

JMH:SP
F. #2022R00307

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
-----X

UNITED STATES OF AMERICA

- against -

Docket No. 23-CR-24 (MKB)

SHAKEEM RANKIN,

Defendant.

-----X

MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S
MOTION TO SUPPRESS

BREON PEACE
UNITED STATES ATTORNEY
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

Stephanie Pak
Assistant U.S. Attorney
(Of Counsel)

TABLE OF CONTENTS

PRELIMINARY STATEMENT.....1

STATEMENT OF FACTS.....1-9

THE MOTION.....9-10

ARGUMENT.....10

I. THE EVIDENCE WAS OBTAINED PURSUANT TO A LAWFULLY EXECUTED SEARCH WARRANT 10

 A. Applicable Law 10

 B. Discussion 11

II. THE DEFENDANT’S STATEMENTS TO LAW ENFORCEMENT SHOULD NOT BE SUPPRESSED BECAUSE THE DEFENDANT WAS NOT IN CUSTODY 14

 A. Applicable Law 14

 B. Discussion 16

III. A HEARING—IF ANY IS REQUIRED—SHOULD BE LIMITED TO THE TIME THE SEARCH WARRANT WAS EXECUTED 19

 A. Applicable Law 19

 B. Discussion 20

CONCLUSION.....21

TABLE OF AUTHORITIES

CASES

Berkemer v. McCarty,
468 U.S. 420 (1984)..... 15

Cruz v. Miller,
255 F.3d 77 (2d Cir. 2001)..... 15

In re Terrorist Bombings of U.S. Embassies in E. Afr.,
552 F.3d 157 (2d Cir. 2008) 19

Florida v. Bostick,
501 U.S. 429 (1991)..... 16

Georgison v. Donelli,
588 F.3d 145 (2d Cir. 2009)..... 15

Kentucky v. King,
563 U.S. 452 (2011)..... 10

Michigan v. Summers,
452 U.S. 692 (1981)..... 11, 12

Miranda v. Arizona,
384 U.S. 436 (1966)..... 9, 14, 15

Muehler v. Mena,
544 U.S. 93 (2005)..... 12

Payton v. New York,
445 U.S. 573 (1980)..... 10

Pennsylvania v. Mimms,
434 U.S. 106 (1977)..... 10, 11

Stansbury v. California,
511 U.S. 318 (1994)..... 15, 16

Tennessee v. Garner,
471 U.S. 1, (1985)..... 10

Texas v. Cobb,
532 U.S. 162 (2001)..... 17

United States v. Badmus,
325 F.3d 133 (2d Cir. 2003)..... 16, 17

United States v. Chandler,
164 F. Supp. 3d 368 (E.D.N.Y. 2016) 20

United States v. Familetti,
878 F.3d 53 (2d Cir. 2017)..... 16

United States v. Faux,
828 F.3d 130 (2d Cir. 2016)..... 16, 17

United States v. FNU LNU,
653 F.3d 144 (2d Cir. 2011)..... 15, 16

United States v. Galloway,
316 F.3d 624 (6th Cir. 2003) 15, 18

United States v. Ganais,
824 F.3d 199 (2d Cir. 2016)..... 11

United States v. Gillette,
383 F.2d 843 (2d Cir. 1967)..... 19

United States v. Knights,
534 U.S. 112, (2001)..... 11

United States v. Mathurin,
148 F.3d 68 (2d Cir. 1998)..... 20

United States v. Messalas,
No. 17-CR-339 (RRM), 2020 WL 4003604 (E.D.N.Y. July 14, 2020) 11, 12, 14

United States v. Miller,
430 F.3d 93 (2d Cir. 2005)..... 11, 15

United States v. Mitchell,
966 F.2d 92 (2d Cir. 1992) 16, 17

United States v. Moore,
670 F.3d 22 (2d Cir. 2012)..... 17

United States v. Moya,
74 F.3d 1117 (11th Cir. 1996) 16

United States v. Newton,
369 F.3d 659 (2d Cir. 2004)..... 16

United States v. Pena,
961 F.2d 333 (2d Cir. 1992)..... 21

United States v. Schaffer,
No. 12-CR-430 (ARR), 2014 WL 1515799 (E.D.N.Y. Apr. 18, 2014)..... 16

United States v. Spencer,
No. 06-CR-413 (DLI), 2016 WL 6781225 (E.D.N.Y. Nov. 15, 2016) 2041€

United States v. Townsend,
No. 15-CR-653 (DLI), 2016 WL 3562055 (E.D.N.Y. June 23, 2016)..... 20

United States v. Yilmaz,
508 F. App'x 49 (2d Cir. 2013) 15

STATUTES

18 U.S.C. § 2252(a)(2)..... 1, 3, 8

RULES

Fed. R. Crim. P. 41(e)(2)(A)(ii)..... 11

PRELIMINARY STATEMENT

The government respectfully submits this memorandum in opposition to the defendant's motion to suppress ("the Motion"): (i) the evidence recovered from the search warrant executed at the defendant's residence on March 16, 2022 and (ii) the defendant's statements to law enforcement agents on March 16, 2022.¹ First, as to the evidence recovered from the search warrant, the Motion fails because the warrant was reasonably and properly executed between the hours of 6:00 a.m. to 10:00 p.m. as authorized on the face of the warrant. Second, as to the defendant's statements to law enforcement, the Motion fails because the defendant was not in custody at the time that he made his statements. There was no Sixth Amendment violation.

The Motion should be denied as to the suppression of the defendant's statements. As to the suppression of the evidence recovered from the search warrant executed at the defendant's residence, while the government does not believe a hearing is necessary, any such evidentiary hearing should be limited to the narrow question of the time of execution of the search warrant on March 16, 2022.

STATEMENT OF FACTS

The defendant is charged in a three-count indictment with receipt, possession, and distribution of child pornography, in violation of Title 18, United States Code, Sections 2252(a)(2), (a)(4)(B), b(1) and (b)(2) (receipt, possession, and distribution of child pornography). (ECF No. 1). In the event of an evidentiary hearing, the government expects to establish the following facts²:

In or about 2021, the Federal Bureau of Investigation (FBI) investigated an individual ("the Seller") living in St. Louis, Missouri for production and distribution of child

¹ The Motion does not challenge the quantum of probable cause in the search warrant application itself.

² Unless otherwise indicated, all statements set forth in this memorandum are provided in sum and substance and in part.

sexual abuse material (“CSAM”). The FBI learned from this investigation that the Seller had produced CSAM and advertised the CSAM on the internet, directing others interested in purchasing the CSAM to contact him on Kik Messenger (“Kik”), a mobile messaging application. The FBI additionally learned that the Seller negotiated prices of the CSAM with prospective buyers on Kik, directing them to transmit payment on Cash App, a mobile money transfer application. After receiving the payment, the Seller sent the buyers hyperlinks to CSAM using Mega, a cloud-based application that enables users to share files.

On or about May 4, 2021, law enforcement executed a search warrant at the Seller’s residence and recovered the Seller’s cellphones. Upon law enforcement’s review of the Kik messages on the Seller’s cellphones, law enforcement learned that on or about April 9, 2021, the Seller had sent messages to a Kik account later identified as the defendant’s. During the conversations, the Seller asked the defendant if the defendant wanted CSAM and the defendant responded affirmatively. Law enforcement learned that after one of these conversations, the defendant paid the Seller \$80 via Cash App and then received hyperlinks to Mega. Kik messages on the Seller’s cellphones showed that on April 25, 2021, the defendant sent the Seller \$80 again in exchange for hyperlinks on Mega for CSAM.

Subpoena returns from Kik for the account that communicated with the seller on April 9 and 25, 2021 revealed the Yahoo email address associated with the Kik account, which corresponded to a Verizon IP address registered to the defendant’s mother at the defendant’s residence. Subpoena returns from Yahoo also showed that the above-mentioned email address was associated with the defendant’s cellphone number. Records from Mega also showed an active account user with the defendant’s email address with usage corresponding to the same above-mentioned address, i.e., the defendant’s residence.

Based on the above information, the FBI obtained a search warrant issued by the Honorable James R. Cho, United States Magistrate Judge for the Eastern District of New York, on March 15, 2022 for the defendant's residence and person for evidence, instrumentalities, fruits or contraband of violations of Title 18, United States Code, Sections 2252 and 2252A to be executed on or before March 29, 2022 in the daytime 6:00 a.m. to 10:00 p.m. See Search Warrant and Attachments A and B attached hereto as Exhibit 1.

According to an FBI report documenting the search warrant execution, law enforcement entered the defendant's residence at approximately 6:10 a.m. on March 16, 2022. Law enforcement agents knocked on the door to the defendant's residence, announced themselves as law enforcement and stated that they had a search warrant. Photos that law enforcement took before entering the location and after entering the location are consistent with a time of entry at approximately 6:10 a.m. The following photo depicts the front door to the residence as it appeared at approximately 6:00 a.m.:³ In the photo, the surroundings are dark and not well-lit because the sun had not risen yet that day at 6:10 a.m.⁴

³ Although the metadata in this first photograph recorded the time as 5:16 a.m., the camera settings had not been adjusted for daylight savings time. The correct time of this photo is 6:16 a.m. This would be consistent with the search warrant execution being completed in approximately one hour so that the time of exit is at approximately 7:15 a.m., when the sun had risen, as depicted in the next photograph. See <https://www.timeanddate.com/sun/usa/new-york?month=3&year=2022>.

⁴ See <https://www.timeanddate.com/sun/usa/new-york?month=3&year=2022>.



A woman, later identified as the defendant's mother, opened the door. The metadata in the first photo that law enforcement took upon entering the residence, depicted below,⁵ also supports that the time of entry was at approximately 6:00 a.m.⁶

⁵ This photograph was cropped to avoid revealing the faces or identities of individuals other than the defendant. No other alterations were made.

⁶ The metadata in this photograph recorded the time of this photo as 5:17 a.m. However, as described in footnotes four through six, the actual time is 6:17 a.m. because the camera settings had not been adjusted for daylight savings time.



Law enforcement entered the residence and began to secure the location. The defendant emerged from one of the rooms in the residence and inquired as to what was happening. Law enforcement informed the defendant that they had a search warrant and asked him to momentarily hold his questions so that they could continue securing the location. Shortly thereafter, law enforcement spoke with the defendant in a recorded conversation, noting that it was now 6:16 on March 16, 2022, identified themselves again as law enforcement agents and showed the defendant a copy of the search warrant.⁷ The defendant was interviewed in a bedroom at his residence, seated on a bed. Two law enforcement agents sat in chairs across from the defendant, with another agent who came in intermittently to confirm if certain electronic devices recovered belonged to the defendant. The door to exit the bedroom was never obstructed to prevent the defendant from leaving. Law enforcement had the following conversation with the defendant:

Law enforcement agent: So, we do apologize for how we came in this morning. Again, we, this is how we have to do things. We have to secure everything first. Make sure everything's okay for everybody. And then we can explain to you guys what's going on. **Nobody's under arrest.** This is just a search warrant. Obviously, you can read as much as you'd like. You can also, you know, go through it with you. But we are just here on a search warrant. So,

⁷ This conversation was audio recorded by law enforcement in its entirety. There were no other conversations with the defendant apart from this recording.

your alarm, I think, on your phone went off a minute ago. **So, if there's anywhere you need to go, you're welcome to. You're free to.**

[...]

Law enforcement agent: Before we get too far, you understand, like, you know, do you have anywhere to be today?

The defendant: Work.

Law enforcement agent: This morning? Okay. **I just want to make sure that you understand that you can leave.** What time do you have to go to work? You're [nodding] your head. Do you understand?

The defendant: Um, I have to be at work at 8:30, but I usually get up around this time.

Law enforcement agent: **Are you cool with talking with us for a little bit?** We can sort this stuff out, or **do you need to get out of here?**

The defendant: I mean, I need to get to work at, by 8:30.

Law enforcement agent: Okay.

The defendant: So, I usually leave here like 7:00.

Law enforcement agent: All right. If we talk for a few minutes, **is that okay?**

The defendant: Yeah, I'd rather not, but –

Law enforcement agent: **Well, you don't have to.** I mean, we just wanna obviously go through this and obviously kind of let you know what we're doing here, what we're taking. We obviously have some questions.

The defendant: Wait you haven't told me what you're doing here yet, though. I don't understand.

Law enforcement agent: Well, that's what we're getting into, but I want to make sure that you're okay. You're – 'cause **you're not under arrest. I wanna make sure you understand that. Do you understand that?**

The defendant: Yeah. But what's the problem, though? I don't understand.⁸

(emphases added). See Motion Ex. C at 02:31-03:23. The defendant continued conversing with law enforcement, and law enforcement informed the defendant that they were aware that the defendant had purchased and received CSAM, and that they were investigating whether the defendant produced CSAM. The defendant initially denied purchasing CSAM but later stated, among other things, in a conversation that lasted approximately 52 minutes, that he had purchased CSAM once or twice from one person on Kik and that he had used Cash App for payment. The defendant also stated that he resold CSAM that he had received from Mega and Dropbox to recoup his own payments for purchasing CSAM.

As a result of the search warrant, law enforcement recovered: (i) one white and beige iPhone, (ii) two black Samsung cellphones, (iii) two black iPhones and (iv) one white and pink iPhone. Upon a search of the devices, law enforcement recovered numerous files of CSAM and child erotica images and videos.

In contrast to the photo of the front door taken prior to law enforcement's entry into the residence, the photo below shows the front door to the residence as it appeared at approximately 7:15 a.m. when the search warrant execution had been concluded and law enforcement was preparing to depart:⁹

⁸ The transcript provided in the Motion as Attachment C is a fair and accurate transcript of the recorded conversation between law enforcement and the defendant.

⁹ Although the metadata in this photograph recorded the time as 6:20 a.m., the camera settings had not been adjusted for daylight savings time. The correct time of this photo, depicting the daytime, is 7:20 a.m., which is consistent with the sunrise on March 16, 2022 having been recorded as 7:05 a.m. See <https://www.timeanddate.com/sun/usa/new-york?month=3&year=2022>.



In the above photograph, the surrounding areas of the outside of the premises are comparatively well-lit because the sun had risen. This is consistent with the timeline of the search warrant execution beginning at approximately 6:10 a.m. and ending at approximately 7:15 a.m., given that the sun rose that day at 7:05 a.m. See <https://www.timeanddate.com/sun/usa/new-york?month=3&year=2022>.

The defendant was not placed under arrest during or after the conclusion of the search, which lasted approximately one hour. On January 17, 2023, approximately seven months after the challenged search took place, a grand jury sitting in the Eastern District of New York returned a three-count indictment charging the defendant with receipt, possession, and distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2), (a)(4)(B), b(1) and (b)(2). (ECF No.

1). The defendant was arrested pursuant to a corresponding arrest warrant on January 23, 2023, arraigned before the Honorable James R. Cho that same day, and released on bond.

THE MOTION

The Motion argues that the evidence recovered from the search warrant execution must be suppressed as fruits of an improperly executed search warrant. The Motion also argues that the defendant's statements to law enforcement must be suppressed because the defendant was in custody and should have received Miranda warnings. As to the search warrant execution, the Motion alleges that law enforcement agents violated the terms of the search warrant by executing it at approximately 5:00 a.m., one hour earlier than the timeframe of 6:00 a.m. through 10:00 p.m. set forth on the warrant. In support of this argument, the Motion attached affidavits from the defendant and the defendant's mother, both of whom recall the time as approximately 5:00 a.m. when law enforcement entered the premises. Def. Aff. Ex. D ¶ 1, Ex. E ¶¶ 6-7. In particular, the affidavit from the defendant's mother stated that she believed the time to be approximately 5:00 a.m. because she had already been awake to begin tasks in her daily morning routine. Def. Aff. Ex. E ¶¶ 6-7.

As to the defendant's statements to law enforcement, the Motion alleges that the defendant was in custody and not free to leave because execution of the search warrant itself created a coercive atmosphere in which law enforcement confronted the defendant with incriminating evidence. The Motion alleges that although the defendant told law enforcement that he "would rather not talk", law enforcement agents ignored that request and suggested that they already knew the answers to the questions they posed to the defendant. The defendant's affidavit also states that law enforcement did not read the defendant his rights and began questioning him. Def. Aff. Ex. D ¶ 4. The defendant's affidavit also stated that one law enforcement agent was

sitting on a chair in his room, and another was standing by his door, so the defendant felt that he was not free to leave. Def. Aff. Ex. D ¶¶ 4-5.

ARGUMENT

I. THE EVIDENCE WAS OBTAINED PURSUANT TO A LAWFULLY EXECUTED SEARCH WARRANT

The evidence that law enforcement obtained from execution of the search warrant should not be suppressed. Law enforcement executed the search warrant according to its parameters in a reasonable manner during the timeframe authorized by the magistrate court. Law enforcement agents used proportionate tactics to minimize the intrusion of privacy for the occupants of the residence, while balancing safety concerns in entering and securing the location.

A. Applicable Law

The Fourth Amendment requires that all searches and seizures be reasonable and that a warrant must be supported by probable cause with the scope of the permissible search to be laid out with particularity. Kentucky v. King, 563 U.S. 452, 459 (2011) (citing Payton v. New York, 445 U.S. 573, 584 (1980)). See also Tennessee v. Garner, 471 U.S. 1, 8, (1985) (“Because one of the factors is the extent of the intrusion, it is plain that reasonableness depends on not only when a seizure is made, but also how it is carried out” (internal citations omitted)). In assessing whether a Fourth Amendment violation has occurred, courts also consider the reasonableness of the manner in which the search was conducted. United States v. Ramirez, 523 U.S. 65, 65-66 (1998) (citing Pennsylvania v. Mimms, 434 U.S. 106, 108-109 (1977)). Reasonableness is governed by considering the “circumstances of the particular governmental invasion of a citizen’s

personal security” and a “balance between the public interest and the individual’s right to personal security free from arbitrary interference by law officers.” Mimms 434 U.S. at 108-09.

Execution of a search warrant must comport with the terms of the warrant and in a reasonable manner. United States v. Ganais, 824 F.3d 199, 209 (2d Cir. 2016). See also United States v. Miller, 430 F.3d 93, 97 (2d Cir. 2005) (alteration omitted) (quoting United States v. Knights, 534 U.S. 112, 118, (2001)). Courts have found that in executing a search warrant for a premises, detaining the occupants in a limited fashion so that a proper search can be conducted is reasonable. Michigan v. Summers, 452 U.S. 692, 705 (1981) (“Thus, for Fourth Amendment purposes, we hold that a warrant to search for contraband founded on probable cause implicitly carries with it the limited authority to detain the occupants of the premises while a proper search is conducted.”) Additionally, the time that a search is conducted is a factor in assessing reasonableness, e.g., executing a search warrant on a residence during the night is deemed a greater intrusion of privacy than doing so during the daytime. United States v. Messalas, No. 17-CR-339 (RRM), 2020 WL 4003604, at *8 (E.D.N.Y. July 14, 2020). (“This concern about nighttime entry finds expression in Federal Rule of Criminal Procedure 41(e)(2)(A)(ii), which requires that search warrants command that agents ‘execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time.’”).

B. Discussion

Law enforcement executed the search warrant reasonably and properly according to the limitations on the face of the warrant. The defendant argues that law enforcement violated the terms of the search warrant by entering the defendant’s residence at approximately 5:00 a.m. However, this is inaccurate. Law enforcement entered the residence at approximately 6:10 a.m., in compliance with the search warrant’s permitted times of entry between 6:00 a.m. and 10:00 p.m.

See Exhibit 1. Once they entered the residence, they executed the search warrant in a proper and reasonable manner.

Law enforcement's execution of the search warrant also shows that they exercised reasonable measures in entering the location, conducting a safety sweep, detaining any occupants, and conducting the search itself. Law enforcement knocked on the door to the defendant's residence, seeking to have an occupant open the door, rather than using more intrusive means such as destroying the door itself. Accordingly, the defendant's mother allowed the agents inside and the agents quickly began ascertaining who else was inside the residence, so that the executing agents could be sure that the premises were safe and secure before conducting the search, necessarily requiring momentary detentions of each occupant for safety purposes. See Summers, 452 U.S. at 694 (holding that it was lawful to temporarily detain the target of the search warrant who encountered law enforcement on the front steps to his house when they approached it to execute a search warrant on the premises). See also Muehler v. Mena, 544 U.S. 93, 93 (2005) (noting that Summers held "that minimizing the risk of harm to officers is a substantial justification for detaining an occupant during a search [internal citations omitted] and ruled that authority to detain incident to a search is categorical and does not depend on the 'quantum of proof justifying detention or the extent of the intrusion to be imposed by the seizure'"). This brief detention was, at most, six minutes long, enough time for law enforcement to enter the premises, secure the location, and begin the recorded conversation with the defendant at 6:16 a.m., after all the occupants had been located and detained. The reasonableness of the totality of the circumstances in which law enforcement acted to effectuate the search warrant, on balance, therefore lends credibility to law enforcement's documentation that the search warrant execution took place at a proper time, approximately 6:10 a.m. See Messalás at *8 (crediting law enforcement's assertions

that the search warrant was executed at 6:00 a.m. based on the testimony from three FBI agents and other independent corroboration and finding that the defendant's arguments that the search warrant was executed at 5:00 a.m. were unpersuasive).

To support the defendant's claim that the search warrant was executed approximately one hour before the permissible timeframe, the defendant attached affidavits signed by his mother and himself attesting that law enforcements entered at approximately 5:00 a.m. and were overly aggressive in securing the premises.¹⁰ But this Court need not consider whether if the defendant's statements were credited, suppression would still be warranted because there is corroboration that the search warrant was executed at approximately 6:10 a.m., as described above. In real time, law enforcement agents recorded the conversation with the defendant, noting the time and date of the search warrant execution. An FBI report drafted the next day also corroborates the timing of the search warrant execution as 6:10 a.m. rather than at 5:00 a.m. Photographs taken throughout the search warrant execution also support this timeline, in that in the photograph immediately prior to entry a timeline of the search warrant executing beginning it was dark because the sun had not yet risen. When law enforcement exited the location, the area was then well-lit because the sun had risen a few minutes before, at 7:05 a.m. If law enforcement had entered at approximately 5:00 a.m. and departed at approximately 6:00 a.m., both photographs of the area outside the residence's front door would have appeared similar, still dark because the sun would not have risen yet. Instead, the two photographs are starkly different in their depictions of the lighting condition at the beginning and conclusion of the search warrant execution.

¹⁰ The Motion and the two affidavits state that law enforcement agents were at the residence for two hours, from approximately 5:05 a.m. though 7:15 a.m. Motion at 4; Def. Ex. D, ¶¶ 1, 6; Ex. E, ¶¶ 7, 11. However, the Motion also states that law enforcement concluded the challenged search at 6:16 a.m., seemingly contradicting the perception of the defendant and the defendant's mother. Motion at 3.

The defendant, on the other hand, cannot corroborate his claim in the Motion with affidavits from himself and his mother that only contains conclusory statements that are dated more than 20 months after the date of the events at issue, and in direct tension with the photographic evidence generated on the day of the search.¹¹ See Messalas at *8 (finding that the Court need not reach the question of whether suppression would be warranted if the search warrant had in fact been executed at 5:00 a.m. instead of 6:00 a.m. because the Court found the testimony of law enforcement agents to be credible and independently corroborated in asserting that the search warrant had been executed at 6:00 a.m.).

II. THE DEFENDANT’S STATEMENTS TO LAW ENFORCEMENT SHOULD NOT BE SUPPRESSED BECAUSE THE DEFENDANT WAS NOT IN CUSTODY

The defendant’s statements that he made to law enforcement on March 16 during the search warrant execution should not be suppressed. The defendant’s Sixth Amendment claim must fail because he was not in custody at the time of his interview with law enforcement. The conditions in which he spoke with law enforcement show that he was clearly in a noncustodial setting: he was in his home and was told multiple times that he was free to leave and not under arrest. Thus, Miranda warnings were not required, and the Motion fails to show that the defendant’s statements to law enforcement were anything other than voluntary.

A. Applicable Law

Generally, a person must be advised of certain rights before being subject to a “custodial interrogation.” Miranda v. Arizona, 384 U.S. 436, 444 (1966). In order for Miranda

¹¹ On March 12, 2023, daylight savings time for the Eastern Time zone began at 3:00 a.m. so that clocks were to be adjusted one hour forward. Thus, a clock that had not yet been adjusted to reflect daylight savings time would, on March 16, 2023, have displayed a time approximately one hour behind the accurate time. In other words, 6:00 a.m. would have appeared on such a clock to be 5:00 a.m.—as appears to have been the case with the camera used to take photographs during the search as reflected above. See n.4-n.9, above.

warnings to be required, the Court must find both that (1) there was an interrogation of the defendant, and (2) the interrogation was while the defendant was in “custody.” United States v. FNU LNU, 653 F.3d 144, 148 (2d Cir. 2011) (citing Cruz v. Miller, 255 F.3d 77, 80–81 (2d Cir. 2001)).

An individual is in custody when “subjected to restraints comparable to those associated with a formal arrest.” Berkemer v. McCarty, 468 U.S. 420, 441 (1984). The Second Circuit has held that even “the mere fact of incarceration does not necessarily require that an individual be in the sort of custody that warrants Miranda warnings before an interview.” Georgison v. Donelli, 588 F.3d 145, 157 (2d Cir. 2009). Whether a defendant was in custody during questioning involves an objective inquiry into the totality of the circumstances, considering “how a reasonable person in the suspect’s position would view the situation.” FNU LNU, 653 F.3d at 151 (emphasis in original) (citing Stansbury v. California, 511 U.S. 318, 323 (1994)). More specifically, the overarching inquiry is whether “a reasonable person in the suspect’s position would have understood h[im]self to be subjected to restraints comparable to those associated with formal arrest.” United States v. Yilmaz, 508 F. App’x 49, 51 (2d Cir. 2013) (quoting FNU LNU, 653 F.3d at 154). This inquiry necessarily involves “considering the circumstances surrounding the encounter with authorities,” including:

the interrogation’s duration; its location (e.g., at the suspect’s home, in public, in a police station, or at the border); whether the suspect volunteered for the interview; whether the officers used restraints; whether weapons were present and especially whether they were drawn; [and] whether officers told the suspect he was free to leave or under suspicion . . .

FNU LNU, 653 F.3d at 153. Whether a person is in custody for Miranda purposes “is determined by neither the perception of the defendant nor of the police.” United States v. Galloway, 316 F.3d 624, 629 (6th Cir. 2003). Rather, it is determined by the “objective perception of a reasonable man

in the defendant's shoes." Id. (citing Stansbury v. California, 511 U.S. 318, 323 (1994)); FNU LNU, 653 F.3d at 153. Notably, the reasonable person from whose perspective "custody" is defined is a reasonable innocent person. Florida v. Bostick, 501 U.S. 429, 437–38 (1991); United States v. Moya, 74 F.3d 1117, 1119 (11th Cir. 1996). Whether a defendant knows he is guilty and believes incriminating evidence will soon be discovered is irrelevant. Bostick, 501 U.S. at 437–38; Moya, 74 F.3d at 1119.

Questioning of a defendant in their own home often signals to the court that a defendant is not in custody. "[C]ourts rarely conclude, absent a formal arrest, that a suspect questioned in her own home is 'in custody.'" United States v. Faux, 828 F.3d 130, 135-36 (2d Cir. 2016) (citing United States v. Badmus, 325 F.3d 133, 139 (2d Cir. 2003) (finding a suspect not in custody when questioned at home for two hours while agents executed a search warrant); see also United States v. Familetti, 878 F.3d 53, 60-62 (2d Cir. 2017) (holding that the defendant was not in custody during the execution of a search warrant where the defendant was in his own home, not restrained and law enforcement did not have their guns drawn); United States v. Mitchell, 966 F.2d 92, 99 (interrogation in familiar surroundings of one's home generally not custodial). In addition, when evaluating whether a defendant is in custody, it is an important factor that he is told that he is not under arrest. United States v. Schaffer, No. 12-CR-430 (ARR), 2014 WL 1515799, at *8 (E.D.N.Y. Apr. 18, 2014) (citing United States v. Newton, 369 F.3d 659, 676 (2d Cir. 2004)); see also United States v. Badmus, 325 F.3d 133, 139 (2d Cir. 2003) (agents told defendant and his wife that they were not under arrest and conducted interview in familiar setting of defendant's home).

B. Discussion

As a preliminary matter, the defendant's claims under the Sixth Amendment are without legal basis because the Sixth Amendment is inapplicable under the circumstances. The

defendant was not charged with any crime at the time of his interview with law enforcement on March 16, 2022. The Sixth Amendment right to counsel is offense specific and does not attach until a prosecution is commenced. Texas v. Cobb, 532 U.S. 162, 173 & n.3 (2001); United States v. Moore, 670 F.3d 22, 233-35 (2d Cir. 2012). The defendant was prosecuted not on March 16, when the search warrant was effectuated, but on January 17, 2023 when a grand jury indicted him. Accordingly, the defendant was indisputably in custody when he was arrested on January 23, 2023 pursuant to the arrest warrant issued in connection with the January 17, 2023 indictment, and not before.

In addition to the factual timing of when the defendant's Sixth Amendment right attached, the circumstances surrounding the defendant's interview with law enforcement on March 16 demonstrate that he was not in custody at the time he made his statements. The defendant was not only clearly told multiple times by law enforcement that he was free to leave, but also was told that no one was under arrest. The defendant was also interviewed for the entirety of the conversation in his own residence, further indicating that he was not in custody. See Faux 828 F.3d at 135-36 (2d Cir. 2016) (citing Badmus, 325 F.3d at 139); Mitchell, 966 F.2d 99 (holding that the defendant being at home while the search warrant is being executed there indicates that he is not in custody). Additionally, the defendant was seated on a bed during the conversation, with two law enforcement agents seated across from him in chairs. There was no law enforcement agent blocking or standing watch by the door.

The manner in which law enforcement also addressed the defendant during this conversation also demonstrates that the defendant was not under arrest, as the agent on the recorded conversation apologizes for the intrusion, explains why he is there, shows the defendant the warrant, offers to explain the warrant to the defendant, informs the defendant he is not under arrest

and that the defendant can leave if he must go to work or otherwise wishes to leave. See Motion Ex. C at 00:48-02:57. A reasonable person in the defendant's situation would have understood, based on such indicia, that he was not in custody—and the defendant's response comports with the reasonable person standard that the court explained in Galloway—while the defendant told law enforcement that he would rather not be in this situation, he does not leave the location and instead engages in a conversation with law enforcement for approximately 52 minutes about their investigation into his CSAM purchases.

The dialogue between the defendant and law enforcement, including the multiple reminders to the defendant that he is not under arrest and that he is free to leave, clearly show that the defendant was not in custody at the time of the interview, and that he made his statements to law enforcement officers lawfully and voluntarily. At three different points during the conversation, the defendant was told, in sum and substance, that continuing the conversation was voluntary and not required. The defendant was also told twice that he was not under arrest. The law enforcement agent who spoke with the defendant presented the defendant's options, clearly in plain terms and multiple times—leaving or staying. At no point did law enforcement ever tell the defendant that he had to answer a single question posed to him. The law enforcement agent also asked after informing the defendant, repeatedly, that he was free to leave and that he was not under arrest, if the defendant understood what the law enforcement agent was saying. At no point did the defendant indicate that he did not understand his two options or ask for clarification. Instead, the defendant chose to stay and chose to continue the conversation, asking the law enforcement

agents why they were at the residence and what the search warrant was about. Accordingly, his choice to speak was a voluntary one, and his statements should not be suppressed.

III. A HEARING—IF ANY IS REQUIRED—SHOULD BE LIMITED TO THE TIME THE SEARCH WARRANT WAS EXECUTED

There is sufficient evidence in the record for the Court to deny the Motion without a hearing, by crediting the statements on the recording that the interview began at 6:16 a.m. and the photographs depicting sunrise as set forth above. Should the Court wish to hold a hearing, however, any evidentiary hearing should be limited to the narrow issue of the time of the search warrant execution on March 16, 2022. While there are no material facts in dispute regarding the circumstances and manner in which law enforcement obtained statements from the defendant, the time of day at which law enforcement carried out the search warrant is the sole issue that has any bearing on the suppression of any evidence.

A. Applicable Law

A defendant has no absolute right to an evidentiary hearing on a motion to suppress evidence. See In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 165 (2d Cir. 2008) (“[A]n evidentiary hearing on a motion to suppress ordinarily is required if the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact going to the validity of the search are in question.” (internal quotation marks and citation omitted)). A material factual dispute must exist for a hearing to be justified. See United States v. Gillette, 383 F.2d 843, 848 (2d Cir. 1967) (holding that suppression hearing is available only if there is a “factual issue to be resolved”); United States v. Ashburn, 76 F. Supp. 3d 401, 436 (E.D.N.Y. 2014) (NGG) (“defendant must show that disputed issues of material fact exist before an evidentiary hearing is required). “If the defendant’s request for a hearing is not accompanied by a sufficient ‘specification of the factual basis for the

characterization, the district court is not required to have a hearing.” United States v. Spencer, No. 06-CR-413 (DLI), 2016 WL 6781225, at *5 (E.D.N.Y. Nov. 15, 2016) (quoting United States v. Mathurin, 148 F.3d 68, 69 (2d Cir. 1998) (per curiam) (alteration omitted)).

It is not enough simply to attach an affidavit to moving papers; the defendant must assert facts which, taken as true, would merit the suppression of the challenged evidence. See United States v. Chandler, 164 F. Supp. 3d 368, 376 (E.D.N.Y. 2016) (“[I]f facts urged in support of a hearing would not entitle the moving party to relief as a matter of law, no evidentiary hearing is required.”) (quotation marks and citation omitted); see also United States v. Townsend, No. 15-CR-653 (DLI), 2016 WL 3562055, at *2 (E.D.N.Y. June 23, 2016).

B. Discussion

Should the Court hold a hearing, it should be limited to the narrow issue of the time that law enforcement executed the search warrant. The government anticipates that at such a hearing, it will present the evidence as described above that the search execution began shortly after 6:00 a.m. on the date in question, as authorized on the face of the warrant. The remainder of the Motion should be denied without a hearing.

Here, other than the time at which the search warrant was executed, there are no material facts in dispute that would result in the suppression of any evidence. The Motion to suppress the defendant’s statements should be denied without a hearing because it fails to identify a material factual dispute this Court must resolve in order to determine whether the defendant was in custody at the time that he made statements to law enforcement. The material facts in this case regarding the circumstances of the defendant’s statements are not in dispute. Although the defendant submitted two affidavits in support of the Motion, the affidavits lack specific or disputed facts required for a hearing regarding the legality of his statements. In other words, even if each

of the facts alleged in the affidavits were true, nothing in the affidavits raise a sufficiently “definite, specific, detailed, and nonconjectural” factual basis that bears on the legality of law enforcement obtaining the defendant’s statements. See United States v. Pena, 961 F.2d 333, 339 (2d Cir. 1992).

CONCLUSION

For the foregoing reasons, the government respectfully submits that the Motion to suppress the defendant’s statement should be denied. As to the Motion to suppress the evidence recovered from the search warrant, should a hearing be held, such hearing should be limited to the narrow issue of the time of execution of the search warrant.

Dated: Brooklyn, New York
December 29, 2023

Respectfully submitted,

BREON PEACE
UNITED STATES ATTORNEY
Eastern District of New York
Attorney for Plaintiff
271 Cadman Plaza East
Brooklyn, New York 11201

By: /s/ Stephanie Pak
Stephanie Pak
Assistant United States Attorney
(718) 254-6064

EXHIBIT 1

TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK



APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

IN THE MATTER OF THE SEARCH OF (1)
THE PREMISES KNOWN AND DESCRIBED
AS 799 PINE STREET, APT. 1, BROOKLYN
NEW YORK AND (2) THE PERSON OF
SHAKEEM RANKIN

22-MJ-298

Docket Number

SUBMITTED BY: Plaintiff ___ Defendant ___ DOJ
Name: Nina Gupta
Firm Name: USAO-EDNY
Address: 271-A Cadman Plaza East
Brooklyn, New York 11201
Phone Number: (718)-254-6257
E-Mail Address: nina.gupta@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO

If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: _____; or C.) This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

3/15/2022
DATE

Nina C. Gupta
SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____

Judge/Magistrate Judge: _____

Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing criminal investigation

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
AND MAY NOT BE UNSEALED UNLESS ORDERED BY
THE COURT.**

DATED: Brooklyn, NEW YORK

3/15/2022

James R. Cho

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE _____

DATE

AB:MAA/NCG

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF (1)
THE PREMISES KNOWN AND
DESCRIBED AS 799 PINE STREET,
APT. 1, BROOKLYN NEW YORK
INCLUDING ANY CLOSED AND
LOCKED CABINETS AND CONTAINERS
FOUND THEREIN; AND (2) THE PERSON
OF SHAKEEM RANKIN (DATE OF
BIRTH: AUGUST 10, 1994) AND THE
AREA WITHIN HIS IMMEDIATE REACH,
INCLUDING ANY PERSONAL EFFECTS
LOCATED THEREIN

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH
WARRANT

Case No. 22-MJ-298

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, ANGELA TASSONE, being first duly sworn, hereby depose and state as
follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”),
and have been for almost eight years. I am currently assigned to the Child Exploitation and
Human Trafficking Task Force, where I investigate violations of criminal law relating to the
sexual exploitation of children. In the course of these investigations, I have reviewed thousands
of photographs depicting children being sexually exploited by adults and have executed search
warrants of premises and electronic devices. Through my experience in these investigations, I
have become familiar with methods of determining whether a child is a minor.

2. I submit this affidavit, pursuant to Federal Rule of Criminal Procedure 41, in support of an application for a warrant and order authorizing the search of:

- a. the premises known and described as 799 Pine Street, Apt. 1, Brooklyn New York (the "PREMISES"), including any closed and locked cabinets and containers found therein. The PREMISES is further described below and in Attachment A.
- b. the person of SHAKEEM RANKIN (date of birth August 10, 1994) and the area within his immediate reach, including any personal effects located therein.

RANKIN is further described below and in Attachment A.

3. Collectively, I refer to RANKIN and the PREMISES as the "SUBJECT PREMISES." Based on the facts set forth in this affidavit, there is probable cause to believe that a search of the SUBJECT PREMISES will yield evidence, instrumentalities, fruits or contraband of violations of Title 18, United States Code, Sections 2252 and 2252A (receipt of child pornography, possession of and access with intent to view child pornography), 2252A(a)(2)(A) and (b)(1) receipt and distribution of child pornography, and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography (the "SUBJECT OFFENSES") committed by SHAKEEM RANKIN and others.

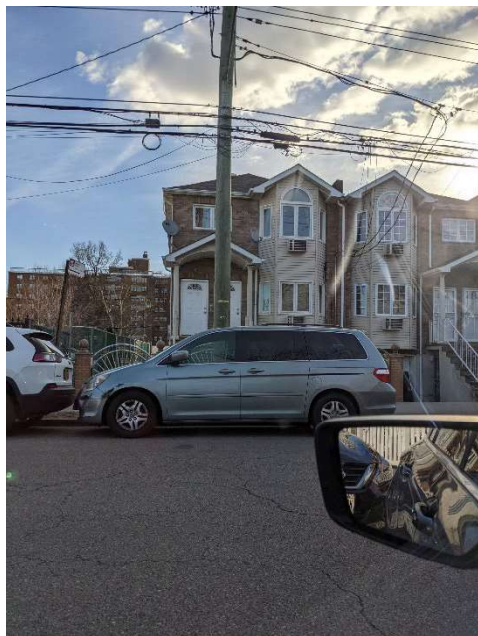
4. This affidavit is based on my training and experience, my personal knowledge of the investigation, my review of relevant records and reports and information obtained from other law enforcement agents, and my training and experience concerning the use of criminal activity and the forensic analysis of electronically stored information ("ESI"). This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where the contents of documents and

the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

RANKIN AND THE PREMISES

5. The PREMISES is a multi-level residential dwelling located at 799 Pine Street, Apt. 1, Brooklyn New York. The building containing the PREMISES is brick, with part of it painted in a tan color and with white trim. The building containing the PREMISES contains two apartments. There are two white front doors at the front of the building, accessed by going up a flight of outside steps, with the door on the right (while facing the apartment) leading to Apartment 1 and the door on the left leading to Apartment 2. The following photographs depict the building containing the PREMISES:





6. RANKIN was born on August 10, 1994. He is a 28-year-old male who stands approximately 5 feet 10 inches tall. He has a dark-skinned complexion, black hair, and brown eyes. As described further herein, there is probable cause to believe that RANKIN will be present at the PREMISES at the time the search warrant is executed and may have instrumentalities used to commit the SUBJECT OFFENSES—particularly, cellular telephones—on his person at that time. A photograph of RANKIN is in Attachment A.

7. Based on open-source information, RANKIN currently resides at the PREMISES. At least one other adult male and one adult woman, all seemingly relatives of RANKIN's, seemingly also live at the PREMISES. Upon information and belief, RANKIN's relatives also live in Apartment 2.

8. This application seeks authorization to search the entirety of the PREMISES, as well as all attachments, attics, basements, garages (including the detached garage), carports, vehicles, outbuildings, storage units, appurtenances thereto, and all other areas

within the curtilage, and all closed and locked containers and electronic devices located therein; however, this application does not seek authorization to search Apartment 2.

9. This application also seeks authorization to search RANKIN and the area within his immediate reach, including any personal effects located therein.

PROBABLE CAUSE

The SUBJECT OFFENSES

10. Law enforcement officers currently are investigating RANKIN for distribution, receipt, and possession of child pornography.

11. Based on my conversations with other law enforcement officers involved in this investigation, my review of law enforcement reports and records, I have learned the following, in substance and in part:

12. Law enforcement officers have been investigating an individual (“Subject 1”) in St. Louis, Missouri, for production and distribution of child sexual abuse material (“CSAM”). Based on its investigation, law enforcement has determined that Subject 1 produced CSAM with his 9-year-old niece and advertised CSAM on Tumblr and Reddit. Subject 1’s advertisements directed individuals interested in CSAM to communicate with Subject 1 via Kik Messenger (also known as “Kik”), a mobile chat application that allows individuals to, among other things, engage in group conversations and share photographs and videos. Using Kik, Subject 1 negotiated prices to be paid to him for CSAM via “Cash App,” an application that enables users to send and receive money. After Subject 1 received the agreed-upon money, Subject 1 sent buyers links to CSAM images and/or videos using MEGA, an application that enables users to share files.

13. On or about May 4, 2021, law enforcement executed a judicially-authorized search warrant at Subject 1's residence. Pursuant to the search warrant, law enforcement searched Subject 1's cellular phones, on which they found Kik conversations.

14. Based on information recovered from Subject 1's phone, one of the buyers of MEGA links was Kik user "mulaDussa" (the "Subject Kik Account"). The links purchased by the Subject Kik Account contained over 2000 videos and images that law enforcement agents were able to identify as CSAM.

15. According to Kik chat logs, on or about April 9, 2021, Subject 1 sent messages to the Subject Kik Account asking if the Subject Kik Account wanted "cp," which Subject 1 described as "young young young content no preteens younger than preteens." After Subject 1 seemingly provided examples, Subject 1 stated "I got better stuff if u wanna buy." The Subject Kik Account responded "yeah I want all the Cp lol." Subject 1 instructed the Subject Kik Account to "Send \$80 I got u," and a few minutes later, the Subject Kik Account responded "Sent." Subject 1 then sent, among other things, links to MEGA and stated "If u want more let me kno."

16. According to Kik chat logs, on or about April 25, 2021, the Subject Kik Account asked Subject 1 to re-send "that link," explaining "It's not popping up anymore for some reason." Subject 1 responded "Resend fee," to which the Subject Kik Account asked "80?" and Subject 1 replied "Yop" and seemingly provided information for a new Cash App account. The Subject Kik Account requested "Send more Black girls if u got," in response to which Subject 1 subsequently stated "all black cp giant file there u go" and seemingly sent a MEGA link. The Subject Kik Account then asked about "the regular cp from B4," to which Subject 1 seemingly sent a MEGA link.

17. Based on information recovered from Subject 1's phone, Cash App user "Shamula" sent Subject 1 approximately \$80 on or about April 9, 2021 and another approximately \$80 on or about April 25, 2021, *i.e.*, on the dates of the Kik chats described above.

18. Based on subpoena returns from Kik, the email address associated with the Subject Kik Account is blab705@yahoo.com. The Kik subpoena returns also include the IP address used by the Subject Kik Account to access Kik. Based on subpoena returns from Verizon, the physical address associated with the IP address is the PREMISES, without the apartment number specified, in the name of "Jem Rankin," who law enforcement believes to be a relative of RANKIN's.

19. Based on Yahoo returns for the Yahoo blab705@yahoo.com email account, the associated telephone number is 212-518-8371. Based on open sources, the subscriber for that phone number is RANKIN.

20. To date, law enforcement officers have not been able to determine the MEGA accounts associated with the Kik chats between Subject 1 and the Subject Kik Account on April 9, 2021 and April 25, 2021. However, information from MEGA indicates an active account by user blab705@yahoo.com, *i.e.*, the same email address associated with the Subject Kik Account. Information from MEGA also includes the IP address from which user blab705@yahoo.com accessed MEGA, which is the same IP address used by the Subject Kik Account to access Kik. As indicated above, the physical address associated with this IP address is the PREMISES, without the apartment number specified.

21. Based on my training and experience, and the foregoing, I believe that RANKIN is the user of the Subject Kik Account and the blab705@yahoo.com MEGA account.

Moreover, given that the payment dates and amounts made from the “ShaMula” Cash App account correspond with the payment dates and amounts by the Subject Kik Account referenced in the Kik chats with Subject 1, I believe that RANKIN is the user of the “ShaMula” Cash app account.

22. On March 14, 2022, I conducted surveillance outside the PREMISES, and I observed RANKIN exit Apartment 1.

23. Based on my training and experience, I know that individuals who maintain and transmit child pornography often maintain lists of names, email addresses, telephone numbers, and screen names of others with whom they can share child pornography, and frequently do share child pornography with others. I also know that producers and collectors of child pornography typically retain their materials for extended periods of time. In this case, RANKIN twice purchased links containing over 2000 videos and images that law enforcement agents were able to identify as CSAM, and he asked for additional CSAM focused on a particular race and gender, in response to which he received a collection of materials. RANKIN therefore appears to be a collector of CSAM. Producers and collectors of child pornography frequently collect and view sexually explicit materials in a variety of media, such as videos, photographs, magazines, books, drawings, and other visual media that they use for sexual arousal and gratification. These examples of visual media are often stored on electronic devices including, but not limited to, phones, computers, disk drives, modems, thumb drives, digital cameras, and scanners.

24. In addition, based on my training and experience, I know that while individuals might delete chats, photographs and videos from their electronic devices, the metadata on electronic devices retains the chats, photographs and videos significantly longer.

Specifically, I know that chats, photographs and videos from Kik are recoverable for a significant period of time through searching the metadata, including with respect to deleted files. Finally, based on my training and experience, I know that individuals who possess and operate electronic devices often store, maintain, and/or utilize those devices in their place of residence.

25. Based on my training and experience, and the foregoing, I submit there is probable cause to believe that RANKIN has received images and videos of child pornography while physically present at the PREMISES. Moreover, I submit there is probable cause to believe that the SUBJECT PREMISES contain evidence, instrumentalities, contraband, and fruits of the SUBJECT OFFENSES.

TECHNICAL TERMS

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

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: 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.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

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

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

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

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

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the

United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

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

32. In addition to there being probable cause to believe that phones and/or computer devices will be found on the SUBJECT PREMISES that contain evidence of the SUBJECT OFFENSES, there also is probable cause to believe that these devices constitute instrumentalities and/or contraband subject to seizure, in that the devices were used to commit the SUBJECT OFFENSES and contain contraband child pornography.

33. *Biometric Unlocking.* In my training and experience, it is likely that if a subject has any electronic devices on his person or in his belongings, then one or more of those devices uses biometric unlocking features, such as facial recognition unlocking. The warrant I am applying for would permit law enforcement to compel the subject to unlock any electronic devices using the devices' biometric features. 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, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through 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, this feature is available on certain cellular phone devices. In order to activate this unlocking mechanism, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.
- d. If a device is equipped with an iris recognition feature, a user may enable the

ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared sensitive camera detects the registered irises. Iris recognition features on other manufacturers’ devices have different names but operate similarly to Windows Hello.

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. 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 48 hours has elapsed since the device was last unlocked, or (2) when the device has not been unlocked using a fingerprint for eight hours and the passcode or

password has not been entered in the last six days. Biometric features from other electronic device 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. The passcode or password that would unlock a given device recovered during execution of the requested warrant likely will not be known to law enforcement. Thus, in attempting to unlock any such devices for the purpose of executing the search authorized by the requested warrant, it will likely be necessary to press the finger(s) of the user on the fingerprint reader of any device capable of biometric unlocking. The government may not otherwise be able to access the data contained on the electronic devices for the purpose of executing the search authorized by this warrant.
- h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device.

34. Due to the foregoing, if any of RANKIN's electronic devices may be unlocked using one of the aforementioned biometric features, then the warrant I am applying for would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of RANKIN against the fingerprint scanner of the device; (2) hold RANKIN in place while holding the device in front of his face to activate the facial recognition feature; and/or (3) hold RANKIN in place while holding the device in front of his face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by

this warrant.

35. Based on the foregoing, I respectfully submit there is probable cause to believe that RANKIN committed the SUBJECT OFFENSES, and that evidence of this criminal activity is likely to be found in the PREMISES and in the closed containers/items stored therein, including any electronic devices found on RANKIN's person while he is physically present in the PREMISES.

A. Execution of Warrant for ESI

36. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," including for "later review." Consistent with Rule 41, this application requests authorization to seize the items listed in Attachment B and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- a. First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- b. Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- c. Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- d. Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

37. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

38. An item may be seized if law enforcement officers reasonably believe that (a) the item belongs to RANKIN, based on the location of the item, identifying information on the exterior of the device, other information available to the officers, and statements made by residents of the PREMISES at the time of the search, and (b) the item does not otherwise appear to belong to a resident of the PREMISES who is not involved in the commission of the SUBJECT OFFENSES.

B. Review of ESI

39. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

40. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

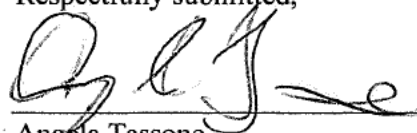
41. If the government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the government will return these items. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the SUBJECT OFFENSES.

CONCLUSION

42. Based on the foregoing, there is probable cause to believe that a search of the SUBJECT PREMISES described in Attachment A to search for and/or seize the items set forth in Attachment B will uncover evidence, fruits, instrumentalities or contraband of the SUBJECT OFFENSES.

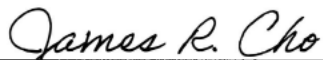
43. I respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this affidavit and the search warrant. These documents discuss an ongoing criminal investigation that is neither public nor known to the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure might seriously jeopardize that investigation, including by giving subjects an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,



Angela Tassone
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone
on March 15, 2022



HONORABLE JAMES R. CHO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Premises to Be Searched

The person of SHAKEEM RANKIN (date of birth August 10, 1994) and the area within his immediate reach, including any personal effects located therein. RANKIN is a 28-year-old male who stands approximately 5 feet 10 inches tall. He has a dark-skinned complexion, black hair, and brown eyes. He is pictured here:



The premises to be searched includes is a multi-level residential dwelling located at 799 Pine Street, Apt. 1, Brooklyn New York (“the SUBJECT PREMISES”). The building containing the SUBJECT PREMISES is brick, with part of it painted in a tan color and with white trim. The building containing the SUBJECT PREMISES contains two apartments. There are two white front doors at the front of the building, accessed by going up a flight of outside steps, with

the door on the right (while facing the apartment) leading to Apartment 1 and the door on the left leading to Apartment 2. The following photographs depict the building containing the

SUBJECT PREMISES:



ATTACHMENT B

Property to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized include the following evidence, instrumentalities, fruits or contraband of violations of Title 18, United States Code, Sections 2252 and 2252A (receipt of child pornography, possession of and access with intent to view child pornography), 2252A(a)(2)(A) and (b)(1) receipt and distribution of child pornography, and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography (the “SUBJECT OFFENSES”) committed by SHAKEEM RANKIN and others, described as follows:

1. Computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the SUBJECT OFFENSES. For purposes of this Attachment A, computer devices, storage media, and related electronic equipment includes, but is not limited to, any computer, computer system and high-speed data processing device, including, but not limited to, desktop computers, notebook computers, tablets, and server computers; mobile phones, including, but not limited to, smart phones capable of transmitting electronic messages (such as text messages and email messages); tapes; cassettes; cartridges; streaming tape; commercial software and hardware; network hardware and software; computer disks; disk drives; monitors; computer printers; modems; tape drives; disk application programs; data disks; system disk operating systems; tape systems and hard drive and other computer related operation equipment; routers, modems, and network equipment used to connect to the Internet; cameras; video cameras; scanners; computer photographs; graphic interchange formats and/or photographs; undeveloped photographic film, slides, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG); any electronic data storage devices including, but not limited to, hardware, software, diskettes, magnetic media floppy disks; backup tapes, CD-ROMs, DVDs, RAM, flash memory devices, and other storage mediums; and any input/output peripheral devices, including, but not limited to, data security devices;
2. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
3. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
4. Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
5. Correspondence and records pertaining to violation of the SUBJECT OFFENSES including, but not limited to, envelopes, letters, mailings, electronic mail, chat logs, electronic messages, books, ledgers, and records bearing on the production, reproduction,

receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

6. Communications with any minor from whom any child pornography, as defined by 18 U.S.C. § 2256(8), is solicited or received;
7. Any child pornography as defined by 18 U.S.C. § 2256(8);
8. Any visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
9. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, envelopes, letters, papers, electronic mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
10. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
11. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the SUBJECT OFFENSES, including, but not limited to, sales receipts, warranties, bills for Internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs;
12. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence; and
13. Evidence that SHAKEEM RANKIN subscribed to and accessed Kik, and any other evidence relating to Kik that demonstrates user attribution.

An item may be seized if law enforcement officers reasonably believe that (a) the item belongs to SHAKEEM RANKIN, based on the location of the item, identifying information on the exterior of the device, other information available to the officers, and statements made by residents of the PREMISES at the time of the search, and (b) the item does not otherwise appear

to belong to a resident of the PREMISES who is not involved in the commission of the SUBJECT OFFENSES.

B. Search and Seizure of ESI

The items to be seized also include any computer devices and storage media that may contain any electronically stored information (“ESI”) falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (which may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the Government in this investigation, and outside technical experts under Government control) are authorized to review the ESI contained therein for information responsive to the warrant.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other ESI within the categories identified in Sections A and B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

D. Biometric Unlocking

If it is determined that one or more of electronic devices covered by this warrant can be enabled or unlocked with “Touch ID” or other biometric unlocking features, law enforcement officers are authorized to (1) press or swipe the fingers (including thumbs) of RANKIN against the fingerprint scanner of the device; (2) hold RANKIN in place while holding the device in front of his face to activate the facial recognition feature; and/or (3) hold RANKIN in place while holding the device in front of his face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the Eastern District of New York

In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address)

(1) THE PREMISES KNOWN AND DESCRIBED AS 799 PINE STREET, APT. 1, BROOKLYN NEW YORK INCLUDING ANY CLOSED AND LOCKED CABINETS AND CONTAINERS FOUND THEREIN; AND (2) THE PERSON OF SHAKEEM RANKIN (DATE OF BIRTH: AUGUST 10, 1994) AND THE AREA WITHIN HIS IMMEDIATE REACH, INCLUDING ANY PERSONAL EFFECTS LOCATED THEREIN

Case No. 22-MJ-298

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York (identify the person or describe the property to be searched and give its location):

(1) THE PREMISES KNOWN AND DESCRIBED AS 799 PINE STREET, APT. 1, BROOKLYN NEW YORK INCLUDING ANY CLOSED AND LOCKED CABINETS AND CONTAINERS FOUND THEREIN; AND (2) THE PERSON OF SHAKEEM RANKIN (DATE OF BIRTH: AUGUST 10, 1994) AND THE AREA WITHIN HIS IMMEDIATE REACH, INCLUDING ANY PERSONAL EFFECTS LOCATED THEREIN, AS SET FORTH IN ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before March 29, 2022 (not to exceed 14 days) in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge (United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for days (not to exceed 30) until, the facts justifying, the later specific date of

Date and time issued: 3/15/2022 at 6:04 p.m.

James R. Cho Judge's signature

City and state: Brooklyn, New York

Hon. James R. Cho U.S.M.J. Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:
22-MJ-298

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

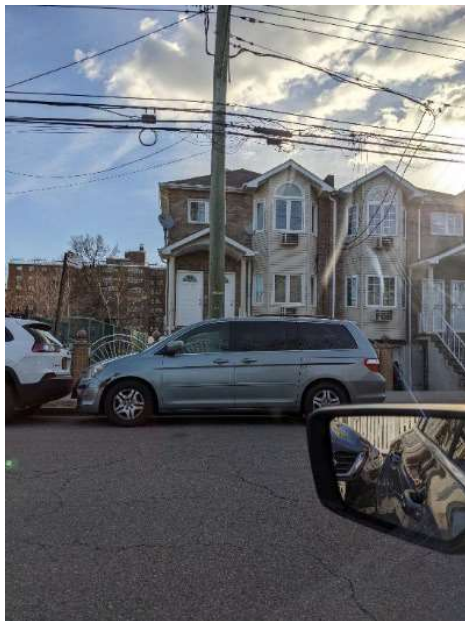
Premises to Be Searched

The person of SHAKEEM RANKIN (date of birth August 10, 1994) and the area within his immediate reach, including any personal effects located therein. RANKIN is a 28-year-old male who stands approximately 5 feet 10 inches tall. He has a dark-skinned complexion, black hair, and brown eyes. He is pictured here:



The premises to be searched includes is a multi-level residential dwelling located at 799 Pine Street, Apt. 1, Brooklyn New York (“the SUBJECT PREMISES”). The building containing the SUBJECT PREMISES is brick, with part of it painted in a tan color and with white trim. The building containing the SUBJECT PREMISES contains two apartments. There are two white front doors at the front of the building, accessed by going up a flight of outside steps, with

the door on the right (while facing the apartment) leading to Apartment 1 and the door on the left leading to Apartment 2. The following photographs depict the building containing the SUBJECT PREMISES:



ATTACHMENT B

Property to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized include the following evidence, instrumentalities, fruits or contraband of violations of Title 18, United States Code, Sections 2252 and 2252A (receipt of child pornography, possession of and access with intent to view child pornography), 2252A(a)(2)(A) and (b)(1) receipt and distribution of child pornography, and 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography (the “SUBJECT OFFENSES”) committed by SHAKEEM RANKIN and others, described as follows:

1. Computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the SUBJECT OFFENSES. For purposes of this Attachment A, computer devices, storage media, and related electronic equipment includes, but is not limited to, any computer, computer system and high-speed data processing device, including, but not limited to, desktop computers, notebook computers, tablets, and server computers; mobile phones, including, but not limited to, smart phones capable of transmitting electronic messages (such as text messages and email messages); tapes; cassettes; cartridges; streaming tape; commercial software and hardware; network hardware and software; computer disks; disk drives; monitors; computer printers; modems; tape drives; disk application programs; data disks; system disk operating systems; tape systems and hard drive and other computer related operation equipment; routers, modems, and network equipment used to connect to the Internet; cameras; video cameras; scanners; computer photographs; graphic interchange formats and/or photographs; undeveloped photographic film, slides, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG); any electronic data storage devices including, but not limited to, hardware, software, diskettes, magnetic media floppy disks; backup tapes, CD-ROMs, DVDs, RAM, flash memory devices, and other storage mediums; and any input/output peripheral devices, including, but not limited to, data security devices;
2. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment;
3. Originals, copies, and negatives of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
4. Motion pictures, films, videos, and other recordings of visual or written depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);
5. Correspondence and records pertaining to violation of the SUBJECT OFFENSES including, but not limited to, envelopes, letters, mailings, electronic mail, chat logs, electronic messages, books, ledgers, and records bearing on the production, reproduction,

receipt, shipment, orders, requests, trades, purchases, or transactions involving any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

6. Communications with any minor from whom any child pornography, as defined by 18 U.S.C. § 2256(8), is solicited or received;
7. Any child pornography as defined by 18 U.S.C. § 2256(8);
8. Any visual depictions of minors engaged in sexually explicit conduct as defined by 18 U.S.C. § 2256(2);
9. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, envelopes, letters, papers, electronic mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes, related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
10. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors) related to the possession, distribution, receipt, or production of, or access with intent to view, child pornography as defined in 18 U.S.C. § 2256(8), or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);
11. Records or other items which evidence ownership, control, or use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the SUBJECT OFFENSES, including, but not limited to, sales receipts, warranties, bills for Internet access, handwritten notes, registry entries, configuration files, saved usernames and passwords, user profiles, email contacts, and photographs;
12. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence; and
13. Evidence that SHAKEEM RANKIN subscribed to and accessed Kik, and any other evidence relating to Kik that demonstrates user attribution.

An item may be seized if law enforcement officers reasonably believe that (a) the item belongs to SHAKEEM RANKIN, based on the location of the item, identifying information on the exterior of the device, other information available to the officers, and statements made by residents of the PREMISES at the time of the search, and (b) the item does not otherwise appear

to belong to a resident of the PREMISES who is not involved in the commission of the SUBJECT OFFENSES.

B. Search and Seizure of ESI

The items to be seized also include any computer devices and storage media that may contain any electronically stored information (“ESI”) falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (which may include, in addition to law enforcement officers and agents, attorneys for the Government, attorney support staff, agency personnel assisting the Government in this investigation, and outside technical experts under Government control) are authorized to review the ESI contained therein for information responsive to the warrant.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other ESI within the categories identified in Sections A and B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

D. Biometric Unlocking

If it is determined that one or more of electronic devices covered by this warrant can be enabled or unlocked with “Touch ID” or other biometric unlocking features, law enforcement officers are authorized to (1) press or swipe the fingers (including thumbs) of RANKIN against the fingerprint scanner of the device; (2) hold RANKIN in place while holding the device in front of his face to activate the facial recognition feature; and/or (3) hold RANKIN in place while holding the device in front of his face to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.