were used to obtain or store images of child pornography.

43. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock electronic devices

subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many 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 and facial 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.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five 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 Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. 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,

Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, 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.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than a certain number of hours have elapsed since the device was last unlocked or (2) when, within a certain number of hours, the device has not been unlocked using a fingerprint and the passcode or password has not been entered. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the

device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the **Subject Premises** and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of WOODSLEY to the fingerprint scanner of the device;[2] and (2) hold the device in front of the face of WOODSLEY for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

V. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

44. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A-1 and on the person described in Attachment A-2 so that they may be reviewed in a

[2] Law enforcement will select the fingers to depress to the fingerprint scanner to avoid compelling the user of the device to disclose information about his or her knowledge of how to access the device.

secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

45. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A-1 and the person described in Attachment A-2 may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachments B-1 and B-2;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachments B-1 and B-2 (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachments B-1 and B-2;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachments B-1 and B-2.

46. The government will return any electronic storage media removed from the premises described in Attachment A-1 or the person described in Attachment A-2 within 60 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

VI. CONCLUSION

47. Based on the above information, I respectfully submit that there is probable cause:

a. that WOODSLEY knowingly received and distributed child pornography in violation of Title 18, United States Code, Section 2252(a)(2)(A); and

b. that possession, receipt, and distribution of child pornography offenses, in violation of Title 18, United States Code, Sections 2252 and 2252A, have been committed, and that evidence, instrumentalities, fruits, and contraband relating to this criminal conduct, as further described in Attachments B-1 and B-2, will be found in the **Subject Premises**, as further described in Attachment A-1, and on the person of JARON WOODSLEY, as further described in Attachment A-2. I therefore respectfully request that this Court issue a search warrant for the **Subject Premises**, more particularly described in Attachment A-1, and the person of JARON

WOODSLEY, more particularly described in Attachment A-2, authorizing the seizure of the items described in Attachments B-1 and B-2, pursuant to the protocol described in the addendum to Attachments B-1 and B-2.

FURTHER AFFIANT SAYETH NOT.

Meghan Crooks by MV

Meghan Crooks
Special Agent
Federal Bureau of Investigation

Sworn to and affirmed by telephone 31st day of July, 2025

Honorable MARIA VALDEZ
United States Magistrate Judge