AO 91 (Rev. 11/11) Criminal Complaint AUSA Sushma Raju (312) 353-5329

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

v.

KHAMRYN ZYIEL JOHNSON

CASE NUMBER: 25 CR 328
UNDER SEAL

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. From on or about May 16, 2025 to on or about May 26, 2025, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant(s) violated:

Code Section	*Offense Description*
Title 18, United States Code, Sections 2251(a) and 2252A	Production and possession of child pornography

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

MACKENZIE SKAY
Special Agent, Homeland Security Investigations (HSI)

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

Date: June 23, 2025

Judge's signature

City and state: Chicago, Illinois

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

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Mackenzie Skay, being duly sworn, state as follows:

1. I am a Special Agent with the Homeland Security Investigations (HSI). I have been employed with HSI since approximately September 2020 and have been a Special Agent with HSI since September 2022.

2. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography offenses, including violations pertaining to the illegal distribution, receipt, possession, advertisement, and production of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A, as well as violations pertaining to the enticement, transportation, and travel in interstate commerce to engage in sexual activity with minors, in violation of Title 18, United States Code, Sections 2422 and 2423. I have received training in the area of child pornography and child exploitation investigations. I have participated in investigations that have led to the issuance of search warrants, including for cell phones and computers, involving child pornography and child exploitation offenses.

3. This affidavit is made in support of:

a. a criminal complaint alleging that KHAMRYN ZYIEL JOHNSON has committed the offenses of production and possession of child pornography, in

violation of Title 18, United States Code, Sections 2251(a) and 2252A (the "**Subject Offenses**"); and

b. an application for a warrant to search the single family home located at 308 Alyssa St, Plano, Illinois, described further in Attachment A (the "**Subject Premises**"), for evidence, instrumentalities, and contraband described further in Attachment B, concerning the "**Subject Offenses**."

4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant and criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence, instrumentalities, and contraband of violations of Title 18, United States Code, Sections 2251(a) and 2252A, are located at 308 Alyssa St, Plano, Illinois.

I. SUMMARY OF PROBABLE CAUSE

5. Law enforcement authorities in the United Kingdom ("UK") contacted the Department of Homeland Security regarding the death of Victim 1, a 13-year-old girl residing in the UK, who had been in contact with KHAMRYN ZYIEL JOHNSON through the internet-based chat application WhatsApp shortly before her death. UK authorities reviewed WhatsApp chats on Victim 1's phone that showed she had been producing and sending child sexual abuse material ("CSAM") to JOHNSON at his

request. Among other things, JOHNSON urged Victim 1 to create videos where she asphyxiated herself with an Apple Watch charger cord while she masturbated. Victim 1 complied with that specific request on at least one occasion on or about May 21, 2025. JOHNSON also sent to Victim 1 videos and images, some of which showed his face, depicting himself masturbating. On or about May 22, 2025, Victim 1's mother discovered Victim 1 nude, unresponsive, and hanging from a bed post by an Apple Watch charger cord around her neck. Data from Victim 1's phone indicated that she had been on a WhatsApp video call with JOHNSON shortly before Victim 1's mother found her unconscious. Victim 1 died several days later. Historical information provided to law enforcement by online social media platforms suggests that JOHNSON has possessed child pornography as far back as 2021.

6. Based on images and videos sent to Victim 1 showing JOHNSON's face and other identifying features included in the WhatsApp messages, such as the area around JOHNSON's home, his date of birth, the use of the nickname "Neato"—a moniker used by JOHNSON in other online contexts, and his vehicle, there is probable cause to believe that JOHNSON is the user of the WhatsApp account that enticed and persuaded Victim 1 to create sexually explicit material.

7. Additionally, based on images sent by JOHNSON to Victim 1, law enforcement encounters in which JOHNSON identified his address, and surveillance by HSI agents, there is probable cause to believe that JOHNSON resides in the

Subject Premises, and that a search of the **Subject Premises** would yield evidence, instrumentalities, and contraband related to the **Subject Offenses**.

II. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

A. Death of Victim 1

8. On or about June 10, 2025, HSI Chicago began reviewing law enforcement materials provided by a UK Detective Constable in the Child Abuse Investigation Team in the Gloucestershire Police. According to the UK records, Gloucestershire Ambulance responded to an emergency call from Victim 1's mother, who had found Victim 1 nude and in cardiac arrest. Victim 1's mother told UK police that Victim 1 had been left home alone at approximately 14:08 (BST).[1] Victim 1's mother told Victim 1 that she would return home in approximately 20 minutes. Victim 1's mother returned home at 14:32. At approximately 14:58, Victim 1's mother called for an ambulance after she discovered Victim 1 hanging unresponsive by an Apple Watch charger tied to her bedframe. Victim 1 was taken to a hospital and found to have suffered a catastrophic hypoxic injury to her spinal cord. Victim 1 was removed from life support after five days and died on or about May 26, 2025.

B. Data From Victim 1's Phone

9. According to UK law enforcement reports, Victim 1's phone was seized on or about May 23, 2025 from Victim 1's bedroom. Following a forensic examination, UK Detective Constable Lisa Hawthorne discovered sexual conversations on

[1] All dates and times in this paragraph reflect the dates and times in British Summer Time ("BST") on a 24-hour clock. BST is six hours ahead of Central Standard Time.

WhatsApp[2] between Victim 1 and an individual with the WhatsApp username "Rag€" (the "JOHNSON WhatsApp Account"), from between on or about May 17, 2025, and on or about May 22, 2025.[3] The JOHNSON WhatsApp Account was associated with the phone number +1 (630) XXX-9013. HSI Chicago reviewed the WhatsApp conversation between Victim 1 and the JOHNSON WhatsApp Account and identified the following messages of note.[4]

10. On or about May 17, 2025, at approximately 16:38, the JOHNSON WhatsApp Account sent three videos to Victim 1. The first video depicts a black adult male masturbating with what appears to be a black cylindrical object intended to imitate a vagina. At the end of the video, a portion of the male's face is visible and shows he has a beard and heart-shaped glasses. The second video is similar to the first video. Several seconds into the second video, a portion of the same male's face is visible again. The third video depicts an adult black male using the same black

[2] Based on my experience and training, WhatsApp is a secure messaging platform that allows users to exchange end-to-end encrypted messages. According to WhatsApp, no one other than the WhatsApp users who are engaged in a chat, including WhatsApp itself, has access to read the messages. However, WhatsApp messages may be preserved on a user's phone, as they were in the case of Victim 1's phone.

[3] All dates and times reflect the dates and times as they appeared on Victim 1's phone at the time of the forensic extraction and are thus provided in BST on a 24-hour clock.

[4] The WhatsApp communications described herein do not include all statements made or topics covered during the WhatsApp conversation between Victim 1 and the JOHNSON WhatsApp Account. In some instances, I have included my interpretations of the quoted language in brackets. My interpretations are based on the contents and context of the conversations, my training and experience as a Special Agent, my knowledge of this investigation as whole, and information provided by other law enforcement officers assigned to this investigation.

cylindrical object. The male appears to be on a bed that has a yellow sheet, a white blanket, and a patterned purple blanket. A white dresser is also visible in the video.

11. On or about May 17, 2025, the following communications also occurred between the JOHNSON WhatsApp Account and Victim 1:

> **Victim 1 (19:09):** How would u like me to torture myself while alone while ur out
>
> **JOHNSON WhatsApp Account (19:13):** Hmm by sending videos of you choking yourself, spitting ok [on] yourself telling me you're my little 13 year old whore and videos of you smacking your ass and pussy with a charger cord
>
> And when I say choke I mean I wanna see ur face change colors
>
> . . . .
>
> **Victim 1 (21:51)**: Do u want me to torture myself while [you are] sleeping
>
> But I'm [in] 7 mins my phone turns off so I won't text back
>
> **JOHNSON WhatsApp Account (21:55)**: Yes please
>
> **Victim 1 (21:56)**: What do I do
>
> **JOHNSON WhatsApp Account (21:56)**: And try to make videos if you can even if u can't send them p
>
> **Victim 1 (21:56)**: Ok….What do I do
>
> **JOHNSON WhatsApp Account (21:56):** Choke yourself until your face changes color
>
> Play with your pussy until your about to cum but stop EVERYTIME
>
> **JOHNSON WhatsApp Account (21:57)**: And I want you to pinch and twist your nipples and the skin around it until you get bruises
>
> And record EVERYTHING and I love you moreee

12. On or about May 18, 2025, the JOHNSON WhatsApp Account told Victim 1 to "resend those videos and pictures." At approximately 12:13, Victim 1 sent the JOHNSON WhatsApp Account five videos depicting herself. One video with file name "3a1253ee-6127-4ffd-aca0-6eb5b9359a1a.mov.mp4" is approximately 14 seconds in length. Victim 1's face is visible, and she appears to be at least partially nude and pinching and twisting her nipples as instructed by the JOHNSON WhatsApp Account. Victim 1 appears to be wincing in pain throughout the video and saying the words "ow" and "daddy." Another video with file name 665b7fda-42c6-4a4d-9605-331a222af099.mp4 is approximately one minute and 37 seconds in length and depicts a female masturbating with her fingers and with what appears to be an electric toothbrush. The toothbrush is being inserted inside her vagina.[5] At approximately 12:13, the JOHNSON WhatsApp Account responded to Victim 1, "Oh I'm stroking my morning wood rn baby[.]"

13. On or about May 20, 2025, at approximately 18:15, the JOHNSON WhatsApp Account wrote to Victim 1 via WhatsApp, "Ok I still want to play with your right little pussy…Tight…And ooo look for something thicker or longer then your toothbrush baby that you can use[.]" At approximately 18:27, Victim 1 and the JOHNSON WhatsApp Account had a video call that lasted approximately nine minutes and 22 seconds. At approximately 18:37, Victim 1 and the JOHNSON

[5] According to Victim 1's WhatsApp records, a notation under this video indicated that the message had been "unsent." At the present time, law enforcement does not know whether the video was received or opened by the user of the JOHNSON WhatsApp Account.

WhatsApp Account had another video call that lasted approximately 37 minutes and 31 seconds. At approximately 19:30, Victim 1 and the JOHNSON WhatsApp Account had another video call that lasted approximately 14 minutes and 11 seconds. At approximately 20:40, Victim 1 and the JOHNSON WhatsApp Account had a video call that lasted approximately 53 minutes and 23 seconds.

14. On or about May 21, 2025, the JOHNSON WhatsApp Account and Victim 1 had the following communications via WhatsApp.

JOHNSON WhatsApp Account (16:54): Who's home

Victim 1 (16:54): No one

JOHNSON WhatsApp Account (16:55): Good I want you to strip completely
Then start by rubbing your clit for 2 minutes straight
Then in the next video I want you to torture yourself

Victim 1 (16:55): How

JOHNSON WhatsApp Account (16:58): I'll tell you after the first video is made

Victim 1 (17:07): *Victim 1 sends a video with file name c690bfef-77dc-4d71-858a-5ed2073f4366.mp4 which is approximately two minutes and 18 seconds in length. In the video, Victim 1 is standing in front of the camera with her face and body down to her upper thigh visible. She is masturbating while facing the camera. At the end of the video, she says "I miss you."*

JOHNSON WhatsApp Account (17:09): Excellent noww you must sit on the bottom bunk and hang yourself like I taught you, then start pounding your pussy at the same time until you cum once, after you cum, you are to undo the cord and start whipping your pussy exactly 25 times

Victim 1 (17:09): Yes master

JOHNSON WhatsApp Account (**17:09)**: This time
You MUST
Say
And talk about how young you are
And how wrong it is that your a slut and under my complete control
That you too young and everything like that

JOHNSON WhatsApp Account (17:10): Id love to rape my little princess hehe

Victim 1 (17:11): Should I also right [write] ur name on me

JOHNSON WhatsApp Account (17:12): Yes big bold letters on your chest and tummy and thighs
Saying
Neato's slut
Neato's whore
And I want u to write cum in me on ur tummy with arrow pointing to ur pussy
Show me after u wrote all of this

Victim 1 (17:13): Should I also right [write] neato's property

JOHNSON WhatsApp Account (17:14): Yes ofc

15. On or about May 21, 2025, at approximately 17:22, Victim 1 sent three videos of herself to the JOHNSON WhatsApp Account. One video with file name c7e255b3-9f0b-4b10-8b8a-2ae5d5b408e1.mp4 shows Victim 1 with writing visible on her in black ink which reads "neato's property" across her chest and on her breasts. Writing on her stomach reads "cum in me" with an arrow leading to her vagina. One inner thigh reads "neatos whore[,]" and the other inner thigh reads "neatos slut." Victim 1's vagina is visible in the video. Another video with file name 461c6e98-3e88-4e25-9c43-8ef419b1adef.mp4 depicts Victim 1 laying on what appears to be the

bottom bunk of a bunk bed. Her back is against one of the bed posts, and she is completely nude with her face visible. Some of the writing from the first video is visible on her body, and Victim 1 is masturbating with an unidentified object. Victim 1 holds what appears to be an Apple Watch charging cord wrapped around her neck and through the bottom of the bunk bed post, and she periodically tights the cord with her hand. Victim 1's face turns red multiple times throughout the video as she pulls the cord. During the video, she says, "daddy I just came" and adds, "If you were to call me, you'd probably say keep going pull harder….and you'd say take it off and whip myself like twenty something times." In a third video with file name fe7acc76-1515-49e9-9929-f2d998342e57.mp4, Victim 1 is in the same position as in the second video described above. She hits herself on the vagina with the Apple Watch charging cord. She appears to be wincing in pain while she counts out the number of times she hits herself with the cord. The video stops once she hits herself 25 times.

16. On or about May 21, 2025, at approximately 17:38, the JOHNSON WhatsApp Account messaged Victim 1, "Cum two times only then after that I want you to keep riding and start pinching your nipple, twisting it while hitting your temple with your other hand[.]" The JOHNSON WhatsApp Account sent further messages between approximately 17:39 and 17:40, saying "After you cum two you must do the second part for 5 minutes as well taking a break after every 5 palms to the temple…MAKE SURE TO REPEAT THOSE 3 SENTENCES. I AM WORTHLESS I AM USELESS I AM DADDYS FUCK TOY[.]"

17. On or about May 21, 2025, at approximately 20:25, Victim 1 and the JOHNSON WhatsApp Account had a WhatsApp video call lasting approximately 27 minutes and 18 seconds. At approximately 20:43, while the WhatsApp video call appeared to be ongoing, the JOHNSON WhatsApp Account sent a screenshot to Victim 1. The screenshot appears to show results from a Google search. The screenshot also reflects that Victim 1 and an adult black male are engaged in a video call at the time the screenshot was taken. Specifically, the bottom right of the screenshot depicts an image of a female's chest and a smaller image of the face of an adult black male with his hand over the screen as if attempting to take a screenshot using the side buttons on a phone. A portion of the male's face is visible, showing that he wears a mustache and glasses. Based on my experience and training, this screenshot appears to have been taken by the user of the JOHNSON WhatsApp Account, an adult black male with a mustache and heart-shaped glasses, while he was video calling Victim 1. The appearance of this black male is consistent the male who appears in the videos sent to Victim 1 on or about May 17, 2025 (*see* paragraph 10, above).

18. On or about May 22, 2025, at approximately 8:06, the JOHNSON WhatsApp Account sent Victim 1 an image via WhatsApp. The image shows an adult black male wearing heart-shaped glasses with facial hair and blue beads on a dreadlock.

19. On or about May 22, 2025, at approximately 13:56, the JOHNSON WhatsApp Account and Victim 1 exchanged the following messages:

JOHNSON WhatsApp Account (13:56): Wyd

Victim 1 (13:57): Lying in bed

JOHNSON WhatsApp Account (13:57): Who's all home baby
Just you lol [?]

Victim 1 (13:57): Only my mum

20. On or about May 22, 2025, at approximately 13:58, the JOHNSON WhatsApp Account and Victim 1 began a video call on WhatsApp that lasted until approximately 14:27. At approximately 14:28, 14:29, 14:32, and 15:07, the JOHNSON WhatsApp Account called Victim 1 on WhatsApp, but the calls went unanswered by Victim 1.

21. According to data on Victim 1's phone, the phone last moved at approximately 14:23, four minutes before the video call with the JOHNSON WhatsApp Account ended. According to UK law enforcement records, Victim 1's mother discovered her nude, unresponsive, and hanging from an Apple Watch charging cord attached to her bed shortly before 14:58 (the time that Victim 1's mother called for an ambulance). Based on a review of the UK law enforcement records, Victim 1 was found by her mother in a pose similar to the one seen in the videos that Victim 1 sent to the JOHNSON WhatsApp Account on or about the previous day, May 21, 2025. The foregoing WhatsApp data, the movement data, and

the time of Victim 1's discovery are consistent with Victim 1 asphyxiating while on a video call with the user of the JOHNSON WhatsApp Account.

C. IDENTIFICATION OF JOHNSON AS THE USER OF THE JOHNSON WHATSAPP ACCOUNT

22. On or about June 10, 2025, HSI served an administrative summons to T-Mobile for the phone number 630-XXX-9013, the number associated with the JOHNSON WhatsApp Account,[6] requesting subscriber data. T-Mobile records identified the subscriber as Individual A at a billing address in Oswego, Illinois.[7] According to open-source and law enforcement database records, Individual A, whose last name is Johnson, appears to be a close female relative to JOHNSON.

23. The phone number 630-XXX-9013 and the name "Neato" are associated with Internet-based money transfer applications used by JOHNSON. For instance, according to CashApp records, a CashApp account associated with the verified name "KHAMRYN JOHNSON," a June 3, 1998 date of birth, and the **Subject Premises** bore the display name "Young Neato" and "YNeato" between in and around November 2021 through in and around September 2023. According to Illinois Secretary of State records, JOHNSON's driver's license lists his date of birth as June 3, 1998. Additionally, according to PayPal records, an account registered to "KHAMRYN

[6] On or about June 18, 2025, HSI served WhatsApp with a subpoena for subscriber information associated with the JOHNSON WhatsApp Account. WhatsApp records confirmed that this phone number is associated with an active WhatsApp Account.

[7] On or about June 16, 2025, HSI served T-Mobile with a grand jury subpoena for the same information and is awaiting a response.

JOHNSON" lists (630) XXX-9013 as the phone number, identifies the **Subject Premises** as the user's primary address, and lists the email as khamgohammy@gmail.com.

24. Through open-source searches, HSI also identified a Facebook account that appears to be used by JOHNSON (the "JOHNSON Facebook Account").[8] The profile name on the account is "Zyiel Johnson," which reflects JOHNSON's middle name as reflected in law enforcement database records. The Illinois state driver's license issued to KHAMRYN JOHNSON lists "Z" as the middle initial. The vanity name or username on the Facebook account, which appears in the URL to the profile, is "YoungNeato."

25. Pictures posted on the JOHNSON Facebook Account depict an individual consistent in appearance with JOHNSON's Illinois driver's license photograph. Image 1 below reflects a screenshot of the profile and banner photo posted on the JOHNSON Facebook Account. These images are consistent with the appearance of the black male wearing heart-shaped glasses who appears in the videos sent to Victim 1 by the JOHNSON WhatsApp Account on or about May 17, 2025.[9]

[8] On or about June 18, 2025, HSI served Facebook with a grand jury subpoena for subscriber information for this Facebook and is awaiting a response.

[9] As noted above, the male's full face is not visible in the images sent to Victim 1.

Image 1

26. Additionally, on or about May 1, 2025, the JOHNSON Facebook Account posted a photo of JOHNSON, shown below in Image 3, that appears to be visually consistent with the image of JOHNSON that the JOHNSON WhatsApp Account sent to Victim 1 on or about May 22, 2025, shown below in Image 4.

Image 3

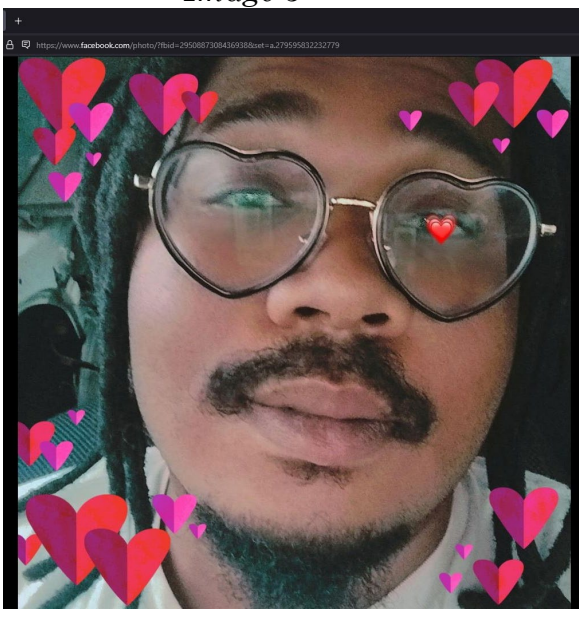
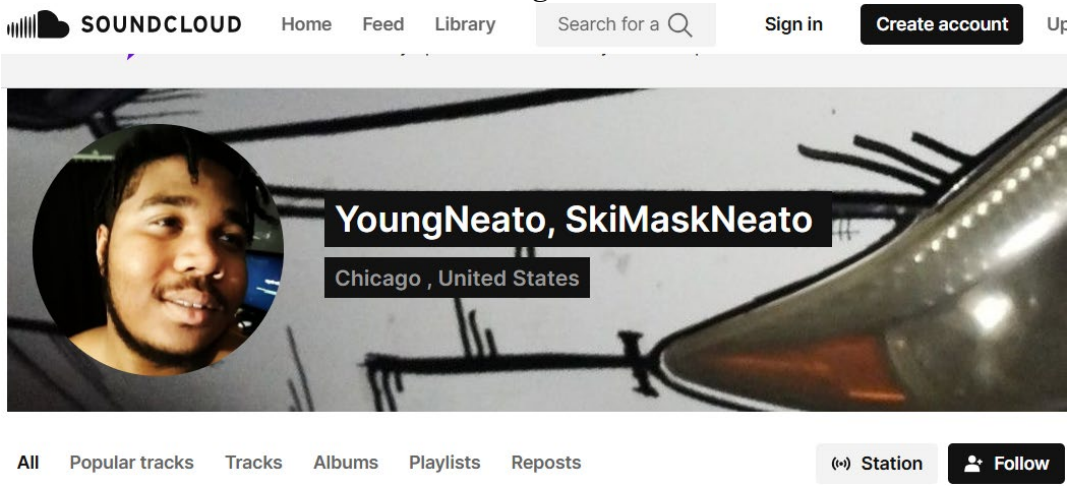


Image 4

27. HSI conducted an open-source search of SoundCloud, a website that allows users to create accounts to upload, promote, and share music, and located a user with the account name "YoungNeato." The account contains a profile picture, shown below in Image 5, which is consistent in appearance with JOHNSON and lists the user's location as Chicago.

Image 5



28. According to a UK law enforcement report, on May 29, 2025, a Detective Constable revisited the home of Victim 1 and discovered that a wall of Victim 1's bedroom contained a list of birthdays, which included the handwritten notation "Rag€" followed by the date "3 June." As noted above, "Rag€" is the display name associated with the JOHNSON WhatsApp Account, and June 3 is JOHNSON's birthdate.

29. On or about May 17, 2024, the JOHNSON WhatsApp Account sent Victim 1 a photo, shown below as Image 6, depicting a steering wheel and dashboard of a vehicle. The steering wheel appears to read "SCION." Based on open-source

records, this is consistent with the steering wheel and dashboard that appears in models of the Toyota Scion.

Image 6

30. JOHNSON has been identified as the driver of a Toyota Scion by law enforcement on multiple occasions. According to a report from the Kendall County Sheriff's Office, JOHNSON was the subject of a traffic stop on or about September 30, 2022. During this encounter, JOHNSON was the operator and sole occupant of a white Scion TC bearing Illinois license plate BY27755. According to Illinois Secretary of State records, this vehicle is registered to Individual B, who shares the last name Johnson and appears to be a close female relative of KHAMRYN JOHNSON. The vehicle is registered to the **Subject Premises**. According to records provided by the Plano Police Department ("PPD"), on or about November 1, 2023, a PPD Officer

conducted a traffic stop on a white Scion TC bearing Illinois license plate BY27755 which was being operated by JOHNSON.

31. At the time of the above-described WhatsApp communications between Victim 1 and JOHNSON, Victim 1 resided in United Kingdom and, based on pictures and messages sent to Victim 1, JOHNSON appears to have been in the United States. Accordingly, JOHNSON's messages enticing and persuading Victim 1 to produce sexually explicit materials, and the materials themselves, moved in interstate or foreign commerce.

D. JOHNSON'S ASSOCIATION WITH THE SUBJECT PREMISES

32. According to PPD records, on or about January 3, 2024, PPD officers responded to the **Subject Premises** in response to a call from JOHNSON regarding damage to his vehicle. During the encounter, JOHNSON identified the **Subject Premises** as his residence.

33. A Google street view image of the **Subject Premises** dated May 2024 shows a white Toyota Scion parked in the driveway of the residence.

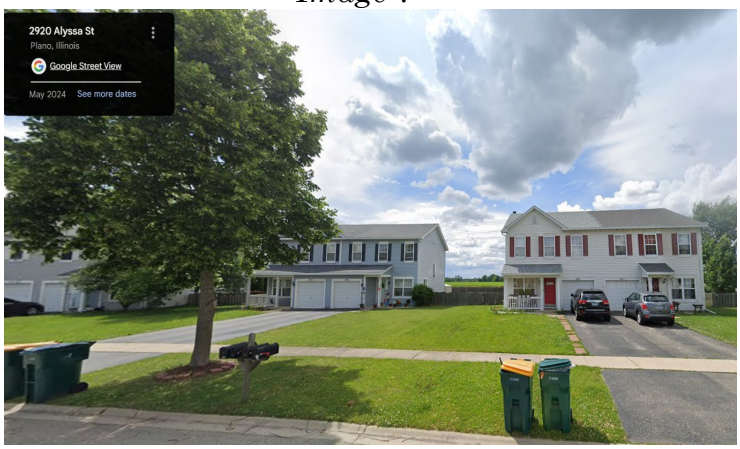
34. DHS database records reveal that JOHNSON has received multiple international packages addressed to him at the **Subject Premises**. The most recent of these packages was released by Customs and Border Protection to the **Subject Premises** on or about April 2, 2025.

35. As noted above, Image 6 (shown again below) was sent by JOHNSON through the JOHNSON WhatsApp Account to Victim 1 on or about May 17, 2025. In the background of Image 6, two houses and a tree are visible. According to a Google

street view, shown below in Image 7, these homes and tree are consistent with the homes directly across the street from the **Subject Premises**. This is consistent with JOHNSON having taken Image 6 while seated in the Scion while it was backed into the driveway of the **Subject Premises**.

Image 6

Image 7



36. On or about June 18, 2025, HSI officers observed a white Toyota Scion TC bearing Illinois license plate BY27755 parked in the driveway of the **Subject Premises**. The vehicle was backed into the driveway, facing the opposite side of the street. At approximately 12:17 p.m., a HSI officer observed a black male matching the description of JOHNSON exit the **Subject Premises** and enter the driver's seat of the white Toyota Scion TC. The black male was observed wearing a black sweatshirt, black pants, glasses, and had black braids. A white female was observed

entering the passenger seat of the vehicle. The HSI officer observed the vehicle exit the driveway of the **Subject Premises**.

E. JOHNSON'S HISTORICAL POSSESSION OF CHILD PORNOGRAPHY

37. The National Center for Missing and Exploited Children's Cybertipline[10] has provided to law enforcement the following historical information about online accounts bearing identifiers consistent with JOHNSON that appeared to have engaged in the possession of child pornography.

38. A CyberTipline Report dated on or about January 11, 2023 from the internet-based media-sharing application Snapchat identified activity from an account associated with the username "youngneato," an email address of "youngneatoofficial@gmail.com," (consistent with JOHNSON's use of the nickname "Neato"), and a date of birth of June 3, 1998 (which is JOHNSON's date of birth). According to the report, the IP address associated with the activity resolved to Plano, Illinois (where the **Subject Premises** is located). On or about February 16, 2023, the PPD obtained a search warrant to view the contents of the CyberTip. According to a report completed by a PPD Investigator who reviewed the contents, the CyberTip was associated with two uploaded video files that appeared to be duplicates. The PPD investigator described the video to show a prepubescent female unclothed from the waist down being vaginally penetrated by a penis.

[10] The Cybertipline is a national centralized reporting system for public and electronic service providers to report suspected online enticement of children for sexual acts.

39. Another CyberTipline Report dated on or about September 5, 2021 from Dropbox, an internet-based file hosting service that provides cloud storage, identified activity from an account associated with the email address "khammyjay@gmail.com" with username "Kkjj Kkjj." According to the report, Dropbox determined at least three files associated with the account to contain prepubescent minors involved in a sex act. According to reports from the Yorkville, Illinois Police Department, on or about October 27, 2021, the Yorkville Police Department ("YPD") obtained a search warrant to review the files associated with this Cybertip and the identified Dropbox account. The YPD detective reported finding an additional 24 video files that appeared to be CSAM.

40. According to YPD reports, a YPD detective issued an administrative subpoena for the Google account associated "khammyjay@gmail.com." According to the YPD reports, the Google account records for the email "khammyjay@gmail.com" list the name on the account as KHAMRYN JOHNSON. The Google Pay information for the account lists JOHNSON's name and the address of the **Subject Premises**. An additional name listed in the Google Pay activity is Individual B. In addition, there were multiple IP addresses listed in the Google records for the khammyjay@gmail.com account that matched IP addresses listed in the CyberTip from Dropbox. Based on my experience and training, this indicates that the Google account and Dropbox account were accessed from the same IP address.

41. Based on my training and experience, I know that individuals who possess child pornography typically store media on multiple devices, which are in turn, commonly maintained at their residences.

III. BACKGROUND INFORMATION CONCERNING CHILD PORNOGRAPHY

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

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

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

45. The computer's capability to store images in digital form makes it a common repository for child pornography. Internal and external computer hard drives typically store vast amounts of data, and hard drives with the capacity of 500 or more gigabytes – which can store tens of thousands of images at very high resolution – are not uncommon. Other electronic storage media, such as thumb drives and memory sticks, can store hundreds of images and dozens of videos. Likewise,

optical storage media, which includes CD-ROMs and DVDs, and electromagnetic storage media also can hold hundreds of images and multiple videos. Such electronic, optical, and electromagnetic storage media are very commonly used by those who collect child pornography to store images and videos depicting children engaged in sexually explicit activity. Agents who execute child pornography search warrants often find electronic, optical, and/or electromagnetic storage media containing child pornography in the same location as or near the computer that was used to obtain, access, and/or store child pornography.

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

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

b. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, Internet Relay Chat, newsgroups, instant messaging, and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute child pornography often collect, read, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in address books or notebooks, on computer storage devices, or merely on scraps of paper.

d. The majority of individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. These individuals almost always maintain their collections in the privacy and security of their homes or other secure location. These individuals may keep their collections in locked containers including

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

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

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

IV. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

47. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most

or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

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

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

50. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock electronic devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a

numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

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

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices

produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

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

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For

example, Apple devices cannot be unlocked using Touch ID when (1) more than a certain number of hours have elapsed since the device was last unlocked or (2) when, within a certain number of hours, the device has not been unlocked using a fingerprint and the passcode or password has not been entered. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of KHAMRYN ZYIEL JOHNSON, if found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device;[11] (2) hold the device in front of the face of KHAMRYN ZYIEL JOHNSON and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

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

V. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

51. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

52. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures if those procedures are designed to minimize the review of information not within the list of items to be seized as set forth in Attachment B:

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

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;

c. surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

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

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment B.

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

VI. CONCLUSION

54. Based on the above information, I respectfully submit that there is probable cause to believe that production and possession of child pornography offenses, in violation of Title 18, United States Code, Sections 2251(a) and 2252A, have been committed by JOHNSON, and that evidence, instrumentalities, and contraband relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Premises**, as further described in Attachment A. I therefore respectfully request that this Court issue a search warrant for the single family home located at 308 Alyssa St, Plano, Illinois, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.

Mackenzie Skay
Special Agent
Homeland Security Investigations

Sworn to and affirmed by telephone 23rd day of June, 2025

Honorable MARIA VALDEZ
United States Magistrate Judge