AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent Christopher Henschel, with the Federal Bureau of Investigation (FBI), being duly sworn, deposes and states the following:

INTRODUCTION

1. This affidavit is submitted in support of a search warrant pursuant to Rule 41(b)(6)(A) of the Federal Rules of Criminal Procedure for law enforcement to use a remote access search technique. In particular, I request approval for law enforcement to use a remote access search technique to send one or more communications to the servers of the online company Telegram Messenger, Inc. to access the account of Telegram User ID: 7467415149 with a display name of "@Unknown 69" and phone number of 717-708-1660 (the "Subject Account"). Each such communication is designed to cause the servers to transmit information to law enforcement, including "@Unknown 69" communications and other information from the Subject Account on Telegram. Once that information is downloaded to a computer in this district and/or the Subject Phone in this district, law enforcement will not attempt to gain access to the Subject Account without approval from the Court through further legal process, if necessary.

2. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), that is, the receipt, distribution, possession, and access with intent to view child pornography (collectively, the "Subject Offenses") have occurred and that evidence and instrumentalities of the Subject Offenses exist on Telegram servers described in Attachment A. The whereabouts of those Telegram servers and the information sought in the search warrant is unknown and concealed through technological means.

3. Accordingly, this affidavit is made in support of an application for a warrant authorizing a remote access search of Telegram servers for evidence and instrumentalities of the Subject Offenses, as described in Attachment B. Attachments A and B are incorporated herein by reference.

4. The information set forth in this affidavit is based upon my personal knowledge of this investigation and information conveyed to me by others involved with the investigation, including others with knowledge regarding both the technical aspects of Telegram and how it stores its data. Since this affidavit is being submitted for the limited purpose of establishing probable cause for the requested search warrant, I have not included every detail of every aspect of the investigation known to me or to the government. Rather, the following paragraphs set forth only those facts necessary to support a finding of probable cause.

AGENT BACKGROUND

5. I, Christopher Henschel, am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation ("FBI") and have been employed with the FBI since February 2013. I am a graduate of the FBI Academy in Quantico Virginia. I am currently assigned to the FBI Philadelphia Division Allentown Resident Agency ("ARA").

6. As part of my duties as an FBI agent, I investigate criminal violations relating to the sexual exploitation of children, including the illegal coercion and enticement of minors, and the production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2422, 2251, 2252, and 2252A. I have received training in the area of child exploitation and have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256, in all forms of media.

7. I am an "investigative or law enforcement officer of the United States" within the meaning defined in 18 U.S.C. § 2510(7), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

STATUTORY AUTHORITY

8. Title 18 U.S.C. § 2252(a)(2) prohibits the knowing receipt or distribution of any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in or affecting interstate or foreign commerce, by any means, including by computer.

9. Title 18 U.S.C. § 2252(a)(4)(B) prohibits the knowing possession or access with intent to view of one or more books, magazines, periodicals, films, or other materials which contain any visual depictions of minors engaged in sexually explicit conduct that have been transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce, by any means, including by computer.

DEFINITIONS

10. The following definitions apply to this Affidavit and its Attachments:

a. 18 U.S.C. § 2256(1) defines "minor" as any person under the age of eighteen years.

b. 18 U.S.C. § 2256(8) defines "child pornography" in relevant part as "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 … the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

c. 18 U.S.C. § 2256(2) defines "sexually explicit conduct" as actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals, or pubic area of any person.

d. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or by 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.

e. "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 in sexually explicit poses or positions.

f. "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.

g. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other highspeed 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, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

h. "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.

i. "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.

CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN OR VISUAL DEPICTIONS OF CHILDREN

11. I know from my training and experience that the following characteristics are prevalent among individuals who collect child pornography:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, 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. Due to the accessibility and availability of child pornography on the Internet, in my recent experience, instead of maintaining collections, some offenders engage in a pattern of viewing or downloading child pornography online and then deleting the material.

b. Individuals who have a sexual interest in children or images of children 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. They may also 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. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections can be maintained for several years to enable the individual to view the collection, which is valued highly.

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

e. Individuals who have a sexual interest in children or images of children 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.

f. Individuals whose sexual interest in children or images of children has led them to purchase access to paid websites or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences.

BACKGROUND CONCERNING TELEGRAM

12. Telegram Messenger (also known as "Telegram") is an encrypted cloud-based mobile and desktop messaging application purportedly owned and/or controlled by Telegram Messenger Inc. Telegram can be used on smartphones, such as Apple iOS and Google Android devices, and on desktop computers, by users to send messages and media to each other.

13. Telegram was founded in Russia, but, according to its website, it purportedly "has tried a number of locations as its base," and currently its "development team is based in Dubai."[1]

14. To sign up for a Telegram account, a user must provide a phone number. Telegram users can also select a username but are not required to. Usernames are unique, meaning only one user can have a particular username. Users can also select a display name, such as a first and last name. Display names are not unique.

15. Telegram is supported on various devices including smartphones, tablets, desktop computers and laptop computers, and Telegram can by synced on multiple devices at the same time. A user can log into Telegram using a phone number from as many devices as that user likes, even simultaneously. Unless a user enables a "lock" on the Telegram application, which may include two-factor authentication, anyone who gains access to an unlocked smartphone, tablet, or computer running Telegram will be able to access and view a user's Telegram account.

16. Telegram offers a variety of communication methods for its users:

a. Chats. Users on Telegram can communicate with each other through chats. They can send each other text messages, photos, videos, any files, and make voice calls.

[1] https://telegram.org/faq (last visited September 24, 2025).

b. Secret Chats. Secret chats use end-to-end encryption, which means only the sender and recipient have the ability to view the content of the chats. These secret chats also disappear and can be set to self-destruct.

c. Groups. Telegram allows collections of users to communicate with each other in chat rooms called groups. Groups may be by invitation only.

17. According to Telegram's privacy policies, Telegram stores basic user account data, including mobile number, profile name, profile picture, screen names, and e-mail address, to the extent a user has provided this information.[2] Telegram also stores messages, photos, videos and documents from a user's chats and private messages, as well as from public channels and public groups in which the user participates.

18. In my training and experience, evidence of who was using a Telegram account and from where, and evidence related to criminal activity, including the Subject Offenses, may be found in the files and records described above. This evidence may establish 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. The records and information described in Attachment B represent the type of data expected to be located in the Subject Account based on my experience and that of other federal agents.

19. Telegram advertises that it provides server-client encryption for private and group chats, and optional client-client encryption for chats and video calling.[3] Some Telegram users

[2] https://telegram.org/privacy (last visited September 24, 2025).

[3] https://telegram.org/faq#q-so-how-do-you-encrypt-data (last visited on September 24, 2025).

likely use its services to address legitimate concerns to keep online information private. However, in my training and experience, Telegram is known to law enforcement as a tool used by some individuals for the purpose of discussing or even furthering criminal activity because those individuals believe that their communications are untraceable due to the application's encryption option. Multiple newspaper articles have even described Telegram as the "app of choice" for terrorists.[4] In my training and experience with investigating child exploitation cases and from speaking with other law enforcement agents, I am aware that some individuals who traffic in child sexual abuse material use Telegram because they believe their communications are untraceable due to Telegram's encryption option.

20. According to Telegram's "Who Your Personal Data May Be Shared With" section of its privacy policy, Telegram states that if it ("If Telegram receives a valid order from the relevant judicial authorities that confirms you're a suspect in a case involving criminal activities that violate the Telegram Terms of Service, we will perform a legal analysis of the request and may disclose

---

[4] *See, e.g.*, Ben Quinn, *Telegram is warned app 'nurtures subculture deifying terrorists'* (Oct. 14, 2021), https://www.theguardian.com/uk-news/2021/oct/14/telegram-warned-of-nurturing-subculture-deifying-terrorists ("The risk of radicalisation has grown on some platforms after sweeping bans on larger, more mainstream platforms encouraged many conspiratorial networks to migrate to often largely unmoderated alternatives such as Telegram, the report says."); Maggie Rowland, *Extremism and Encryption: Terrorists on Telegram* (Aug. 10, 2017), https://www.hsdl.org/c/extremism-and-encryption-terrorists-on-telegram/ ("Telegram is now the app of choice for terrorist propaganda, communication, and organization."); Jessica Clarence, *The trouble with Telegram (part 1)* (Jul. 11, 2018), https://www.aspistrategist.org.au/the-trouble-with-telegram-part-1/ ("Telegram is also structured to resist government requests and subpoenas. It's incorporated in Dubai, but its servers' locations and employees' names are secret, thanks to a complex of transnational shell companies scattered worldwide. Access to user data requires not only international cooperation, but knowing where the data is located—a nearly impossible task without cooperation from the messaging service.").

your IP address and phone number to the relevant authorities. If any data is shared, we will include such occurrences in a quarterly transparency report published at: https://t.me/transparency.[5]) Telegram further states:

> To protect the data that is not covered by end-to-end encryption, Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force us to give up any data.
>
> Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world.
>
> To this day, we have disclosed 0 bytes of user data to third parties, including governments.[6]

21. Telegram's description of a "distributed infrastructure" is somewhat at odds with other information Telegram has provided. Currently, Telegram states that UK or the Economic European Area account data "is stored in data centers in the Netherlands." But Telegram's website does not state where United States account data is stored. In a 2014 tweet, Telegram stated it used "San Francisco" servers for "American" data.

[5] *See, e.g., United States v. Elshinawy*, No. CR ELH-16-009, 2018 WL 1521876 (D. Md. Mar. 28, 2018), aff'd, 781 F. App'x 168 (4th Cir. 2019) (defendant conceded that he used Telegram to talk to ISIS contacts for the purpose of encrypted communications; FBI agents testified that the government could not recover any of the defendant's communications on Telegram).

[6] https://telegram.org/faq#q-do-you-process-data-requests (last visited September 24, 2025).

22. Law enforcement is not aware of where United States account data is stored at this time, and Telegram will not provide that information to law enforcement. Even if law enforcement knew where United States account data is stored, Telegram states that the information stored at its data centers is "heavily encrypted so that local Telegram engineers or physical intruders cannot get access."

23. Ultimately, in my training and experience, Telegram's business model is designed to conceal information related to customer accounts in the United States and elsewhere through technological means. Telegram's founder and CEO, Pavel Durov tweeted, "We've no issue with formalities, but not a single byte of private data will ever be shared with any government."[7]

24. Based on my training and experience, information provided by other agents, and Telegram's own description of its services, Telegram is supported on various devices including smartphones, tablets, desktop computers and laptop computers, and Telegram can by synced on multiple devices at the same time. Although Telegram provides the options of (1) 2-step verification for logging in; and/or (2) requiring a passcode before a Telegram user's account can be accessed, typically once a user logs into a Telegram from a device (like a smartphone), anyone who later possess that same device can access a user's Telegram account from that device, without a password or other verification, unless the user logged out of Telegram the last time the user used Telegram from any device. Typically, a Telegram user does not log out of Telegram after using it. A user (or a third party with access to a user's account on a device that was already logged on) who accesses an account can retrieve the user's previous activity on Telegram, including chats,

[7] https://twitter.com/durov/status/880114461075439616 (last visited September 24, 2025).

messages in groups, etc., if the user did not previously delete it or Telegram did not automatically delete it.[8]

JURISDICTION

25. This Court has jurisdiction to issue the requested warrant under Rule 41(b)(6)(A) because the above facts establish there is probable cause to believe that the district where the information is located has been concealed through technological means. In addition, the below facts establish that there is probable cause to believe that activities related to the Subject Offenses being investigated occurred within this judicial district. As discussed more fully below, acts or omissions in furtherance of the Subject Offenses under investigation occurred within the Eastern District of Pennsylvania. *See* 18 U.S.C. § 3237.

26. As explained above, Telegram uses technological means to anonymize the location of customer account information and the methods by which Telegram stores that information. Although various other cloud-based communications platforms deploy technologies and techniques similar to Telegram for data privacy reasons, Telegram is the only major provider known to ignore law enforcement requests for information—even boasting about doing so—including in cases involving terrorism and other serious offenses. Accordingly, a search warrant issued by this court to Telegram under the Stored Communications Act, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), would not result in "***required*** disclosure of customer communications or records," and would otherwise be futile because (1) Telegram does not respond to legal process; (2) a search warrant or other legal process cannot be served in the jurisdiction of

[8] https://telegram.org/faq#q-i-have-a-new-phone-number-what-do-i-do; https://telegram.org/faq#q-how-do-i-change-my-phone-number ("You can change your number in Telegram and keep everything . . .") (last visited September 24, 2025).

the location of the Subject Account's information because the location of Telegram servers is unknown and Telegram states it uses technological means, i.e., a "distributed infrastructure," to store customer account information in multiple physical locations at any given time; and (3) even if the location of the Subject Account's information were known and the information were in a single jurisdiction, Telegram states it uses technological means, i.e., encryption, to prevent customer account information from being accessed in jurisdictions where servers are located.

PROBABLE CAUSE

27. In April 2025, FBI New York began an investigation into the Telegram account "Steve Jobs" with the username "@perv_94," which was used to trade child sexual abuse material (CSAM) with other Telegram users. The investigation yielded information that the Telegram account "Steve Jobs" @perv_94 was operated by Mario Pineiro (PINEIRO). The investigation showed that other Telegram users interested in trading child pornography originally found the @perv_94 Telegram account via the social media website and application X.

28. On May 27, 2025, FBI New York obtained a search warrant issued by United States Magistrate Judge Robyn F. Taronofsky of the United States District Court of the Southern District of New York, which authorized the search of the residence of PINEIRO located in New York, New York for evidence of the distribution and receipt of child pornography.

29. On May 29, 2025, Special Agents of FBI New York's Child Exploitation and Human Trafficking Task Force executed the search warrant at the residence of PINEIRO in New York, New York.

30. On May 29, 2025, PINEIRO confirmed that he was the user of the "Steve Jobs" @perv_94 Telegram account and that he used the account to receive and distribute CSAM.

PINEIRO provided consent to the FBI to assume the online identity of the Telegram account "Steve Jobs" @perv_94.

31. On or about May 29, 2025, an FBI Online Cover Employee (OCE) accessed the "Steve Jobs" @perv_94 Telegram account. FBI New York observed communications between "Steve Jobs" @perv_94 and a Telegram user with the display name of "Unknown 69" (Telegram User ID: 7467415149) (hereinafter "Unknown 69"), the Subject Account. The communications contained both the distribution and receipt of CSAM.

a. On or about May 26, 2025," Unknown 69" sent "Steve Jobs" @perv_94 the message, "Any black Megas[.]" "Steve Jobs" @perv_94 responded with, "nah sorry" and "any straight vids to trade" to which "Unknown 69" replied affirmatively, "Yeah."

b. Subsequently, on or about May 26, 2025, "Steve Jobs" @perv_94 sent "Unknown 69" approximately 80 video files containing CSAM that primarily depicted female children, some of whom appeared to be pre-pubescent, engaging in sexual conduct. A review of files sent from "Steve Jobs" @perv_94 to "Unknown 69" depicted multiple child pornography videos, including video file "video_35@26-05-2025_21-46-53," a 39 second video depicting a female toddler being forced to perform oral sex on an adult male. The toddler is seen crying at the end of the video.

c. On or about May 27, 2025, "Unknown 69" sent "Steve Jobs" @perv_94 approximately 99 video files containing CSAM that primarily depicted female children, some of whom appeared to be pre-pubescent, engaging in sexual conduct. A review of files sent from "Unknown 69" to "Steve Jobs" @perv_94 depicted multiple child pornography videos, including video file "video_112@27-05-2025_01-45-43," a 41 second video depicting an adult male

pulling the diaper of a female toddler to the side while attempting to digitally penetrate the vagina of the toddler.

d. Further, "Unknown 69" and "Steve Jobs" @perv_94 exchanged MEGA[9] folders and "Uknown 69" asked, "You have any Yandex[3] or DropBox[?]"

32. On June 17, 2025, Telegram provided information regarding Telegram user "Unknown 69," which revealed that the user utilized phone number (717) 708-1660 and IP address 73.230.77.193 on June 17, 2025 at 4:06:41 Eastern Daylight Time (EDT) to access Telegram.

33. On July 1, 2025, Comcast provided subscriber information regarding IP address 73.230.77.193 utilized on June 17, 2025 at 4:06:41 EDT. The account resolved to ALEXIS JOHNSON, located at 136 Elm Street, Apartment 2, Reading, Pennsylvania 19601-2982.

34. On July 11, 2025, Verizon Wireless provided the account information regarding phone number (717) 708-1660, which resolved to ALEXIS JOHNSON at 438 South 5th Street, Reading, Pennsylvania 19602. After review of law enforcement databases, it appears this phone number is linked to both ALEXIS JOHNSON and MATTHEW MCKINNEY.

35. On July 29, 2025, Telegram user "Unknown 69" sent the FBI OCE one video containing CSAM that depicted an adult male engaging in penetrative vaginal intercourse with a female child who appeared to be approximately 10 or 11 years old. "Unknown 69" requested the FBI OCE send videos depicting "booty" and "lesbian." Subsequently, "Unknown 69" sent the

9 Mega is a company that provides file-hosting and communications services to the public through the website Mega.nz. Mega is headquartered at Level 21, Huawei Centre, 120 Albert Street, Auckland, New Zealand. Much of Mega's computer architecture is believed to be located in New Zealand, and Mega does not have offices or employees in the United States. Based on my training and experience, I know Mega to be a file-sharing system commonly used for the exchange of child pornography.

FBI OCE a MEGA link containing approximately 1,100 videos. A review of the files sent from "Unknown 69" depicted multiple child pornography videos, including video file "VID20180108-WA0034," a 49 second video depicting a nude 3 to 5 year-old minor female performing oral sex on an adult male.

36. On July 29, 2025 the FBI OCE requested Telegram user "Unknown 69" add the OCE on MEGA. On July 30, 2025, "Unknown 69" told the OCE via a message on Telegram, "There I sent Inv" and "Get the inv[?]" Upon checking the OCE's MEGA account, the OCE observed a new contact add from a MEGA account with the username tattedmf97@gmail.com. "Unknown 69" confirmed in a Telegram message sent to the OCE that "tatmf" was the Mega account belonging to "Unknown 69."

37. On August 1, 2025, FBI Philadelphia ARA Agents served a subpoena to Google, Inc. for subscriber information for Google account tattedmf97@gmail.com. On August 1, 2025, Google provided the subscriber information account for tattedmf97@gmail.com. Tattedmf97@gmail.com resolved to Google Account ID 365561245056 and the user was listed as "Name: Mat" and "Given Name: Mat."

38. A Pennsylvania Department of Transportation record query yielded that MATTHEW MCKINNEY with date of birth December 27, 1997 resides at 136 Elm Street, 6 Apartment B, Reading, Pennsylvania 19601. MCKINNEY's driver's license photo yielded numerous and distinctive tattoos across his face. Open-source searches revealed ALEXIS JOHNSON and MATTHEW MCKINNEY are married.

39. On August 1, 2025, FBI ARA conducted surveillance at 136 Elm Street, Apartment 2, Reading, Pennsylvania. Agents observed that a small black mailbox affixed to the front of the

house near the entrance listed “Matt MCK” and “Lexi MC” on the mailbox. Based upon this investigation I believe that these initial refer to Matthew McKinney (Matt MCK) and his wife, Alexis Johnson (Lexi MC).

40. On August 4, 2025, FBI ARA conducted surveillance at the 136 Elm Street, Apartment 2, Reading, Pennsylvania. An agent observed a white Ford SUV with license plate “MTY9601,” which was registered to MATTHEW MCKINNEY, address 136 Elm Street, Apartment B, Reading, Pennsylvania 19601, parked in front of the residence.

41. On August 4, 2025, an FBI ARA Agent traveled to 438 South 5th Street, Reading, Pennsylvania, the address associated with ALEXIS JOHNSON in Verizon’s records for phone number (717) 708-1660. The building contained three separate apartments. The Agent observed the mailboxes affixed near the front entrance of the building, and Apartments #1 and #2 were marked as vacant. Agent spoke with a tenant in Apartment #3. The tenant identified Pennsylvania driver’s license photographs of MATTHEW MCKINNEY and ALEXIS JOHNSON as the previous tenants in Apartment #2 at 438 South 5th Street. The tenant related MCKINNEY and JOHNSON moved out of the apartment sometime in late 2024 to an unknown location.

42. On August 7, 2025, your affiant applied for and was granted a federal search warrant by United States Magistrate Judge Pamela A. Carlos, Eastern District of Pennsylvania, to search the residence at 136 Elm Street, Apartment 2, Reading, Pennsylvania 19601, for evidence of violations of Title 18 U.S.C., Section 2252 (transportation, receipt, distribution, and/or possession of child pornography).

43. On August 8, 2025, the search warrant was executed at 136 Elm Street, Apartment 2, Reading, Pennsylvania. At the time the search warrant was executed, MATTHEW MCKINNEY was inside the residence, along with his wife, ALEXIS JOHNSON, and the couple's three minor children.

44. During the execution of the search warrant, FBI recovered an Apple iPhone 16 Pro Max in a black case (Subject Device), which ALEXIS JOHNSON identified as MATTHEW MCKINNEY's cellular phone.

45. After being advised of his Miranda warnings (both orally and in writing), MATTHEW MCKINNEY agree to speak with FBI Special Agents Eddie Garcia and Carmen Dvorak de Morales. This interview was audio-recorded.

46. During the interview, MATTHEW MCKINNEY stated that his phone number was (717) 708-1660, the phone number associated with the Telegram account "Unknown 69." ALEXIS JOHNSON confirmed that while the account was in her name, MATTHEW MCKINNEY was the user of phone number (717) 708-1660.

48. MATTHEW MCKINNEY admitted to being the user of the Telegram account "Unknown 69," but stated that he deleted the Telegram app from his cell phone. He also confirmed that tattedmf97@gmail.com was his email address. MATTHEW MCKINNEY admitted that he used both the Telegram and MEGA apps to send, receive, and view child pornography.

49. At the request of FBI Special Agents Garcia and Dvorak de Morales, MATTHEW MCKINNEY redownloaded the Telegram app to his cellular phone. Within the app, agents were able to observe hundreds of depictions of child pornography, including both images and videos.

This included a nineteen-second video of a prepubescent female, approximately 5 to 7 years old, who is lying on a bed nude as an adult male digitally penetrates her anus with his finger. This image was received by "Unknown 69" via the Telegram app on August 4, 2025 at 5:30a.m. Based on a manual review of the Telegram account, agents were unable to access the full content within the account.

50. On August 8, 2025, MATTHEW MCKINNEY was arrested via complaint and warrant and charged with one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2).

51. Based on my training, experience, and research regarding Telegram, I know the only way to obtain the full chat history and files being received and distributed is to access the Telegram server where the files are stored.

52. Your Affiant believes that a remote access search of the Subject Account on Telegram servers is necessary in order to obtain complete communications and files exchanged between users regarding the receipt, distribution, possession, and access with intent to view child pornography.

THE REMOTE ACCESS SEARCH TECHNIQUE

53. Based on my training, experience, the investigation described above, I have concluded that using a remote access search technique will help law enforcement access the Subject Account on Telegram servers. Accordingly, I request authority to use the remote access search technique, which will be deployed via electronic communications, to search the Subject Account. This remote access search technique will consist of one of the following actions by law enforcement, with the assistance of a forensic expert, to access the Subject Account, which may include a limited search

of the Subject Device: (1) use a forensic tool like Cellebrite Cloud Analyzer or Oxygen Forensic Cloud Data tool to access the Subject Account in a forensic manner; (2) using tokens and encryption keys already extracted from or stored on the Subject Device and lawfully in possession of law enforcement (collectively, the "Credentials") to enter those Credentials into Telegram's online webpage in order to access the Subject Account, or (3) powering on the Subject Device, enabling its internet connection in order to access the Subject Account through the Telegram application on the Subject Device, and using the Telegram application to login to the Subject Account on Telegram's online webpage. If law enforcement accesses the Subject Account using the online webpage, the forensic expert will extract the existing communications and other information from the Subject Account, and then exit the Subject Account. If law enforcement accesses the Subject Account by powering on the Subject Phone and enabling its internet connection, and is unable to login to the Subject Account using Telegram's online webpage, the forensic expert will conduct a manual search of the Telegram application and then re-image the Subject Device. After the search is completed, law enforcement will disconnect the Subject Device from the internet. Law enforcement will not re-access the Subject Account once this remote access search technique has been fully completed without seeking further legal process from the Court, if necessary.

54. Based on my training, experience, and consultation with forensic computer experts, I know that information gathered from the remote access search can be effective in searching and seizing communications of the Subject Account in the Telegram application. This is because the information will be obtained directly from Telegram servers and may be able to defeat the various anonymization techniques that Telegram employs.

55. The remote access search technique is designed to collect the items described above and in Attachment B, to include the Subject Account's Telegram chats, secret chats, and group communications which may be evidence of violations of the Subject Offenses described above.

CONCLUSION

56. Based on the information herein, your affiant submits that there is probable cause to believe that the Subject Account has been utilized to violate federal criminal laws including Title 18 U.S.C. § 2252(a)(2) and 2252(a)(4)(B), that is, the receipt, distribution, possession, and access with intent to view child pornography. Your Affiant also respectfully submits there is probable cause to believe that a remote access search of the Subject Account on Telegram servers, which is further described in Attachment A, will reveal additional evidence, fruits, and/or instrumentalities of the Subject Offenses, including the items listed in Attachment B.

Respectfully submitted,

/s/ *Christopher Henschel*
Christopher Henschel
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on September 25, 2025.

PAMELA A. CARLOS
Digitally signed by PAMELA A. CARLOS
Date: 2025.09.25 15:15:16 -04'00'

HONORABLE PAMELA A. CARLOS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Locations to be searched

(1) The portion of Telegram servers that stores communications and other information from the Telegram account registered to "@Unknown69", phone number 717-708-1660, Telegram User ID 7467415159.

(2) One Apple iPhone 16 Pro Max cellular telephone, IMEI: 354276357504982, which is in the custody of the FBI located at the FBI Allentown RA, 504 West Hamilton Street, Suite 2401, Allentown, Pennsylvania 18101.

ATTACHMENT B

Items to be seized

Any and all evidence and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), that is, the receipt, distribution, possession, and access with intent to view child pornography, including:

1. All files, documents, communications, images, videos, logs, and contacts associated with the Telegram account @Unknown 69 related to visual depictions of minors engaging in sexually explicit conduct, child pornography, or child erotica;

2. Records identifying the users of the account described in Attachment A;

3. Records of names, phone contacts, phone numbers, phone call lists, incoming calls, outgoing calls, missed calls;

4. Messages, including chat messages, secret chats messages, and group messages or recorded voice messages, which may reflect communications with co-conspirators and/or victims, along with any evidence that would tend to show the true identities of the persons committing these offenses or the identifiers of the persons depicted in the images, videos, or other files.

5. GPS location information, maps, saved points, and any other information identifying or describing the location of the user of the device described in Attachment A.

6. Evidence of who used, owned, or controlled the account described in Attachment A at the time the things described in this warrant were created, edited or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, user profiles, messages and message logs, photographs, and correspondence.

7. Evidence of the time the account described in Attachment A was used;

8. Passwords, encrypted keys, and other access devices that may be necessary to access the account described in Attachment A;

9. Documentation and manuals that may be necessary to access the account described in Attachment A or to conduct a forensic examination of the account;

10. Contextual information necessary to understand the evidence described in this attachment.