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 regarding the search of his cell phone, filed September 17, 2024. ECF No. 72. He asserts the search warrant was issued based on an affidavit containing statements the agent knew were false or at least 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. 75. It contends Defendant has failed to show a false statement was made intentionally or recklessly, and the probable cause determination did not depend on the challenged paragraph.

Defendant filed a reply, which he asserts applies to both the motion to suppress evidence from the search of the residence and the instant motion to suppress evidence from the search of the cell phone. ECF No. 78.

A hearing on motions to suppress was held September 24, 2025. This order follows.

BACKGROUND

The facts and background of this investigation are set forth in detail in the Order on Defendant's motion to suppress evidence derived from the search of his residence. ECF No. 83.

The findings in that Order also apply to the instant motion and therefore are incorporated herein by reference.

On August 5, 2024, a search warrant was executed on Defendant's residence. During that search, Defendant identified Target Phone #1, his personal Samsung SM-G781U1 smartphone. It was the same make and model as the phone used to register a Kik account on which someone distributed child pornography, or child sexual abuse material ("CSAM"). Homeland Security Investigators ("HSI") applied for a federal search warrant for Target Phone #1, the Samsung smartphone belonging to Defendant.

In support of the application for search warrant for Target Phone #1, HSI Special Agent Britton Lorenzen submitted an affidavit. The affidavit summarized the background of the investigation, including the CyberTip from Kik, the AT&T IP address beginning in 162, the state search warrants to Kik and AT&T, and Kik messages discussing trades of CSAM with other Kik users. ECF No. 72-1 at ¶¶ 13-19.

Agent Lorenzen stated, in the challenged paragraph:

> 11e. 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 ¶ 11(e).

On August 6, 2024, Magistrate Judge Paige J. Gossett issued a federal search warrant for Target Phone #1. Analysis revealed the Kik application was deleted from the 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 concerning CSAM. 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.

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 hearing were held June 12, 2025. ECF Nos. 13, 16. At the detention hearing, Special Agent Lorenzen testified. Defendant asserts her testimony at page 63, lines 21-25; and page 64, lines 1-3, contradicts paragraph 11(e) of her affidavit:

> Q. 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 63-64.

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). 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).

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

DISCUSSION

Defendant makes the same arguments here as in his motion to suppress evidence from the search of his home. He argues Lorenzen's testimony at the detention hearing shows her statement in the search warrant affidavit at paragraph 11(e) was intentionally false or, at least, made with reckless disregard for the truth, and was integral to the probable cause determination. Defendant asserts paragraph 11(e), that CSAM is often possessed by collectors "indefinitely," should be replaced with Special Agent Lorenzen's statements 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 11(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).

Here, the affidavit in support of the search warrant contained evidence that Defendant had 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 an AT&T IP address beginning 162 utilized to access and transmit the CSAM. State search warrants for Kik and AT&T resulted in evidence the billing party for the 162 IP address was the Defendant, and the service address was Defendant's residence. 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 from other users. Physical surveillance at the residence confirmed vehicles in the driveway registered to Defendant and with a SC Rep license plate confirmed to be registered to Defendant. During the search of the residence, Defendant admitted the Samsung phone was his personal cell phone, and it was located on his nightstand next to his CPAP machine. Target Phone #1 matched the model number of the phone used to register the Kik account joebidennnn69.

As noted by the Government, the affidavit included information that the Samsung cell phone was used to facilitate the offense – to upload CSAM and trade it with other Kik users. In addition, the affidavit noted child pornographers often maintain evidence of peer-to-peer communications, chats, and file share activity with others. ECF No. 75 at 12-13.

The court finds there was probable cause there would be evidence of child pornography offenses on Target Phone #1. Even if the search did not result in location of actual CSAM material, probable cause existed there would be evidence the phone was an instrumentality used to commit violations of laws concerning child pornography.

For the same reasons, the court finds the search warrant for the Target Phone #1 is not stale. 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 11(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. *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.

Forensic analysis could reveal not only deleted files or their remnants long after deletion, but also indirect evidence bearing on how the device had been used in the past. As described above, significant probable cause existed to justify issuing the search warrant for Target Phone #1.

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 for the Target Phone #1 was properly issued and will not suppress the evidence found as a result of its execution. Defendant's motion (ECF No. 72) is denied.

IT IS SO ORDERED.

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

Columbia, South Carolina
September 26, 2025