IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

United States of America, v. Robert John May, III, Defendant.	Cr. No. 3:25-778-CMC **Order**

This matter is before the court on Defendant's *pro se* motion to suppress and request for *Franks* hearing, filed September 10, 2024. ECF No. 64. Defendant seeks to suppress the items found in a search of his home and person conducted August 5, 2024. He asserts the search warrant was issued based on an affidavit containing statements the agent knew were false or at least were made with a reckless disregard for the truth, and/or omitted material statements.

The Government filed a response in opposition, arguing Defendant is not entitled to a *Franks* hearing. ECF No. 74. It contends Defendant has failed to show a false statement was made intentionally or recklessly, and the probable cause determination did not depend on paragraph 9(e) of the affidavit. *Id.* at 5-10. The Government also submits Defendant has failed to show facts were intentionally or recklessly omitted from the affidavit, as the alleged omissions are not facts or evidence. *Id.* at 14.

Defendant filed a reply, which again contends there would be no probable cause if Special Agent Lorenzen's testimony from the detention hearing was added to or substituted in the affidavit. ECF No. 78. He also submits the Government is attempting to "wrongly reclassify" Kik as a cloud storage depository, but it is a chat application. *Id.* at 9. He asserts the affidavit's description of

child pornographers' habits changed depending on whether she was attempting to obtain a search warrant or had already obtained one. *Id.* at 16.

A hearing on Defendant's motion was held September 24, 2025. This order follows.

BACKGROUND

On May 27, 2024, the National Center for Missing and Exploited Children ("NCMEC") received a CyberTip related to information from a peer-to-peer file sharing application, Kik.[1] The CyberTip indicated Kik user joebidennnn69 distributed approximately 50 files containing child pornography, or child sexual abuse material ("CSAM")[2] on March 31, 2024. The IP address associated with the CyberTip was 16223418843 ("the 162 IP address"), registered to an AT&T account that geolocated[3] to West Columbia, South Carolina. The local Internet Crimes Against Children ("ICAC") division of the South Carolina Attorney General's Office forwarded the Tip to the ICAC affiliate in the Lexington County Sheriff's Department ("LCSD"). LCSD submitted

---

[1] Kik is a social media company that operates the Kik Messenger Application, a chat application that allows users to communicate and share videos and photographs in group and person-to-person settings with other Kik users. When a user installs and uses Kik on their phone, the app collects various details about the device, which typically includes: (a) Device Information, such as the make and model of the device, operating system version, device identifiers (such as the device ID), and other hardware characteristics; and (b) System Information, such as the type of operating system, version number, mobile network information, and other technical details. This information is usually gathered during the app installation and whenever the app runs.

[2] NCMEC refers to child pornography images as CSAM outside the legal system to accurately reflect what is depicted – sexual abuse and exploitation of children. *See also United States v. Keuhner*, 126 F.4th 319, 322n.1 (4th Cir. 2025).

[3] Geolocation is the identification of the real-world geographic location of an object, done by generating a set of geographic coordinates through GPS and using the coordinates to determine a meaningful location.

search warrants to AT&T, Google, and Kik. The AT&T search warrant revealed the billing party for the 162 IP address was Robert May and the service address was his home address in West Columbia, South Carolina. The Kik search warrant showed the user, joebidennnn69, registered the account on March 30, 2024, using a Samsung model SM-G781U1 Android smartphone and an email address of joehoe12368@gmail.com. Kik's production showed the joebidennnn69 account contained 265 CSAM videos and exchanged approximately 1,147 messages between March 30 and April 4, 2024, many involving trades of CSAM.

Homeland Security Investigators ("HSI") confirmed Robert May lived at the subject address through property records, Department of Motor Vehicle records, and physical surveillance of the property. Agents also confirmed the resident's Wi-Fi network was password protected, meaning any CSAM activity using the 162 IP address required prior access to Defendant's secure home network.

Using the information above, HSI applied for a federal search warrant for the Target Location, the May residence, and the Target Individual, Robert May.

In support of the application for search warrant, HSI Special Agent Britton Lorenzen submitted an affidavit. The affidavit summarized the background of the investigation, including the CyberTip from Kik including the AT&T 162 IP address, the state search warrants to Kik and AT&T, and Kik messages discussing trades of CSAM with other Kik users. ECF No. 64-1 at ¶¶ 10-16.

In paragraph 9, Special Agent Lorenzen summarized her knowledge regarding child pornography, based on her training and experience, and stated:

a. Persons who are involved with child pornography generally have other sexually explicit materials related to their interest in children, which may consist of photographs, motion pictures, videos, text material, computer graphics and digital or other images for their own sexual gratification, often including child erotica, which may consist of images or text writing involving sex with minors that do not rise to the level of child pornography but nonetheless fuel their deviant sexual fantasies involving minors. Such individuals are usually, but not always male. I am aware this sort of material has been admitted in trials under Fed. R. Evid. 404(b) to prove such things as the possessor's knowledge, intent, motive, and identity and under Fed. R. Evid. 414 to prove the person has a sexual interest in minors.

b. Individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. They do this to gain status, trust, acceptance, and support and to increase their collection of illicit images and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer (P2P) chat and file sharing programs, e-mail, e-mail groups, bulletin boards, Internet Relay Chat (IRC), newsgroups, Internet clubs, and various forms of Instant Messaging such as Yahoo! Messaging, and "chat" that is sometimes saved on the user's computer or other digital storage media.

c. Besides sexual photos of minors and child erotica, such individuals often produce and/or collect other written material on the subject of sexual activities with minors, which range from fantasy stories to medical, sociological, and psychological writings, which they save to understand and justify their illicit behavior and desires.

d. Individuals who collect child pornography often collect, read, copy or maintain names, addresses, including e-mail addresses, phone numbers, and lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. or have child pornography and child erotica for sale or trade. These contacts are maintained for personal referral, exchange or. sometimes, commercial profit. They may maintain these names on computer storage devices, web sites or other Internet addresses, and their discovery can serve as leads to assist law enforcement in proving the instant case and in apprehending others involved in the underground trafficking of child pornography.

As to the issue of staleness, ¶ 9e states:

e. As for staleness concerns, individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their

> collection of illicit materials. The known desire of such individuals to retain child pornography, together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or send it to third party image storage sites via the Internet.

Id. at 5-6. The affidavit avers there is probable cause to believe evidence of violations of laws prohibiting possession of child pornography will be found in the Target Location and on devices therein:

> 19. Based on my training and experience, I submit there is probable cause to believe that the Target Location contains evidence of violations of the target offense including on devices in Target Individual's possession.
> 24. Based on the above and my training and experience, I further submit there is probable cause to believe the Target Location is used by Target Individual to store electronic devices containing evidence of the target offense.
> 25. Based on the above, I respectfully submit that there is probable cause to believe that the Target Location contains evidence of violations of the Target Offense. Accordingly, if the requested warrant is approved, I respectfully submit relevant and probative evidence will likely be recovered.

Id. at 11-12. In paragraph 26, Special Agent Lorenzen sought permission to seize computers, cellular phones, electronic storage media, and other electronic devices, including but not limited to a Samsung SM-G781U1, as described in Attachment B, located within the Target Location. Attachment B notes the warrant authorizes search and seizure of all evidence or property designed for use, intended for use, or used in committing or facilitating violations of the Target Offense, namely 18 U.S.C. § 2252(a)(5)(B), possession of child pornography. ECF No. 64-1 at 16.

On August 1, 2024, Magistrate Judge Paige J. Gossett issued a federal search warrant for the Target Location, Defendant's residence, and the Target Individual, Defendant. The search warrant was executed August 5, 2024. A Samsung SM-G781U1 phone was located on Defendant's nightstand, and Defendant identified it as his personal smartphone. Approximately 30 other electronic devices and storage media were also seized.

A separate federal search warrant was obtained for Defendant's cell phone. Artifacts showed the Kik application had been deleted from his phone on April 4, 2024, along with applications for Telegram, Mega, and Loki, all of which were referenced in Kik messages. The user dictionary on the Samsung phone included terms "joebidennnn" and joehoe12368@gmail.com, the email address used to register the Kik account. Hundreds of notifications from the Kik application were received by the device while the "joebidennnn69" account was active. There was no CSAM found on the device; however, the Kik account registered to joebidennnn69 contained approximately 220 unique files containing child pornography, as well as chats between joebidennnn69 and other users that were explicit in nature and related to CSAM material. Analysis of the Kik logs confirmed the account connected 958 times via Defendant's home Wi-Fi, 67 times via his Verizon account, and 48 times via VPN, which Defendant had installed on his phone.[4]

Defendant was indicted on June 10, 2025, and charged with ten counts of distribution of child pornography in violation of 18 U.S.C. § 2252(a). ECF No. 2. Arraignment and a detention

[4] Defendant now seeks to suppress the federal search warrant for his residence and person, as well as the separate federal search warrant for the forensic analysis of his Samsung cell phone, along with the fruits of both searches, to include the evidence described herein.

hearing were held June 12, 2025. ECF Nos. 13, 16. At the detention hearing, Special Agent Lorenzen testified. She acknowledged no CSAM was found on Defendant's phone, but discussed evidence of deletion of the Kik app and use of cloud storage:

Q. Special Agent Lorenzen, Mr. Phillips asked you if there were any artifacts related to CSAM or CSAM material found on the cellphone. There were apps that were located that were deleted, correct?
A. That is correct, yes.
Q. So, meaning that a Kik app, a Telegram app, a Sessions app, a Mega app had one time been downloaded and used on that phone?
A. Correct.
Q. And you haven't testified much about Telegram and Mega and Sessions, but since he asked you about that, in your training and experience, have you ever investigated cases where those apps are used to trade and distribute CSAM?
A. Yes, they are encrypted apps and they are foreign based so they are used a lot for distribution and receipt of child pornography.
Q. And also Mr. Phillips asked you about whether any of the files had been located and whether you had found CSAM on any device. In your training and experience, is it common for users and distributors of child pornography to use anonymous names in their social media platforms?
A. Yes.
Q. To avoid detection by law enforcement?
A. Correct.
Q. And are those sometimes multiple names used in order to facilitate the transfer of CSAM and to avoid detection?
A. Correct.
Q. And in your training and experience, do users of mobile apps like this sometimes delete their accounts after they have gratified themselves with the child pornography?
A. Yes.
Q. Okay. So, it is not unusual for you to find files that have been deleted?
A. Correct.

ECF No. 64-2 at 56-57. In addition, she testified it is "very common" to execute a search warrant and find no CSAM material or artifacts on any of the devices seized.

Q. [H]ow often is it that you . . . execute a search warrant and there is no CSAM material or artifacts on any of the devices found?
A. Oh, it is very common.

Q. Very common?
A. Yes.
Q. So, if there is a search of federal cases that we will find many, many cases where there is zero evidence on any devices after execution of a search warrant?
A. With the technology of cloud-based systems, yes, you are going to find that there – commonly there are not items actually saved on the camera roll of a phone.
Q. On device or artifacts. We can include the cloud because you don't have any CSAM material in a cloud that connects to Mr. May; is that right?
A. Well, we can connect the Kik accounts with him, which is essentially a cloud-based storage system for their photos and their content.
Q. Yeah, but what you are referring to is say Google Drive, Dropbox, that is generally referred to?
A. Correct.
Q. As, quote, unquote, the cloud?
A. All his CSAM and all his child pornography was still in his Kik account, correct.
Q. As far as the allegations are concerned, correct?
A. Yes.
Q. That's right. And so as far as execution of search warrants either through a cloud service or through a direct device, it is your testimony that it is very, very common to – have an execution of a search warrant in a federal case and there be no CSAM material or artifacts in any of that, either on the devices or in a cloud storage?
A. Of federal and state, yes.

Id. at 62-64. Special Agent Lorenzen testified "everything is related to, essentially, the Kik app in this case." *Id.* at 44.

STANDARD

A warrant affidavit must set forth particular facts and circumstances underlying the existence of probable cause, so as to allow the magistrate to make an independent evaluation of the matter. *Franks v. Delaware*, 438 U.S. 154, 165 (1978). Although there is a presumption of validity with respect to the affidavit supporting the search warrant, in certain narrowly defined circumstances, a defendant can attack a facially valid warrant. *Id.* at 171. Accordingly,

> where a defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

Id. at 155-56. If the defendant establishes the falsity or reckless disregard for truth by a preponderance of the evidence, and the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded. *Id.* at 156.

In the Fourth Circuit, to be entitled to a *Franks* hearing, the defendant must make a "dual showing . . . which incorporates both a subjective and an objective threshold component." *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990). First, the defendant must make a "substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit." *United States v. Allen*, 631 F.3d 164, 171 (4th Cir. 2011) (citing *Franks*, 438 U.S. at 155-56). Second, the information must be essential to the probable cause determination – if it is excluded and probable cause remains, no *Franks* hearing or relief is required. *Id.*

Franks also applies to intentional, material omissions from the affidavit supporting the search warrant application. *Colkley*, 899 F.2d at 301 ("*Franks* protects against omissions that are designed to mislead, or that are made in reckless disregard of whether they would mislead, the magistrate."). The defendant must show the omission is the product of a deliberate falsehood or of reckless disregard for the truth, so as to make the affidavit misleading, and the inclusion of the omitted information in the affidavit was necessary to the determination of probable cause. *United States v. Lull*, 824 F.3d 109, 117 (4th Cir. 2016). However, merely showing an intentional omission of a fact from a warrant affidavit does not fulfill *Franks'* requirements. *United States v. Tate*, 524

F.3d 449, 455 (4th Cir. 2008). The omission must be designed to mislead or made in reckless disregard of whether it would mislead. *Id.* The defendant must not only point out specifically the portion of the affidavit that is claimed to be false and give reasons why it is false, but he must also furnish "[a]ffidavits or sworn or otherwise reliable statements of witnesses" or explain their absence. *Id.* When relying on an omission, rather than a false affirmative statement, the defendant's burden increases even more. *Id.* While omissions may not be *per se* immune from inquiry, the affirmative inclusion of false information in an affidavit is more likely to present a question of impermissible official conduct than a failure to include a matter that might be construed as exculpatory. *Colkley*, 899 F.2d at 301.

There is a presumption of validity with respect to warrant affidavits, and the burden of making the necessary showing is a heavy one. *Tate*, 524 F.3d at 454.

DISCUSSION

Defendant now contends Special Agent Lorenzen's detention hearing testimony indicates her statements in the search warrant application affidavit at ¶ 9(e) were false and/or contained material omissions. He argues her allegedly contradictory testimony shows her statements in the search warrant affidavit were intentionally false or, at least, made with reckless disregard for the truth, and were integral to the probable cause determination.

1. <u>False or Omitted Statements in the Warrant Application</u>

Defendant challenges paragraph 9(e) of the affidavit as false or made with reckless disregard for the truth. He also discusses paragraphs 9(b), (c), and (d), 19, 24, and 25. Specifically, he argues the statements in the affidavit that individuals who collect child pornography rarely dispose of such material, potentially retaining it indefinitely, and may go to great lengths to conceal

it from discovery, conflict with her testimony at the detention hearing, when she agreed it is very common to execute a search warrant and find no CSAM material or artifacts on any devices. He also contends her statements, that it is common not to find CSAM on devices, were omitted from the search warrant affidavit, and constituted material omissions under *Colkley*.

The court finds Defendant has not made a preliminary showing of falsity, reckless disregard for truth, or omissions that were designed to mislead or made with reckless disregard of whether they would mislead the Magistrate Judge. There is no evidence whatsoever of intentional falsity or omission. *See United States v. Pulley*, 987 F.3d 370, 379 (4th Cir. 2021) ("A defendant must show both objective falsity and subjective intent of the affiant through concrete evidence. A defendant cannot rely on a purely subjective disagreement with how the affidavit characterizes the facts. Rather, there must be evidence showing that the statements at issue are *objectively false*.").

In addition, the court finds Defendant has not established reckless disregard by Lorenzen, as he has provided no facts indicating she subjectively acted with intent to mislead or with reckless disregard. *See United States v. Moody*, 931 F.3d 366, 371 (4th Cir. 2019) ("And here too, the defendant must provide facts—not mere conclusory allegations—indicating that the officer subjectively acted with intent to mislead, or with reckless disregard for whether the statements would mislead, the magistrate.").

Here, Defendant contends Lorenzen's statements in the affidavit are contradicted by her testimony at the detention hearing such that both cannot be true, and therefore the affidavit must have been written with reckless disregard for the truth. He also submits the statements made at the detention hearing were intentionally or recklessly omitted from the affidavit, as her testimony shows she believed it to be true that it is not uncommon for no CSAM to be found on recovered

devices after a search warrant is executed. The court finds this does not establish the requisite subjective intent or recklessness.

The affidavit statements in paragraph 9(e) that individuals who collect child pornography "rarely, if ever," dispose of it, and the statement at the detention hearing that it is common not to find any CSAM material on electronic devices after execution of a search warrant, are not mutually exclusive. The affidavit also states illicit materials may be saved on "movable media such as CDs, DVDs, flash memory, thumb drives, and removable hard drives," or sent to "third party image storage sites via the Internet." ECF No. 64-1 at 6. Paragraph 9(b) notes individuals who collect child pornography are likely to seek out like-minded individuals, either in person or over the internet, to share information and trade depictions of CSAM. Special Agent Lorenzen observed individuals involved with child pornography communicate with peer-to-peer chat and file sharing programs, among other avenues, and "chats" are sometimes saved on the user's computer or other digital storage media. *Id.* at 5-6.

Defendant attempts to cherry-pick one paragraph from Special Agent Lorenzen's hearing testimony he asserts is inconsistent with paragraph 9(e) of the affidavit, without taking into account the broader context of the testimony regarding the Kik account and the evidence already in HSI's possession. He focuses on her statements that it is very common not to find CSAM on devices seized after execution of a search warrant, ignoring her additional testimony that this is because of the advent of internet and cloud-based systems that allow users to store CSAM material in locations other than the physical devices. ECF No. 64-2 at 62-64. She testified all Defendant's CSAM remained in the Kik account and that "everything is related to, essentially, the Kik app in this case." *Id.* at 44.

When seeking the instant search warrant, Special Agent Lorenzen already had evidence someone at the IP address connected to the Target Location had used Kik, a peer-to-peer messaging app, to distribute CSAM. *Id.* at 8. She knew the IP address had been traced to the physical address at the Target Location, and had received the full Kik records, including hundreds of videos containing CSAM. *Id.* at 8-9. In Paragraphs 19, 24, and 25, the affidavit notes Lorenzen believed there was probable cause the Target Location contained evidence of violation of the target offense, including on electronic devices. These statements were correct. Even if no CSAM was found actually saved on a device, forensic evidence would likely connect the use of the device to the Kik distributions.

The court finds Defendant has not met his burden of making a preliminary showing of an intentional false statement, one made with reckless disregard for the truth, or material omissions made with intent to deceive or made in reckless disregard of whether they would deceive.

2. Probable Cause Determination

A district court may not hold a *Franks* hearing where, after stripping away the allegedly false statements, the truthful portions of the warrant application would still support probable cause. *Moody*, 931 F.3d at 371.

Defendant asserts paragraph 9(e), that CSAM is often possessed by collectors "indefinitely," should be replaced with Special Agent Lorenzen's testimony at the detention hearing that it is common not to find CSAM on electronic devices when executing a search warrant. Whether replaced or omitted entirely, the court finds paragraph 9(e) would not affect the probable cause determination for this search warrant to issue.

Probable cause is not a high bar, requiring only "a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Sanders*, 107 F.4th 234, 250 (4th Cir. 2024), *cert. denied,* 145 S. Ct. 1434, 221 L. Ed. 2d 557 (2025). The Fourth Circuit has affirmed a finding of probable cause when the affidavit allows an inference to be drawn that someone at the address accessed a URL whose content consisted of child pornography videos. See *United States v. Boysk*, 933 F.3d 319, 329 (4th Cir. 2019); *see also United States v. Vosburgh*, 602 F.3d 512, 526-27 (3d. Cir. 2010) (probable cause to search home when IP address clicked link purporting to contain child pornography). It has also upheld a search warrant relying on a single instance of accessing child pornography on a TOR website requiring affirmative steps to access such material. *Sanders*, 107 F.4th at 250.

Here, the affidavit in support of the search warrant contained significant evidence supporting probable cause that Defendant knowingly accessed CSAM material and transmitted explicit videos via the Kik messenger platform. Specifically, a CyberTip reported transmission of CSAM by Kik user joebidennnn69, and the AT&T 162 IP address was utilized to access and transmit the CSAM. State search warrants to Kik and AT&T resulted in evidence that the billing party for the 162 IP address was the Target Individual, Defendant, and the service address was the Target Location. The Kik account was registered to a Samsung phone and the 162 IP address was used to register the account. The contents of the Kik account contained 265 videos containing CSAM, and the user joebidennnn69 exchanged approximately 1,147 messages with other Kik users from March 30, 2024, to April 4, 2024. Sample chats included requests for CSAM with other users. Physical surveillance at the Target Location confirmed vehicles in the driveway registered to Defendant and with a SC Rep license plate confirmed to be registered to Defendant.

The court finds this is significant probable cause that there would be evidence of a child pornography offense at the Target Location. Even if the search did not result in location of actual CSAM material on electronic devices, probable cause existed there would be instrumentalities or other traces or evidence of such a crime. Defendant asserts "Special Agent Lorenzen had a duty to provide the magistrate judge with sufficient facts so she could make an independent evaluation of probable cause." ECF No. 78 at 17. The court agrees, and finds she did so. The court has no trouble concluding the affidavit supported a fair probability that evidence of instrumentalities of a child pornography offense would be found at the Target Location.

a. Staleness

Paragraph 9(e) of the search warrant affidavit discusses collection of CSAM in the context of "staleness concerns." ECF No. 64-1 at 6. The staleness inquiry is unique in the child pornography context. *See United States v. Krueger*, 145 F.4th 460, 465 (4th Cir. 2025); *Bosyk*, 933 F.3d at 330. "That is — due to (1) the tendency of individuals who intentionally access to collect child pornography, and (2) the material's electronic nature causing evidence of collection to be recoverable long after it is deleted — search warrants can reasonably be sustained months, and even years, after the events that gave rise to probable cause." *Sanders*, 107 F.4th at 251. Evidence of such activity would be recoverable for long periods of time, even after the pornographic material had been deleted from the computer. *Id.; see also Krueger*, 145 F.4th at 465 ("even if a defendant deletes a file from a hard drive or other computer media, a computer expert is still likely to retrieve . . . it through scientific examination of the computer.").

Paragraph 9(e) describes what is commonly referred to as the "collector's inference." Relying on the collector's inference requires a preliminary finding that the target is interested in

CSAM, rather than "the hypothetical inadvertent stumbler." *Krueger*, 145 F.4th at 465. Like the conduct in *Krueger*, in which the defendant repeated downloading and uploading, on multiple occasions over four days, full images of minors engaged in sexually explicit conduct, here an account tied to Defendant sent and received over 1000 messages discussing, seeking, and distributing CSAM from March 31 to April 4, 2024, as well as storing over 200 images of CSAM. The facts in the affidavit were such that the Magistrate Judge could infer Defendant was a "person interested in images of child pornography," and therefore the collector's inference could be applied. *See id.* at 466.

Defendant argues it was improper to rely on the "collector's inference" to avoid staleness, and instead Special Agent Lorenzen was required to tell the Magistrate Judge it is not uncommon to find no CSAM or artifacts, and failure to do so was a material omission. He contends no warrant would have issued if she had included this information.

However, the affidavit advised the Magistrate Judge HSI had already discovered the CSAM stored in the Kik account along with evidence tying the account to the IP address, cell phone, and Target Location. The CSAM remained in the Kik account, and the current billing party associated with the IP address where the Kik app was accessed was the Target Individual, with the service address of the Target Location. The warrant also sought property used in committing or facilitating violations of the Target Offense. Thus, even if the affidavit had included statements that it was common not to find CSAM on seized devices, there was probable cause agents would find a device "designed for use, intended for use, or used in committing or facilitating violations of the Target Offense." ECF No. 64-2 at 16. Accordingly, a sufficient basis was set forth in the

affidavit to find probable cause that evidence of the target offense would be found at the Target Location.

CONCLUSION

Defendant is not entitled to a *Franks* hearing, as he has not met his burden of showing a false statement made with intent or recklessness, or omitted statements intentionally or recklessly withheld. He has also failed to show the allegedly false or omitted statements were material to the probable cause determination. The court finds the search warrant was properly issued and will not suppress the evidence found as a result of its execution. Defendant's motion (ECF No. 64) is denied in full.

IT IS SO ORDERED.

s/Cameron McGowan Currie
CAMERON MCGOWAN CURRIE
Senior United States District Judge

Columbia, South Carolina
September 26, 2025