AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

UNITED STATES OF AMERICA

v.

MATTHEW EDWARD PYSHER,
aka "Piano.Man",

Defendant

Case No. 2:26-mj-00971-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of February 20, 2026 in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 2423(b)	Travel with Intent to Engage in Illicit Sexual Conduct

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Hailey Kryszewski, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: February 22, 2026

Judge's signature

City and state: Los Angeles, California

Hon. Pedro V. Castillo, U.S. Magistrate Judge
Printed name and title

AUSA: Colin S. Scott (x3159)

AFFIDAVIT

I, Hailey Kryszewski, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed as such since October 2023. I am currently assigned to a Domestic Terrorism and Weapons of Mass Destruction Squad of the Los Angeles Field Office, where I primarily investigate people who commit violent criminal acts in furtherance of their political or social ideology. During my career, I have led and participated in numerous criminal and national security investigations, including those involving the use of digital devices and online accounts to facilitate violations of federal law. Through the course of my training and employment with the FBI, I have used a variety of investigative techniques and resources, including the execution of search warrants and review of both physical and digital evidence collected from search warrant returns. I am familiar with the strategy, tactics, methods, tradecraft, and techniques of criminals, terrorists, and their agents. During my employment with the FBI, I attended 21 weeks of New Agent Training at the FBI Academy in Quantico, Virginia. I have received additional formal and informal training from the FBI regarding criminal and counterterrorism investigations, including training concerning the use of electronic communications, digital devices in furtherance of a crime, and violent crimes against children. As a federal agent, I am

authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

II. PURPOSE OF AFFIDAVIT

2. This affidavit is made in support of a criminal complaint against and arrest warrant for Matthew Edward PYSHER ("**PYSHER**"), for a violation of Title 18, United States Code, Section 2423(b) (Travel with Intent to Engage in Illicit Sexual Conduct).

3. This affidavit is also made in support of an application for warrants to search the following digital devices (the "SUBJECT DEVICES"), as further described in Attachment A:

a. one black Samsung phone with IMEI 351219580989581, seized from PYSHER's hotel room on February 20, 2026 ("SUBJECT DEVICE 1"); and

b. one Valve Steamdeck with serial code FYZZ3510BD91, seized from PYSHER's hotel room on February 20, 2026("SUBJECT DEVICE 2").

4. The requested search warrant seeks authorization to seize evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 2251(a), (e) (Sexual Exploitation of Children and Attempted Sexual Exploitation of Children); 18 U.S.C. § 2422(b) (Enticement of a Minor and Attempted Enticement of a Minor); 18 U.S.C. § 2252A(a)(2) (Distribution and Receipt of Child Pornography); 18 U.S.C. § 2252A(a)(5)(B) (Access with Intent to View and Possession of

Child Pornography); and 18 U.S.C. § 2423(b) (Travel with Intent to Engage in Illicit Sexual Conduct) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based on my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, and all dates and times are on or about those indicated.

III. BACKGROUND ON NIHILISTIC VIOLENT EXTREMISM ("NVE") AND THE "764" NETWORK'S FOCUS ON TARGETING CHILDREN FOR VIOLENT CRIME

6. Based on my training and experience and discussions with other FBI special agents, I understand the following about NVE and 764:

a. NVEs are individuals who engage in criminal conduct within the United States and abroad, in furtherance of political, social, or religious goals that derive primarily from a hatred of society at large and a desire to bring about its collapse by sowing indiscriminate chaos, destruction, and social instability. NVEs work individually or as part of a network with these goals of destroying civilized society through the

corruption and exploitation of vulnerable populations, which often include minors.

b. NVEs, both individually and as a network, systematically and methodically target vulnerable populations across the United States and the globe. NVEs frequently use social media communication platforms to connect with individuals and desensitize them to violence by, among other things, breaking down societal norms regarding engaging in violence, normalizing the possession, production, and sharing of Child Sexual Abuse Material ("CSAM") and gore material, and otherwise corrupting and grooming those individuals towards committing future acts of violence.

c. Those individuals are targeted online, often through synchronized group chats. NVEs frequently conduct coordinated extortions of individuals by blackmailing them so they comply with the demands of the network. These demands vary and include, but are not limited to, self-mutilation, online and in-person sexual acts, harm to animals, sexual exploitation of siblings and others, acts of violence, threats of violence, suicide, and murder.

d. Historically, NVEs systematically targeted vulnerable individuals by grooming, extorting, coercing, and otherwise compelling through force, or the threat of force, the victims to mutilate themselves or do violence, or threaten violence, to others, and either film or photograph such activity. The members of the network have edited compilation photographs or videos of targeted individuals and shared the

photographs and videos on social media platforms for several reasons, including to gain notoriety amongst members of the network, and spread fear among those targeted individuals for the purpose of accelerating the downfall of society and otherwise achieving the goals of the NVEs.

e. NVEs have adopted various monikers to identify themselves. The networks have changed names over time, which has led to the creation of related networks. Although the networks change names and use a variety of different social media platforms, the core members and goals remain consistent and align with the overarching threat of NVE.

f. 764 and related groups are NVEs who engage in criminal conduct within the United States and engage with other extremists abroad. The 764 network's accelerationist goals include social unrest and the downfall of the current world order, including the United States Government. Members of 764 work in concert with one another towards a common purpose of destroying civilized society through the corruption and exploitation of vulnerable populations, including minors.

IV. SUMMARY OF PROBABLE CAUSE

7. From at least in or around December 2025 until February 20, 2026, **PYSHER** groomed and encouraged Minor Victim One to send him sexually explicit material and images of self-harm over the internet. Among other things, **PYSHER** specifically encouraged Minor Victim One, via chat messages, to engage in acts of self-harm including by establishing a Discord server

where Minor Victim One could be filmed using blades to cut herself. Minor Victim One recently turned 13 years old.

8. This pattern of abuse culminated in **PYSHER's** travel to Los Angeles, California from Bangor, Pennsylvania on February 20, 2026, in order for **PYSHER** to engage in sexual activity with Minor Victim One. On February 20, 2026, **PYSHER**, along with a co-conspirator, picked Minor Victim One up from a location near her home and transported her to the Rodeway Inn Motel in Castaic, California.

9. After obtaining emergency disclosures and locating **PYSHER** at the Rodeway Inn Motel, law enforcement entered **PYSHER's** hotel room where they found Minor Victim One and **PYSHER**. Also, inside the room, law enforcement found condoms, a knife, lubricant, razor blades, bloody tissues, an American Airlines boarding pass for Flight Number AA827 from Philadelphia to Los Angeles in **PYSHER**'s name.

10. Minor Victim One spoke with law enforcement and told them that **PYSHER** came to California to see her and that they had planned on committing suicide together but were unable to do so before being found by law enforcement. Minor Victim One also told law enforcement that she and **PYSHER** had engaged in sexual conduct and that **PYSHER** had used a knife to repeatedly cut Minor Victim One.

11. Based on **PYSHER's** online activities, his coercion and enticement of minors to create self-harm videos, and my training and experience, I believe **PYSHER** is associated with the nihilistic violent extremist ideology. Additionally, for the

reasons discussed in this affidavit, I believe that **PYSHER's** digital devices (i.e., the SUBJECT DEVICES) likely contain evidence related to the Subject Offenses, including information about additional minor victims.

V. STATEMENT OF PROBABLE CAUSE

12. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Minor Victim One's Mother Contacts The FBI About Online Abuse Of Her Minor Daughter

13. On February 10, 2026, Minor Victim One's Mother contacted the FBI because she was concerned that Minor Victim One was being encouraged to harm herself by an individual named "Matthew".[1] According to Minor Victim One's Mother, Minor Victim One met Matthew via an online platform called Discord.[2] Minor Victim One encountered Matthew on a Discord server related to individuals who were suffering from a mental illness.

14. Minor Victim One's Mother told law enforcement that she had reviewed communications on Minor Victim One's digital devices in which Matthew had encouraged Minor Victim One to cut herself and engage in other acts of self-harm. Furthermore, Minor Victim One's Mother, had reviewed communications between Minor Victim One and Matthew, who also used the username

---

[1] As discussed below, Minor Victim One later identified PYSHER as "Matthew".

[2] Discord is an online communications platform where individuals can meet together to discuss topics of common interest. As relevant to this investigation, Discord is also a common gathering place for NVEs to target and recruit minors to engage in acts of self-harm.

"Piano.Man," in which Minor Victim One told Matthew that she was 14 years old.

15. On February 20, 2026, at approximately 11:30 a.m., I arrived at Minor Victim One's Mother home to pick up Minor Victim One's digital devices. Shortly after leaving the home, I received a call from Minor Victim One's Mother who said that Minor Victim One's grandfather had found a suicide note from Minor Victim One and that she had run away from the home.

B. Law Enforcement Identifies PYSHER as the Abuser

16. Based on conversations with other law enforcement officers, I know that shortly after receiving the phone call from Minor Victim One's Mother, law enforcement returned to Minor Victim One's home. Upon arriving at the home, FBI Special Agent Ryan Scheeler was handed a slip of paper by state authorities with a phone number ending in -1519 (the "1519 Number"). Local law enforcement then told Special Agent Scheeler that Minor Victim One's Mother had found the slip of paper with the 1519 Number in Minor Victim One's room. According to Minor Victim One's Mother, when she asked her daughter about the number, Minor Victim One became defensive and refused to answer any questions. Based on this exchange, law enforcement began to investigate the user of the 1519 Number and whether they might be connected to Minor Victim One's disappearance.

17. After receiving the 1519 Number, law enforcement submitted an Emergency Disclosure Request ("EDR") to Google. I reviewed the results of that EDR which showed that 1519 Number

was linked to two Gmail accounts: pianoman0269@gmail.com[3] and mr.mlg2733@gmail.com. The EDR also showed that both email addresses were linked to Matthew **PYSHER** with addresses located in Bangor, Pennsylvania. I also reviewed IP records for both Gmail accounts which showed logins for both accounts at IP addresses that resolved to eastern Pennsylvania.

18. Furthermore, I submitted an EDR to T-Mobile which showed that the subscriber for the 1519 Number was a Meghan Pysher with a billing address in Quakertown, Pennsylvania.[4] I reviewed location data disclosed pursuant to the EDR which showed that the 1519 Number had been in eastern Pennsylvania on February 19, 2026, but as of February 20, 2026, the user of the telephone (i.e., **PYSHER**) was located in Los Angeles, California.

19. Lastly, I cross-referenced the details of the 1519 Number and Matthew **PYSHER's** name against data provided by American Airlines and determined that a Matthew **PYSHER** had traveled from Philadelphia, Pennsylvania on flight number AA827 to Los Angeles, California on February 20, 2026.

20. Based on these facts, I came to the conclusion that the individual referred to as "Matthew" by Minor Victim One's Mother, who had been encouraging Minor Victim One to cut

[3] As discussed in further detail below, during her interview with law enforcement Minor Victim One stated she messaged with a Discord user by the name of Piano.Man.

[4] I reviewed postal records which indicate that in 2024 a mail address forwarding request was submitted for Meghan Pysher to forward mail from the Quakertown address to an address in Bangor, Pennsylvania.

herself, had likely traveled from Pennsylvania to California in order to see Minor Victim One

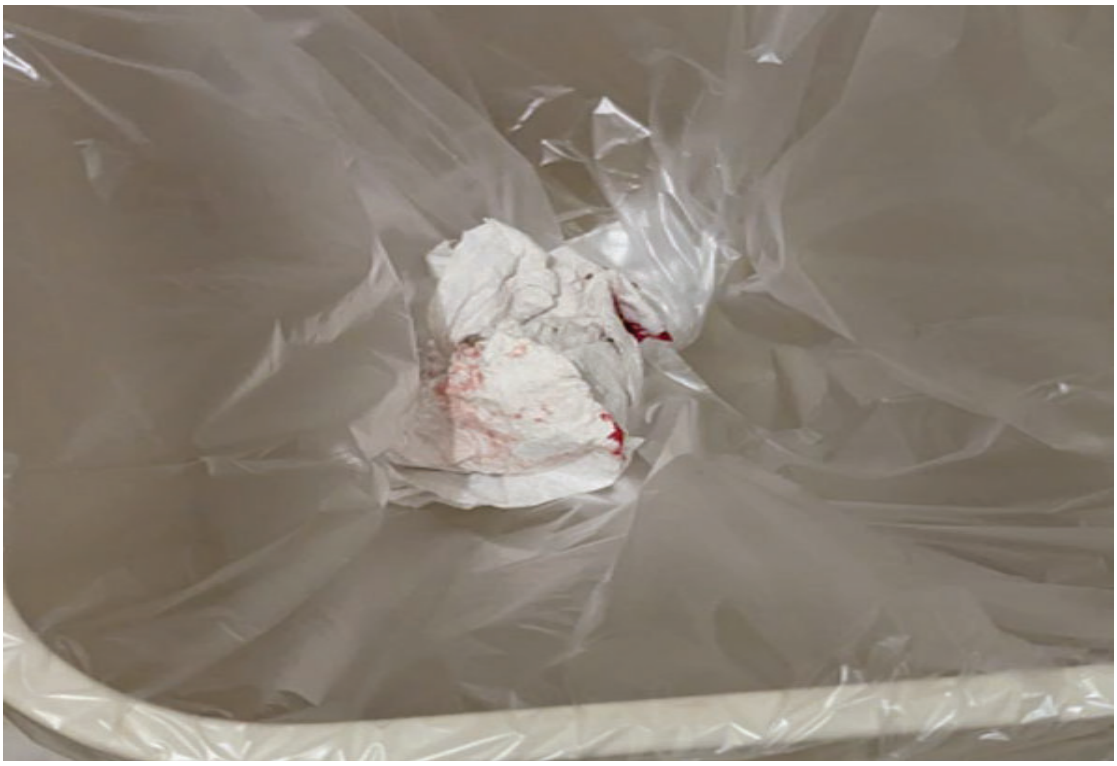
C. Law Enforcement Rescues Minor Victim One at a Motel in Castaic, California After She is Sexually Assaulted

21. Based upon location data from the 1519 Number, I determined that the user of the 1519 Number was in Castaic, California during the afternoon of February 20, 2026.

22. Based on my knowledge of the investigation, I know that law enforcement canvassed hotels in the Castaic area and were able to determine through video surveillance footage that **PYSHER** had checked in to the Rodeway Inn Motel and that Minor Victim One was with **PYSHER** at the time. At that point, management for the Rodeway Inn Motel, gave law enforcement **PYSHER's** room number.

23. Based on conversations with other law enforcement officials, I know that law enforcement subsequently entered **PYSHER's** hotel room based on the danger to Minor Victim One.[5] Inside the room, law enforcement found Minor Victim One hiding in the bathroom as well as a bottle of lubricant on the nightstand, a knife, several razor blades, and bloody tissues as depicted on the following page.

[5] Law enforcement entered the room without a warrant due to the threat to Minor Victim One's life. After entering the hotel room, law enforcement obtained a warrant from the Honorable Daviann Mitchell, Magistrate Judge, Superior Court of Los Angeles, in case number 026-02304-0675-122, which authorized law enforcement to search the hotel room and seize any digital device found within it.



24. Among **PYSHER's** personal items, law enforcement also found multiple condoms inside of a backpack. At that time law enforcement also seized **SUBJECT DEVICES 1** and **2**. Law enforcement found **SUBJECT DEVICE 1** on a chair near the bed next to a faraday bag. Based on my training and experience, I know faraday bags are used to block electronic signals from phones. **SUBJECT DEVICE 2** was found on a desk inside the hotel room.

25. Following her rescue, Minor Victim One spoke with medical and law enforcement professionals. I have reviewed a video recording of one of those conversations and report of the other and learned the following facts:

a. Minor Victim One told law enforcement that she had first started talking with **PYSHER** approximately three months ago via the social media platform Discord. On Discord, **PYSHER**

used the username "Piano.Man." According to Minor Victim One, she had told **PYSHER** she was 14 years old[6] and **PYSHER** told her he was 18 years old.

b. During the time period they were chatting on Discord, **PYSHER** pressured Minor Victim One to send him naked images of herself. Minor Victim One ended up sending approximately four nude images of herself to **PYSHER** at his direction.

c. Minor Victim One said that **PYSHER** had come to California on February 20, 2026 to see her. Minor Victim One said she had left her home and met **PYSHER** by a bridge near her house where **PYSHER** was being driven by a female individual. The female individual then drove **PYSHER** and Minor Victim One to the Rodeway Inn Motel.

d. Once inside the motel, **PYSHER** cut Minor Victim One several times with a knife on her left and right forearms for approximately 15 minutes. After **PYSHER** was done cutting Minor Victim One, a sock was used to stop the bleeding. Afterwords **PYSHER** had sexual intercourse with Minor Victim One even though Minor Victim One said she did not want to. During intercourse, **PYSHER** repeatedly choked her to the point that Minor Victim One could not speak.

e. Minor Victim One told law enforcement that **PYSHER's** plan was for them to go to the top of a "big" hotel and jump off together.

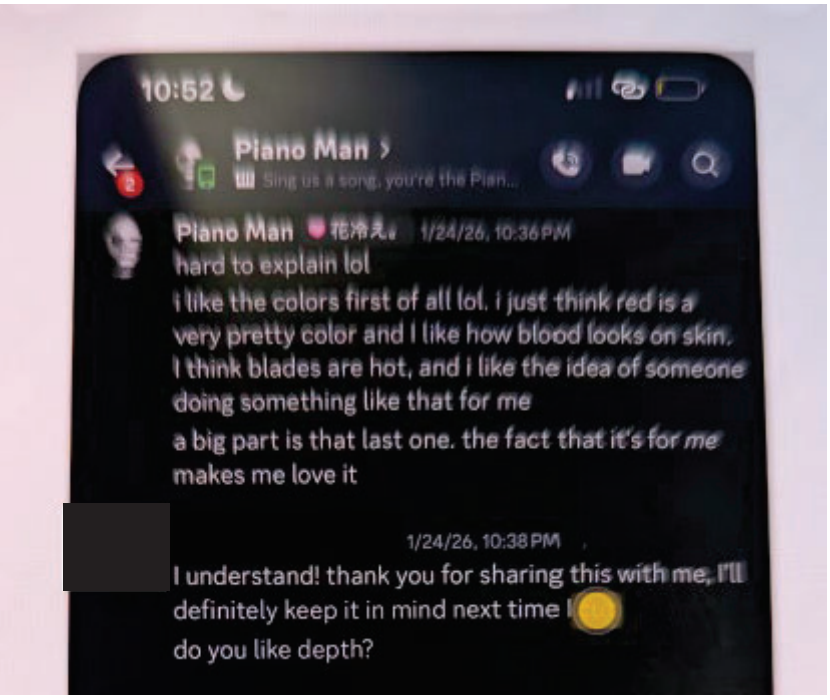
---

[6] Minor Victim One is in fact 13 years and was 12 years old during the majority of the time she was speaking with **PSYHER**.

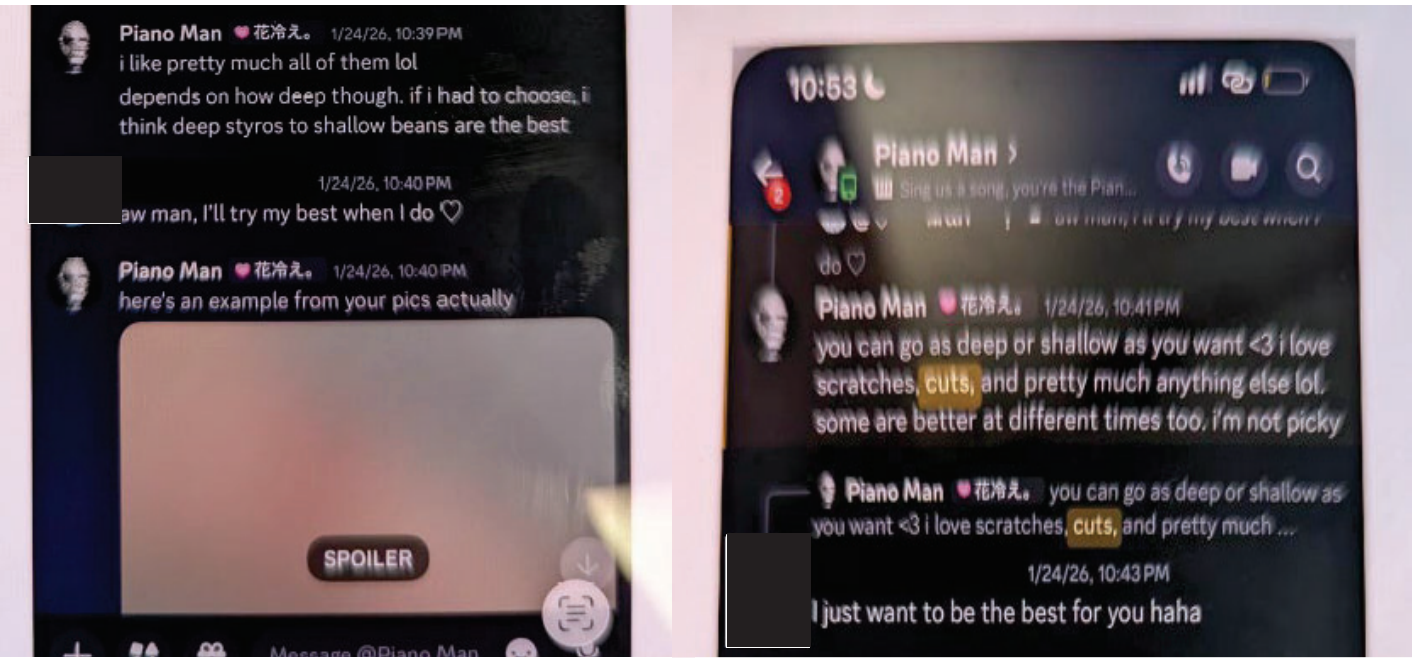
f. Minor Victim One told law enforcement that all the items inside the hotel room were **PYSHER's** including the backpack in which the condoms were found.

D. Seized Communications Show that PYSHER Groomed and Abused Minor Victim One Before Traveling to California

26. Based on my review of communications between "Piano Man" (i.e., **PYSHER**) and Minor Victim One found on Minor Victim One's cellular phone, I know that **PYSHER** engaged in grooming activity that encouraged Minor Victim One to harm herself, including by cutting deep wounds into her body. For example, on January 24, 2026, after Minor Victim One sent **PYSHER** photographs depicting multiple wounds on Minor Victim One's arm, **PYSHER** wrote "i like the colors ... i just think red is a very pretty color and I like how blood looks on skin." **PYSHER** also told Minor Victim One "the fact that [Minor Victim One cut herself] [is] for *me* makes me love it."



27. The text communications also show that **PYSHER** encouraged Minor Victim One to harm herself and gave Minor Victim One directions about how to cut herself, as depicted in the following screenshots:



E. PYSHER Admitted He Traveled to California to Meet With Minor Victim One

28. After entering the hotel room, I met **PYSHER** who agreed to speak with me after being read his Miranda rights, and learned the following:

a. **PYSHER** traveled from Philadelphia to California on February 20, 2026, in order to see Minor Victim One

b. **PYSHER** admitted to meeting Minor Victim One over the internet prior to coming to California.

c. **PYSHER** said he did not buy anything while in California except food and toothpaste.

d. **PYSHER** was amenable to the idea that Minor Victim One should commit suicide.

29. Based on these admissions, I came to the conclusion that **PYSHER** had traveled from Pennsylvania to California with the intent to engage in sexual activity with Minor Victim One. In part, I came to this conclusion based on the fact that **PYSHER** had likely brought condoms and lubricant with him from across the country and had not purchased them here in California meaning that he had planned to engage in sexual acts with Minor Victim One before traveling to California.

30. Based on my training, experience, and conversation with other law enforcement officers, I believe there is probable cause to establish that **PYSHER's** activities are consistent with NVE ideology. Namely, I have come to this conclusion based on **PYSHER's** demonstrated interest in cutting (including of minor victims such as Minor Victim One), his use of Discord to recruit and groom minor victims, and his Nihilistic ideation including his encouragement to Minor Victim One to commit suicide.

VI. BACKGROUND ON CHILD EXPLOITATION OFFENSES, COMPUTERS, THE INTERNET, AND DEFINITION OF TERMS

31. In this affidavit, the terms "minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256. The term "computer" is defined as set forth in 18 U.S.C. § 1030(e)(1).

32. Based upon my training and experience in the investigation of child pornography, and information related to

me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers with child pornography:

a. Computers and Child Pornography. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Child pornographers can now produce both still and moving images directly from a common video camera and can convert these images into computer-readable formats. The use of digital technology has enabled child pornographers to electronically receive, distribute, and possess large numbers of child exploitation images and videos with other Internet users worldwide.

b. File Storage. Computer users can choose their method of storing files: either on a computer's hard drive, an external hard drive, a memory card, a USB thumb drive, a smart phone or other digital media device, etc. (i.e., "locally") or on virtual servers accessible from any digital device with an Internet connection (i.e., "cloud storage"). Computer users frequently transfer files from one location to another, such as from a phone to a computer or from cloud storage to an external hard drive. Computer users also often create "backup," or duplicate, copies of their files. In this way, digital child pornography is extremely mobile and such digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto external hard drives small enough to fit onto a keychain. Just as easily, these files can be copied onto

compact disks and/or stored on mobile digital devices, such as smart phones and tablets. Furthermore, even if the actual child pornography files are stored on a "cloud," files stored in this manner can only be accessed via a digital device. Therefore, viewing this child pornography would require a computer, smartphone, tablet, or some other digital device that allows the user to access and view files on the Internet.

c. Internet. The term "Internet" is defined as the worldwide network of computers -- a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider ("ISP"), which operates a host computer with direct access to the Internet.

d. Internet Service Providers. Individuals and businesses obtain access to the Internet through ISPs. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the

individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

e. IP Addresses. An Internet Protocol address ("IP Address") is a unique numeric address used to connect to the Internet. An IPv4 IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). In simple terms, one computer in a home may connect directly to the Internet with an IP Address assigned by an ISP. What is now more typical is that one home may connect to the Internet using multiple digital devices simultaneously, including laptops, tablets, smart phones, smart televisions, and gaming systems, by way of example. Because the home subscriber typically only has one Internet connection and is only assigned one IP Address at a time by their ISP, multiple devices in a home are connected to the Internet via a router or hub. Internet activity from every device attached to the router or hub is utilizing the same external IP Address assigned by the ISP. The router or hub "routes" Internet traffic so that it reaches the proper device. Most ISPs control a range of IP Addresses. The IP Address for a user may be relatively static, meaning it is assigned to the same subscriber for long periods of time, or dynamic, meaning that the IP Address is only assigned for the duration of that

online session. Most ISPs maintain records of which subscriber was assigned which IP Address during an online session.

f. IP Address – IPv6. Due to the limited number of available IPv4 IP addresses, a new protocol was established using the hexadecimal system to increase the number of unique IP addresses. An IPv6 consists of eight sets of combination of four numbers 0-9 and/or letters A through F. An example of an IPv6 IP address is 2001:0db8:0000:0000:0000:ff00:0042:8329.

g. The following definitions:

i. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

ii. "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit links to electronic files to other individuals within the chat room.

iii. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

iv. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, 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.

v. "Cloud-based storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is typically free and readily available to anyone who has an Internet connection.

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

vii. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

viii. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other

digital form. It commonly includes programs to run operating systems, applications, and utilities.

ix. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates 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 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.

x. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

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

xii. The "Internet" is a global network of computers and other electronic devices that communicate with

each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

xiii. "Internet Service Providers" ("ISPs"), as used herein, 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, email, remote storage, and co-location of computers and other communications equipment.

xiv. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device 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. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

xv. "Log files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

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

xvii. "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.

xviii. "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.

xix. "Remote computing service," 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.

xx. "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 anus, genitals, or pubic area of any person.

xxi. A "storage medium" or "storage device" 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.

xxii. "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.

xxiii. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

VII. TRAINING & EXPERIENCE ON INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

33. Based on my training and experience, and the training and experience of other law enforcement officers with whom I

have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children 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 in other visual media, or from literature describing such activity. These individuals often maintain possession of these items for long periods of time and keep their collections in numerous places – in digital devices in their homes, in their cars, in their workplaces, or on their persons.

b. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials (including through digital distribution via the Internet); conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. These individuals often maintain possession of these items for long periods of time.

34. Digital child pornography on a digital device is easy to maintain for long periods of time. Modern digital devices often have extremely large storage capacities. Furthermore, cheap and readily available storage devices, such as thumb drives, external hard drives, and compact discs make it simple for individuals with a sexual interest in children to download child pornography from the Internet and save it – simply and securely – so it can be accessed or viewed indefinitely.

35. Furthermore, even if a person deleted any images of child pornography that may have been possessed or distributed, there is still probable cause to believe that there will be evidence of the illegal activities – that is, the possession, receipt, and/or distribution of child pornography – at the SUBJECT PREMISES or on his person. Based on my training and experience, as well as my conversations with digital forensic experts, I know that remnants of such files can be recovered months or years after they have been deleted from a computer device. Evidence that child pornography files were downloaded and viewed can also be recovered, even after the files themselves have been deleted, using forensic tools. Because remnants of the possession, distribution, and viewing of child pornography is recoverable after long periods of time, searching the SUBJECT PREMISES could lead to evidence of child exploitation offenses.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[7]

36. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has

[7] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

37. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

38. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a

device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the PYSHER's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of the PYSHER's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

X. CONCLUSION

39. For all the reasons described above, there is probable cause to believe that PYSHER has committed a violation of Title 18, United States Code, Section2423(b) (Travel with Intent to Engage in Illicit Sexual Conduct).

40. Further, for all the reasons described above, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of the Subject Offenses, as

described more fully in Attachment B, will be found in a search of the items described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 22nd day of February, 2026.

HON. PEDRO V. CASTILLO
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DEVICES TO BE SEARCHED

The following digital devices that are currently maintained in the custody of the Federal Bureau of Investigation in Los Angeles, California: (1) one black Samsung phone with IMEI 351219580989581, seized from PYSHER's hotel room on February 20, 2026 ("**SUBJECT DEVICE 1**"); and (2) one Valve Steamdeck with serial code FYZZ3510BD91, seized from PYSHER's hotel room on February 20, 2026("**SUBJECT DEVICE 2**" and collectively, the "SUBJECT DEVICES").

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 371 (Conspiracy); 18 U.S.C. § 2251(a) (sexual exploitation of children and attempted sexual exploitation of children), 18 U.S.C. § 2252A(a)(2) (receipt and distribution of child pornography); 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography); 18, U.S.C. § 2251(a)(e) (production of child pornography); and 18 U.S. Code § 2423(b) (Travel with Intent to Engage in Illicit Sexual Conduct) namely:

a. Child pornography, as defined in 18 U.S.C. § 2256(8).

b. Any communications between **PYSHER** and Minor Victim One regarding their plans to meet in February of 2026;

c. Any communications between **PYSHER** and any co-conspirators regarding the plan to meet Minor Victim One in February of 2026;

d. Any records of **PYSHER**'s travel to Los Angeles on February 20, 2026;

e. Any records, documents, or materials, tending to identify the individual who transported **PYSHER** and Minor Victim One to the motel on February 20, 2026;

f. Any records, documents, or materials, showing **PYSHER** communicating with minors to solicit sexually explicit content and/or related to self-harm and mutilation.

g.

h. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, that refer to child pornography, as defined in 18 U.S.C. § 2256(8), including but not limited to documents that refer to the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, of child pornography.

i. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, including but not limited to financial records, tending to identify persons involved in the possession, receipt, distribution, transmission, reproduction, viewing, sharing, purchase, or downloading, production, shipment, order, requesting, trade, or transaction of any kind, involving child pornography, as defined in 18 U.S.C. § 2256.

j. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, that refer or relate to any production, receipt, shipment, order, request, trade, purchase, or transaction of any kind involving the transmission through interstate commerce by any means, including by computer, of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

k. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, identifying persons transmitting in

interstate commerce, including by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

l. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

m. Any and all records, documents, programs, applications, or materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

n. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, identifying possible minor victims depicted in child pornography and/or minor victims of sexual abuse.

o. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, related to the "764" network or any other known nihilistic violent extremism group, including activities

related to grooming children to produce sexually explicit and/or self-harm images or videos, and extortion of victims.

p. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, which pertain to peer-to-peer file-sharing software.

q. Any records, documents, programs, applications, or materials, including physical items and electronic mail and electronic messages, which pertain to accounts with any Internet Service Provider.

r. Records, documents, programs, applications, materials, and files relating to the deletion, uploading, and/or acquisition of victim files to include photographs, videos, e-mails, chat logs, or other files.

s. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

2. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

3. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, 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 attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

4. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

SEARCH PROCEDURE FOR THE SUBJECT DEVICES

5. In searching the SUBJECT DEVICES or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in

their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 365 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 365-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the scope of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other

sophisticated techniques, including to search for known images of child pornography.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the scope of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the scope of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the scope of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been

able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress PYSHER's thumb and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of PYSHER's face with his eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than

objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.