IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

United States of America v. **Michael Szwarc,** Defendant.	Case No. 3:24-MJ- 117 (MEG) **FILED UNDER SEAL** FEB 8 2024 PM2:03 FILED-USDC-CT-NEW HAVEN February 8, 2024

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND APPLICATIONS UNDER RULE 41 FOR WARRANTS TO SEARCH AND SEIZE

I, Jenny Konecnik, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of:

   a. a criminal complaint and arrest warrant for **MICHAEL SZWARC**, an adult male born in 1988, charging him with violations of 18 U.S.C. § 2252A(a)(2) (receipt of child pornography) and 18 U.S.C. § 2252A(a)(5)(B), (b)(2) (access with intent to view and possession of child pornography) (the **TARGET OFFENSES**); and

   b. applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the person of **SZWARC**, as specifically described in Attachment A-1 of this affidavit, and the locations specifically described in Attachment A-2 of this affidavit, including the entire property located at 74 West 4th Street, Apartment 29B, in Derby, Connecticut (the **SUBJECT PREMISES**) and the content of

electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations or attempted violations of the **TARGET OFFENSES**, which items are more specifically described in Attachment B of this affidavit.[1]

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2019. As such, I am a "Federal Law Enforcement Officer" of the United States. I am currently assigned to the New Haven Division, Violent Crimes Against Children Program and am designated to work a variety of criminal matters, including child sexual exploitation, Internet crimes against children, and human trafficking. As part of my duties, I investigate violations of federal law, including the online exploitation of children, particularly in relation to violations of Title 18, United States Code, Sections 2251, 2252 and 2252A which criminalize, among other things, the production, advertisement, possession, receipt, accessing with intent to view and transportation of child pornography. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

3. The statements contained in this affidavit are based in part on information provided by other members of local, state, and federal law enforcement;

[1] As explained below, on January 3, 2024, the United States Probation and Pretrial Services office seized a laptop computer from **SZWARC**'s residence, which a forensic examination revealed contained child pornography. The forensic examination also showed, as explained below, a history of at least four distinct storage devices connected to the laptop from December 15, 2023, through January 9, 2024. Thus, the warrant being applied for seeks authorization to search for and seize, among other things, other storage devices from **SZWARC**'s person or residence.

my own investigation to include personal observations, documents, and other investigative materials that I have reviewed; and my training and experience as a Special Agent with FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrant.

PROBABLE CAUSE

Background on Michael SZWARC

4. I am investigating **SZWARC** for violations of the **TARGET OFFENSES**. **SZWARC** has two prior convictions for possessing child pornography. I discuss the facts relating to those convictions below.

First Conviction

5. According to court records, in 2012, Connecticut State Police (CSP) became aware that an IP address linked to **SZWARC**'s residence had uploaded child pornography. Investigators conducted a "knock and talk" at **SZWARC**'s residence, but **SZWARC** denied CSP consent to search his devices.[2] CSP obtained a search warrant later that day and seized multiple devices, including laptops, a cell phone, SD cards, and hard drives.

6. About four weeks later, **SZWARC**'s mother contacted police and told them that **SZWARC** had departed the residence and left a note stating that he was

[2] A "knock and talk" is when law enforcement initiates a consensual conversation with an individual in an attempt to obtain information relating to a criminal investigation.

"on the run" due to the execution of the search warrant. His mother also reported finding children's clothing while cleaning **SZWARC**'s room. Law enforcement later located another SD card in **SZWARC**'s bedroom.

7. In total, the investigation revealed that **SZWARC** possessed 1,424 image files and 52 videos files containing child pornography. The images and videos depicted children who appeared to be younger than 16 years of age engaged in sexually explicit activity, including masturbation, oral sex, anal sex, vaginal sex, and/or children either seen naked or partially clothed with their genitalia exposed in a lascivious manner. **SZWARC** pleaded guilty to possession of child pornography in the second degree in violation of Conn. Gen. Stat. § 53a-196e and was sentenced to 10 years' imprisonment, execution suspended after 3 years' imprisonment, and 10 years' probation.

Second Conviction

8. **SZWARC** began his period of probation for the above conviction in November 2015. On September 7, 2018, **SZWARC** reported to his probation officer for a regularly scheduled office visit. During the visit, **SZWARC**'s probation officer asked him if he had been issued a laptop as part of his educational program at Lincoln Tech. **SZWARC** initially claimed that he had refused a computer, but he eventually admitted receiving one, although he claimed to have sold it. When **SZWARC**'s probation officer advised him that he would be searching the shelter where **SZWARC** resided, **SZWARC** admitted possessing two computers in his locker.

9. **SZWARC**'s probation officer then discovered that **SZWARC** possessed an unauthorized cell phone when it beeped in his presence. **SZWARC** admitted owning the phone and assisted his probation officer in locating child pornography on the device. **SZWARC** then admitted using his laptop to download child pornography and transfer it to his smartphone. The probation officer shut down the phone and contacted the Hartford Police Department (HPD). Later, **SZWARC**'s probation officer seized a laptop bag from **SZWARC**'s locker at the shelter he lived at.

10. That same day, **SZWARC** waived his *Miranda* rights and submitted to a voluntary, recorded interview at the HPD. As part of that interview, he provided the following handwritten statement:

> Today I attended a scheduled[sic] appointment with my probation officer [REDACTED], and had my backpack searched by him. I confessed that child pornography is on the phone and that two laptops in my locker at immaculate conception homeless shelter contained child pornography as well. I have provided passwords to the laptops and passwords to the hidden volumes I knew would inevitably be found. My logic was had I not provided the hidden volume information it would only make it more difficult for myself. The collection of photos and videos began about four months ago through Wifi (Public). I had spoofed (changed) my MAC Address to get a free hour of Wifi from XFinity hotspots. This method was used when I lived in Farmington before becoming homeless. Mostly I downloaded from the Tor Network, but some were found: ten to fifteen links from within legal child molesting websites. I had access to the internet mostly at coffee shops and other public locations. These images show underage girls about eight years old or younger in explicit sexual acts or posing nude.

11. I know, on the basis of my training, experience, research, and from consulting with forensic examiners in the FBI's Computer Analysis and Response

Team (CART), that **SZWARC**'s statement makes reference to multiple sophisticated counter-forensic methods used to avoid detection by law enforcement of illegal activities. Because **SZWARC**'s knowledge and use of these methods is relevant to my investigation, I describe them in more detail here.

12. First, **SZWARC**'s reference to "hidden volumes" likely refers to a feature offered by several publicly available encryption software packages to hide data. Encryption is the process of encoding data into an unreadable format to protect it from unauthorized access. Typically, encryption applications take a user-supplied key—often derived from a password—and run the data being encrypted through an algorithm. The output takes the form of encoded and seemingly scrambled data that is intended to be indecipherable. To decrypt the data, the original encryption key must be provided to the decryption software. Encryption can make it difficult, and at times impossible, for law enforcement to recover forensic evidence from a device. Encrypted data may be stored as a volume, i.e., a single area of storage on a filesystem.

13. A hidden volume is, in effect, a second layer of encrypted data hidden within an encrypted volume that is not detectable to individuals who do not know it is there. By structuring the encrypted data in this way, a user can ostensibly decrypt the "visible" volume while leaving the hidden volume encrypted. The intended outcome of this process is leading potential observers into believing that the user has decrypted all volume data when, in reality, only some of that data has been decrypted.

The developer of one popular, publicly available encryption application, VeraCrypt, describes encrypted volumes as follows:

> It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
>
> The principle is that a VeraCrypt volume is created within another VeraCrypt volume (within the free space on the volume). Even when the outer volume is mounted, it should be impossible to prove whether there is a hidden volume within it or not*, because free space on any VeraCrypt volume is always filled with random data when the volume is created** and no part of the (dismounted) hidden volume can be distinguished from random data. Note that VeraCrypt does not modify the file system (information about free space, etc.) within the outer volume in any way.[3]

14. Second, **SZWARC**'s reference to "spoofing" his MAC address refers to a technique used to hide the true identity of a device on a network. A MAC (short for Media Access Control) address is a unique alphanumeric string that is assigned to a device. MAC spoofing is the process of altering or appearing to alter a device's MAC address so that it appears unique or corresponds to a different device. There are a variety of ways that a user can spoof a MAC address.

15. Third and last, **SZWARC** described using the Tor Network to obtain child pornography. I know, on the basis of my training, experience, research, and consultation with members of the FBI's CART, that the Tor Network is a worldwide network of computers configured to mask the source of traffic transmitted over the

[3] VeraCrypt, *Hidden Volume*, https://veracrypt.eu/en/Hidden%20Volume.html (last accessed Feb. 6, 2024).

internet. Tor operates by encrypting and bouncing communications through multiple relay servers—called nodes—run by volunteers all over the globe. This has the effect of anonymizing an individual's internet activity, since the IP address associated with a communication will correspond with the last node relaying the communication, rather than its origin. I further know, from my training and experience, that the Tor Network is frequently used by individuals attempting to obtain and distribute child pornography due to its ability to mask a user's identity.

16. A common method of accessing the Tor Network is with Tor Browser. In addition to all the anonymizing benefits of the Tor Network, Tor Browser is configured to prevent any evidence of a user's web-browsing activities from being saved to the device it runs on. One of the ways it does this is through how it handles browser cookies and cache data.

17. A cookie is a text file created by a web server when the user browses a web page hosted on the server. Typically, cookies contain data about the user's interaction with the web site and are often used to make the site work more efficiently. Cookies exist on the user's device and, from a forensic perspective, often contain valuable information, such as the websites a user has visited.

18. A cache is a storage location for what is usually temporary data. A web browser's cache stores information and resources from web sites that the user has visited. The primary purpose of the browser cache is to permit faster, more efficient web browsing. When a user visits a previously viewed website, the browser compares the online version of the site to the version stored in the cache. If the two are still the

same, the browser loads the web page from the browser cache instead of redownloading it over the Internet. Thus, the browser cache often contains valuable information about a user's web browsing activities, including sites visited and pictures viewed.

19. By default, Tor Browser is configured to wipe all cookies and cache data when the browser is closed, thus destroying any evidence of a user's web browsing activities.

20. However, there is a twofold tradeoff to Tor Browser's anonymizing and privacy features. First, browsing the web using Tor Browser is frequently slow due to the number and distance of the relay nodes that traffic must pass through. Second, the various security features enabled by the browser cause many websites to display improperly or not work at all.

21. On February 5, 2019, a federal grand jury in the District of Connecticut returned an indictment charging **SZWARC** with one count of receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A), (b)(1). **SZWARC** pleaded guilty to that charge on November 21, 2019, and was sentenced on May 31, 2022, to 39 months of imprisonment followed by a term of 42 months of supervised release. *See United States v Szwarc*, Case No. 19-cr-36 (SRU).

22. **SZWARC** commenced federal supervision on May 31, 2022. He has been supervised by a United States Probation Officer with United States Probation and Pretrial Services (USPPS) whose identity is known to me and who shall be referred to throughout this affidavit as Probation Officer-1.

As a result of his convictions, **SZWARC** is a registered sex offender. According to the both the federal and state sex offender databases, **SZWARC** currently resides at the **SUBJECT PREMISES**.

USPPS Conducts a Home Visit to SZWARC's Residence and Seizes Two Unapproved Devices

23. On January 3, 2024, Probation Officer-1 conducted an unannounced home visit to **SZWARC**'s residence at the **SUBJECT PREMISES**. During that visit, Probation Officer-1 observed an unauthorized Hewlett Packard (HP) laptop, serial number 5CD31408H5 (the **HP LAPTOP**), plugged into a television in **SZWARC**'s bedroom. **SZWARC** stated that he purchased the **HP LAPTOP** weeks prior and used it to access the "dark web"[4] for the purpose of purchasing a hallucinogenic drug from South America. Probation Officer-1 also observed an unauthorized Telephone Communication Limited brand smartphone on **SZWARC**'s television stand. Probation Officer-1 seized both devices.

24. In addition to the devices, Probation Officer-1 observed a child-like doll, clad in children's clothing, positioned in a kneeling posture on **SZWARC**'s bed. **SZWARC** admitted that he had engaged in sex acts with the doll the night prior. Probation Officer-1 seized the doll.

[4] As explained below, I know, on the basis of my training and experience, that the "dark web" is a hidden collection of websites that are accessible only through specialized software, such as Tor Browser, which also is described in more detail below.

Probation Officer-1 Examines the HP Laptop and Discovers Child Pornography

25. On January 9, 2024, Probation Officer-1 examined the **HP LAPTOP** and discovered three image files depicting pubescent or prepubescent minor females engaged in sexually explicit conduct. The examination also revealed at least six other images depicting minor females nude or partially nude exposing their genitals.

26. Probation Officer-1's examination of the **HP LAPTOP** further uncovered images of a doll like the one seized from **SZWARC**'s bedroom. Through an open-source search, Probation Officer-1 learned that the doll is sold on the Internet and has three holes of various depths located at the doll's mouth, anus, and vagina. Probation Officer-1 determined that the doll seized from **SZWARC**'s bedroom had similar specifications as the one found during the open-source search.

27. On January 12, 2023, Probation Officer-1 submitted a petition to Senior United States District Judge Stefan R. Underhill seeking a warrant for **SZWARC**'s arrest for violating the conditions of his supervised release. As relevant here, the petition alleged the following: "On January 9, 2024, a scan of the **HP LAPTOP** revealed three images of minor aged females engaged in sexual acts. At least six other images depict minor females that are nude or partially nude, with their genitals exposed."

28. Judge Underhill signed the petition on January 12, 2024, and ordered the issuance of a summons. On or about January 25, 2024, Probation Officer-1

advised the United States Attorney's Office that Judge Underhill had authorized the transfer of the **HP LAPTOP** to federal law enforcement authorities.

29. That same day, on January 25, 2024, SZWARC had his initial appearance on the petition for violating his conditions of supervised release and was released on modified conditions.

The Affiant Meets with Probation Officer-1 and Takes Custody of the HP LAPTOP

30. On January 26, 2024, I met with Probation Officer-1 at the USPP's New Haven office. During the meeting, Probation Officer-1 showed me several of the images of child pornography she discovered while examining the **HP LAPTOP**. According to the results of the examination, each of the files was recovered from the **HP LAPTOP**'s unallocated space. A description of the files is provided below:

a. The first file is a still image depicting a pubescent or prepubescent female child naked and lying across the lap of a clothed adult male, who is sitting on a couch. A black semi-cylindrical object is seen penetrating what appears to be the child's anus.

b. The second file is a still image depicting a pubescent or prepubescent female child positioned in front of what appears to be an adult male. The child's head is positioned at the level of the man's waist, and her mouth is open as he holds his erect penis in front of it. The image cuts off at about the level of the child's neck.

c. The third image depicts a prepubescent female naked and posing with her leg raised to display her vagina. The naked child is the focal point of the image.

31. Probation Officer-1 advised me that her examination also showed that Tor Browser was installed on the **HP LAPTOP**. Probation Officer-1 explained that this was significant because **SZWARC** was interviewed during the investigation that led to his previous federal arrest and conviction for receiving child pornography, and he admitted using the Tor Network to obtain child pornography.

32. Probation Officer-1 stated that although **SZWARC** had told her that he purchased the **HP LAPTOP** in or about November or December, he reported to his mental health treatment provider that he had purchased it earlier, in or about October 2023.

33. Prior to concluding our meeting, Probation Officer-1 turned over custody of the **HP LAPTOP** to me, and I transported it to the FBI's New Haven office.

The Preliminary Examination of the HP LAPTOP

34. On January 29, 2024, the Honorable Robert M. Spector, United States Magistrate Judge, issued a federal search and seizure warrant authorizing law enforcement to search the **HP LAPTOP** for evidence of violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography). *See* Case No. 3:24-MJ-87 (RMS).

35. Following the issuance of the warrant, I conducted a partial review of a digital extraction created from the device. My review was aided by a forensic examiner from the FBI's CART. The following memorializes the results of my partial

review, which at this stage of the investigation is preliminary and does not contain each and every relevant item reviewed by me.

36. As an initial matter, I was advised by the CART forensic examiner that, like **SZWARC**'s previous arrest for possessing child pornography, the **HP LAPTOP** had security and anonymizing software installed. Specifically, the laptop was protected using BitLocker, a whole-disk encryption program capable of encrypting entire hard drives. Disabling BitLocker requires either a user-created password or an automatically generated recovery key. The storage and usage of this key is controlled by the user. In this instance, the CART examiner was able to disable the protection using a password obtained from Probation Officer-1.

37. In addition to the **HP LAPTOP** being protected by BitLocker, the forensic examination also discovered two web browsers installed on the system: Brave, a privacy-focused web browser capable of accessing the Tor Network, and Tor Browser, which **SZWARC** has previously used to obtain child pornography.[5]

38. According to the partial examination, the earliest detectable use of the **HP LAPTOP** was October 16, 2023, when the Windows operating system was installed. There was one identified user account on the system under the username

[5] I have reviewed **SZWARC**'s conditions of supervised release and know that the possession of the unauthorized laptop and use of encryption software and Tor Browser are all violations of the conditions.

"artwo" and the display name "Maggie May." The email address used to create the account is known to me and references a business run by **SZWARC**'s mother.[6]

39. Child pornography was identified in the page file of the **HP LAPTOP**. I know, from my training, experience, research, and consultation with the FBI's CART, that a page file is a hidden system file used by Windows framework operating systems to store data from the computer's random access memory (RAM) when the RAM runs out of storage space. Normally, when an application is opened in Windows, the computer will use RAM to run the application and store data related to it. If, however, no RAM is available at the time the application is opened, the computer will temporarily move data from the RAM to the page file, thus creating more space for the recently opened application. Therefore, the page file contains valuable information at the time a device was seized about applications and data recently stored in RAM but later moved to the page file.

40. The child pornography discovered in the page file consists of 13 images depicting prepubescent minor females engaging in oral or vaginal sex or exposing their vaginas lasciviously. Based on their dimensions and resolution, the files appear to be thumbnails. Six of the images are described below:

[6] According to Probation Officer-1, **SZWARC** had told her that he originally obtained the laptop for his mother but had not yet given it to her.

a. Image 1 has no file name and a corresponding hash value[7] that ends in bc35a82. The image depicts a prepubescent minor female child naked in a bathtub containing water. The minor's legs are spread, and her hands are on the floor of the bathtub. The naked child is the focal point of the image. The walls are blue, and two products are identified on the ledge of the bathtub. An image appearing to be identical was also identified but rotated, with the last seven characters of the hash value being b784a85.

b. Image 2 has no file name and a corresponding hash value that ends in 210d99f. The image depicts a prepubescent minor female child laying on her back, with her legs open. The child's vagina is exposed, and the child is the focal point of the image. The minor is wearing an orange and dark-colored shirt. Beneath her is green bedding.

c. Image 3 has no file name and a corresponding hash value that ends in bd244c3. The image depicts a prepubescent minor female child positioned stomach down on a wood floor. The minor female is wearing only socks from the waist down, and her buttocks and vaginal area are exposed. The child, and specifically her buttocks and vaginal area, are

[7] A hash value functions as a digital fingerprint for computer data. The data is processed through an algorithm that produces an alphanumeric sequence of characters. Even minute changes in the data result in a new hash value being produced.

the focal point of the image. The minor female's face is not visible in the image.

d. Image 4 has no file name or corresponding hash value. The image depicts a prepubescent female child, wearing a light-colored shirt, and an adult female. Both the female child and female adult's mouths are on an erect penis. This engagement of oral sex is the focal point of the image.

e. Image 5 has no file name or corresponding hash value. The image depicts a prepubescent female child, naked from the stomach up. The female child is engaged in oral sex with an adult male, which is the focal point of the image.

f. Image 6 has no file name or corresponding hash value. The image depicts a prepubescent female child, naked from the waist down. The female child is wearing a yellow tank top, pulled up exposing her stomach. The female child is position on her back, with her hands raised above her shoulders. An adult male's penis is penetrating the female child's vagina.

41. Child pornography was also discovered in the Windows thumb cache file, thumbcache.db. I know, on the basis of my training, experience, research, and consultation with the FBI's CART, that the thumb cache contains thumbnail (i.e., miniature) versions of images derived from graphical media files stored in the filesystem. Windows creates this cache so that it can display the stored thumbnails

as icons in Windows File Explorer when a user views a folder containing images or videos.

42. Specifically, I identified a thumbnail corresponding to a file with the filename "00146 (HQ).mp4" and a hash value ending in c5249fb. I know, on the basis of my training and experience, that the file extension "mp4" denotes that a file is an mp4-format video. The thumbnail is a 4 x 4 collage of still images depicting sexual intercourse, including vaginal, oral, and anal intercourse, between a naked adult male and a prepubescent minor female child. The collage contains 16 images displayed in four rows and four columns. The minor female is clothed in only thigh-high socks, described as red and white striped with a blue top around the trim. In at least one of the images from the collage, the minor female has a multicolored top on. A pink couch is visible in the background.

43. The top of the collage image contains a white box containing text that appears to provide details about what appears to be a corresponding video file. For instance, the text references a file titled "00146 (HQ)." In addition to the 4 x 4 collage image, I also located four additional files in the thumbnail cache that appear to be individual images taken from either the collage or the file from which the collage derives.

44. Further review of the extraction located a LNK file corresponding to the file name "00146 (HQ).mp4"—the same file name as identified in the thumb cache just described. LNK files are files created by the operating system automatically whenever a user accesses a file. They contain metadata about a file, including the

file's location in the filesystem. The local file path identified in the LNK file shows that the file was accessed through the user's video folder, located at "C:\Users\artwo\Videos\00146 (HQ)\00146 (HQ).mp4." I know, on the basis of my training and experience, that the text "(HQ")" in a filename normally indicates that the vIdeo file is being advertised as "high quality." The LNK file indicates that the video was created and accessed on December 15, 2023.

45. Moreover, I know, on the basis of my training and experience, that the \Videos folder in the \Users path is one of several default folders created by Windows for a specific purpose—in this case, storing video files. By default, this folder contains no videos, let alone videos containing child pornography. Therefore, files are not typically located in the \Videos folder unless stored there through some user-executed process, such as downloading, extracting, and/or saving the files there.

46. In addition to the LNK file described above, evidence located within the extraction showed that the file "00146 (HQ).mp4" was viewed using the VLC Media Player application (VLC), which is an application used to play video files. Specifically, I know that VLC maintains a history of videos watched by the user along with the file paths of the files played. In this instance, the string "00146" was identified in the VLC history. According to data recovered during the examination, the VLC program was first interacted with by the user on December 15, 2023.

47. The forensic examination also uncovered information that a 7-zip archive had been accessed on the same date that the "00146 (HQ).mp4" video file appeared and was viewed in VLC. 7-zip is a file archiver and compression application

that can compress multiple files into a single file, which can then be decompressed back to the original files. The 7zip archive contained five files: a video file, "00146 (HQ).mp4," (the same file identified in the LNK file), and four image files, "00146 (HQ)_PREVIEW.JPG," "PREVIEW 01.JPG," "PREVIEW 02.JPG," and "PREVIEW 03.JPG." I know, on the basis of my training and experience, that the file extension "jpg" denotes an image file.

48. According to data obtained during the forensic examination, an executable file used to install VLC was downloaded on December 15, 2023, at 10:04:36 p.m. Less than a minute later, at 10:05:19 p.m., the VLC application was opened. About eight seconds after that, at 10:05:27, the file "00146 (HQ).mp4" was accessed and then opened in VLC. Fifteen minutes later, at 10:32:50 p.m., VLC was uninstalled.

49. Thus, on the basis of my preliminary review and the data uncovered, I believe that **SZWARC** received the 7zip archive and extracted the file "00146 (HQ).mp4" to the default Videos directory. **SZWARC** then installed the VLC media player, which he used to view the video. Immediately after viewing the video, **SZWARC** uninstalled the VLC media player.

50. I further believe that the image files of child pornography recovered from the thumbnail cache are the four image files contained within the 7-zip archive, along with the video file. I base this conclusion on two facts. First, the number of thumbnail images recovered (four) corresponds exactly with the number of image files in the 7-zip archive. Second, the file names of three of the images contain the word

"preview," and the images do, in fact, appear to "preview" the contents of what is in the video based on the images in the 4 x 4 collage file. I believe the final image file, "00149 (HQ)_PREVIEW.jpg," is the collage file since the 4 x 4 collage image contains descriptive text referencing the video's filename. Although the "00146 (HQ).mp4" video was not recovered during the forensic examination, I believe the video depicts child pornography because the "preview" images packaged with it in the archive depict sexually explicit conduct involving a minor.

51. Lastly, data from the extraction showed a history of at least four distinct external storage devices connecting to the laptop from December 15, 2023, through January 9, 2024.[8] I know from my discussions with Probation Officer-1 that these devices were never identified or seized by USPPS.

Dark Web Postings

52. In connection with this investigation, law enforcement identified several posts attributed to **SZWARC** on a "dark web" forum. I know, on the basis of my training and experience, that the "dark web" is a hidden collection of websites that are accessible only through specialized software, such as Tor Browser. The posts begin in September 2022, about three months after **SZWARC**'s incarceration ended, and end on September 29, 2022. The name of the dark web forum, as well as a "registration agreement" hosted on it, describe it as a support community for pedophiles. Specifically, the agreement states that the forum exists, in part, to be a

[8] It is possible one of these devices is forensic examination hardware used by Probation Officer-1, since the forensic examination shows that a storage device was attached after the **HP LAPTOP** was seized.

"a warm and friendly environment, to share our journeys together, as we do the best we can, to deal with being loving and caring paedophiles, in a world that does not understand who we really are." The agreement further states: "[W]e are a community geared toward loving, caring, consensual relationships with the ones that we love, rather than just the sexual aspect of our attractions." The agreement further claims that the posting of child pornography is not permitted.

53. Because the forum is a potential investigative target for law enforcement, I refer to in this affidavit only by the name "Forum A." As described below, several of **SZWARC**'s posts on Forum A discuss child pornography, the sexual abuse of children, and child sex dolls.

Identification of SZWARC as the Likely Author of Posts on Forum A

54. Investigators identified several posts on Forum A under the screen name "FlutterDashie88x." I believe that "FlutterDashie88x" is **SZWARC** for the following reasons.

55. First, an HPD police report dated September 7, 2018, states that **SZWARC** provided the phrase "FlutterDash" in connection with his online activity. Additionally, **SZWARC**'s year of birth is 1988, which corresponds with the "88" in the pseudonym.

56. Second, an open-source search for "FlutterDashie88" was conducted and located an account on the social media discussion platform Reddit. According to a review of the "FlutterDashie88" user's posts, the user identifies as a pedophile, was incarcerated, is serving 3.5 years of "probation" (the exact period of supervised release

imposed for **SZWARC**'s most recent conviction), and discusses child sex dolls. Additionally, records provided by Reddit in response to an administrative subpoena stated that the "FlutterDashie88" Reddit account was registered using the email address "michaelszwarc12@gmail.com." This address was discovered on the **HP LAPTOP** as an auto-fill value (i.e., an address the computer saved so that it could be automatically supplied when an email address is requested).

57. Third, as discussed below, the posts by "FlutterDashie88x" reference specific personal details about **SZWARC**'s criminal history, including the number of convictions and the precise sentences he received.

Posts Discovered on Forum A

58. According to timestamps on Forum A, "FlutterDashie88x" made a series of introductory posts on September 25, 2022, starting at 9:46 p.m., in a post entitled, "Two time convicted CP dumbass." The posts begin with the following:

> Hello everyone. So I discovered this community and I'm very greatfull. I intend to be a full member and productive on a daily basis. Anyway, as the subject suggests, I've been convicted of possession of CP twice. Very shameful and it's made my life a living hell. However, this isn't the end of the world.I just have to power through. But, the good news is, I've found a path to own a child like sex doll and use this in therapy. It's been a tough sell, but I've been able to find a path. Matter of fact, I've already posted here about this matter, and waiting for moderators to approve the post. Anyway, I hope this community is a good fit for me, and and I'm a good fit for the community. Thank you all for being here and keeping this site up and running

59. I know, on the basis of my training and experience, that "CP" is shorthand for "child pornography."

60. "FlutterDashie88x" continues at 10:01 p.m.:

> So this is an addendum, to comply with the community welcome standards. Let me continue my into by adding why I feel PSC would be a good fit for me. First, I like the fact that PSC is not a sharing community for CP. That part of my life is behind me, but my interests in children will never go away. I feel that PSC and it's guidelines are aligned with my values.
>
> I did read the welcome packet, and how to structure my first post, but I feel I'm still missing something. In any event I will be very bummed if I get the boot because I missed some money detail. In any event, I'm hoping to stay here for the indefinite future.
>
> Love ya guys, stay safe.

61. At 10:43 p.m., "FlutterDashie88x" continues in the same thread by describing his sexual abuse of a seven-year-old child beginning when he was 20 years old up and continuing until she turned 12 years old, and he ceased being physically attracted to her:

> Damn. I wrote a part 3 for this and got logged out. Anyway, I wanted to add a bit more about myself. When I was ten years old, I had a little girlfriend who I had frequent sex with, who was eight at the time. This relationship lasted for two years. I had an absentee mother, so I stayed with my girlfriend for days at a time. We slept together in her bed, kissing, and petting. We watched porn on TV \(VHS\) and did as they did I ended up moving out of state. We found each other years later. Still on good terms, and she understands my attraction to minors. At twenty, I had another LGF that was seven years old. I was able to form a sexual relationship with her within 6 months for the next seven years, and posted on good terms. She was my across the hall neighbor, and pretty much lived with me. I bought her clothes to wear, especially socks, which was my favorite. She was my little dolly to dress as I pleased. We went out on dates, dinners, water parks and such. Her mom was a drug addict, and I fed her habit to keep her quiet. Even though by the time she was 12 she out paced my physical attraction, I still loved her for her. After that, I went to

> jail for possession of CP. We keep regular contact to today. Anyway. That's my life story... Thanks

62. At 11:17 p.m., "FlutterDashie88x" replies in a thread created by a user who posts about struggling with sexual attraction to his infant daughter. In his reply, "FlutterDashie88x" coaches the user on how to initiate a sexual relationship with the child:

> Well, there's always a safe way if going about things. I have no daughter but I would be great full for a little girl who enjoys the finer things in life. But it's true, it's about her education, and not about your gratification. Certainly you can satisfy yourself but do it safely. Make it fun for her. It's all a game. Of course, little girls do have the sensation of pleasure downstairs, but it has to have a pleasurable association. Never forced. Exposure over time. Get her more comfortable out of her clothes than not. Love guides for maps are out there too. Just find it, and read it in ints entiy. Top to bottom. No skipping. Read up on child psychology too. That helps a boatload. Stay safe my friend.

63. I know, on the basis of my training, experience, and research, that the term "maps" is shorthand for "minor-attracted person," a phrase promoted within the pedophile community to replace the term "pedophile."

64. At 11:25 p.m., "FlutterDashie88x" replies to user in a separate thread with the following:

> Hey friend. I understand your problems. Really really do. However, I've had a little girl friend for years, and I miss her so much. Better to love list than never love at all... Sorry. But, one solution I really hope you look into, is a child like sex doll. I've had one before, and look forward to getting another soon once my situation changes. My doll was a very strong emotional support in time if dire need. We cuddled, and slept together every night. She want a real little girl, but she saved my life, no exaggeration. Hope this helps you.

65. At 11:46 p.m., "FlutterDashie88x" replies to a user in a separate thread with the following:

> I'm so glad you applied here. I'm yet to be a member, approved, but I strongly feel that you would make another great member here as well. You seem to have a solid head on your shoulders, and are asking all the right questions. You also strike me as a cautious and conservative person with what desions you make with your child attraction. I have no doubt your staying safe, but as for me, a person with two prior CP arrests, I've learned the hard way to stay safe.

66. On the following day, September 26, 2022, at 9:55 p.m., "FlutterDashie88x" replies to a thread entitled, "What have you always wanted to see in CP…" and appears to state that he is "having difficulty" finding "high quality" child pornography:

> Oh I love socks. Two girls, three or four, wearing socks. See, I love Ls Magazine, because it's such high quality but there's no HC about it. I'm finding difficulty finding high quality vids. Heck, I know damn well I could make vids and pics better than anything I've seen so far. Girl on girl is great but they often don't have the enthusiasm I need. Plus, rarely do they wear socks...

67. I know, based on reports from other FBI investigations, that "Ls" refers to a series of publications originating in Russia or Ukraine that are known by law enforcement to contain child pornography. I further know, on the basis of my training, experience, and research, that "HC" is often shorthand for "hardcore," which refers to explicit sexual activity usually involving oral, vagina, or anal intercourse.

68. At 10:19 p.m., "FlutterDashie88x" replies to a thread entitled, "Pedos in Prison - Your Jail / Prison Experiences," stating, in part, the following:

> I was cought with CP twice. What a dumb ass, right? Well, the second time I was already on probation... Yeah. I had my laptop open in the back room that I forgot about and the desktop image of some lsm girls kissing each other buck ass naked on a bed. Yep. Do not pass go, do not collect $200. That one was a federal charge too.
>
> My first time I got an okay deal. 3 years jail, ten probation. This next time I was given time served at two years, and give years probation. I'll be getting off probation a month earlier than I would've had I not been arrested the second time\!
>
> I know that I've got gold. Not many people do, and I have a silent prayer every morning I wake up for those who got the book thrown at them. Every night, I remember the great I had while still in jail not knowing how long I'll be sentenced to. I'm very lucky.
>
> In the feds, I was in PC, protective custody, and I got to know many people who was active with children and are looking at 30 years minimum. One guy ducked his little girl with his wife. His little girl took the stand and denied everything. His wife was witness and she was given immunity. Two tiered justice system. Never the less, his daughter still writes him pretending to be an old friend. I read the letters. Sweet girl.
>
> Granted, I never went to a sentenced facility, thankfully, but my time wasn't as bad as it could have been. I played lots of dungeons and dragons every day with other pedos, and we mostly talked in secret about our fantasies.

69. Significantly, in the above post, "FlutterDashie88x" reports receiving the exact same sentences **SZWARC** received for his convictions.

DEFINITIONS

70. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. "Chat," refers to the process of communicating, interacting and/or exchanging messages over the Internet. It involves two or more individuals that communicate through a chat-enabled service or software. Chat is also known as chatting, online chat or Internet chat.

b. "Child erotica," means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

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

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

e. "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 charactersf) 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.

f. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

g. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

h. "Internet Service Providers" ("ISPs"), are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

j. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

k. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

l. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

m. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or

masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

n. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

o. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

71. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic

communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types—to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer—can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can

set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to

electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN OR WHO RECEIVE, AND/OR POSSESS CHILD PORNOGRAPHY

72. Based on my previous investigative experience related to child-exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

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

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the

inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still

discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals 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.

h. Even if the individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in the individual's home, the **SUBJECT PREMISES**, or on the individual's person, as set forth in Attachment A-1 and Attachment A-2, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

73. Based on all of the information contained herein, I believe that **SZWARC** likely displays characteristics common to individuals who have a sexual

interest in children and/or receive or possess images of child pornography. In particular, despite two prior arrests, convictions, and sentences of imprisonment, **SZWARC** was detected by his probation officer possessing child pornography a third time. Additionally, **SZWARC** has employed a number of uncommon countermeasures to avoid detection and hide his Internet and computer activities, including whole disk encryption and using TOR-based web browsers. Lastly, **SZWARC**'s browsing history and possession of a child sex doll indicates that he continues to have a sexual interest in children.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

74. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

75. I submit that if a computer or storage medium is found on the **SUBJECT PREMISES**, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. 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.

b. 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.

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."

76. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** 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, email 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, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected

with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the

computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer 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 computer 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. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

77. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search website all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

78. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be

secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

79. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

80. This warrant permits law enforcement to compel **SZWARC** to unlock any electronic devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

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, 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.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through their 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 their 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 their 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 have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with their irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers their irises by holding the device in front of their face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. 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.

f. As discussed in this affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. 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, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours

has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. 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.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of **SZWARC** to the fingerprint scanner of the devices found at the **SUBJECT PREMISES** or on his person; (2) hold the devices found at the **SUBJECT PREMISES** or on his person in front of the face of **SZWARC** and activate the facial recognition feature; and/or (3) hold the devices found at the **SUBJECT PREMISES** or on his person in front of the face of **SZWARC** and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to

compel that **SZWARC** state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel **SZWARC** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

81. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated by **SZWARC**, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A-1 and Attachment A-2. I respectfully request that this Court issue:

a. an arrest warrant for **SZWARC** charging him with the offenses identified in the criminal complaint; and

b. search warrants for the locations described in Attachment A-1 and Attachment A-2, authorizing the seizure and search of the items described in Attachment B.

82. I am aware that the recovery of data by a computer forensic analyst takes significant time, much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered

from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,

JENNY KONECNIK
Special Agent
Federal Bureau of Investigation

The truth of the foregoing affidavit has been attested to me by FBI Special Agent Jenny Konecnik over the telephone on February 8, 2024.

HONORABLE MARIA E. GARCIA
United States Magistrate Judge

ATTACHMENT A-1

Property to be Searched

The property to be searched is the person of **MICHAEL SZWARC**, an adult male born in 1988, provided he is located in the District of Connecticut at the time of the search.

ATTACHMENT A-2

Property to be Searched

The property to be searched is 74 West 4th Street, Apartment 29B, in Derby, Connecticut (the **SUBJECT PREMISES**), further described as a two-story brick apartment complex containing multiple units. The subject of the search is Apartment 29B.

ATTACHMENT B

Items to be Seized

All property, records, and information, in any format, that constitute fruits, evidence, and instrumentalities of violations of 18 U.S.C. 2252A(a)(2) (receiving child pornography) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession and access with intent to view child pornography) (the **TARGET OFFENSES**) and involve **MICHAEL SZWARC** since September 1, 2022, including:

1. Child pornography, as defined in 18 U.S.C. § 2256(8);
2. Child erotica;
3. Computers or storage media capable of being used as a means to commit the violations described above;
4. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including storage, and chat applications;
5. In any format or media, all originals, copies and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
6. Any and all notes, documents, records, correspondence, and materials, in any format and media (including, but not limited to, letters, e-mail, chat logs and electronic messages), pertaining to the possession or, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions

of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

7. Any and all names, addresses, contact information or lists of names, addresses or contact information, in any format and medium, of those who may have been contacted by computer or other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
8. Any and all notes, documents, records, or correspondence, in any format or medium, concerning communications about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography;
9. Any and all notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make child pornography accessible to members;
10. Any and all records, documents, invoices and materials, in any format or medium that concern any accounts with an Internet Service Provider;
11. Any and all records, documents, invoices and materials, in any format or medium that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user

logins and passwords for such online storage or remote computer storage;

12. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

13. Routers, modems, and network equipment used to connect computers to

the Internet.

14. Records, information, and items relating to violations of the statutes described above including:

    a. Records, information, and items relating to the occupancy or ownership of the 74 West 4th Street, Apartment 29B, in Derby, Connecticut, including utility and telephone bills, mail envelopes, or addressed correspondence;

    b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

    c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

    d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the locations described in Attachment A-1 and Attachment A-2, law enforcement personnel are also specifically authorized to compel **MICHAEL SZWARC** to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- any of the devices found upon the person of **MICHAEL SZWARC** or at the **SUBJECT PREMISES**, and
- where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the **SUBJECT PREMISES** to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device. Further, this warrant does not authorize law enforcement personnel to request that **SZWARC** state or otherwise provide the password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.