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

UNITED STATES OF AMERICA	)	CRIMINAL NO. 3:25-cr-778-CMC
	)	
v.	)	
	)	
ROBERT JOHN MAY, III,	)	
a.k.a. "joebidennnn69,"	)	
a.k.a. "Eric Rentling"	)	

Government's Response in Opposition to
Defendant's Motion to Suppress and Request for a *Franks* Hearing

Defendant Robert John May, III's motion to suppress evidence extracted from his phone by virtue of a search warrant for the contents of the phone issued on August 6, 2024, and for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), should be denied. To warrant a *Franks* hearing, a defendant must make a substantial preliminary showing of intentional or reckless falsehood (or intentional omission of material information) and must show that the corrected affidavit would not establish probable cause. *United States v. Moody*, 931 F.3d 366, 370 (4th Cir. 2019). May has not met this heavy burden. Contrary to his assertions, Special Agent (SA) Britton Lorenzen of Homeland Security Investigations (HSI) did not make knowingly false or recklessly misleading statements in her affidavit, and she did not omit material facts that, if included, would have negated probable cause. (*See* ECF No. 72 at 6-9). The challenged statement is accurate and consistent with later testimony; there is no evidence of intentionality or recklessness; and probable cause existed independent of the statement he attacks. The alleged omissions are likewise unsupported and immaterial. The Court should deny May's motion to suppress and his request for a *Franks* hearing.

I. Factual and Procedural Background

On May 27, 2024, Kik[1] reported to the National Center for Missing and Exploited Children (NCMEC) that on March 31, 2024, the account "joebidennnn69" distributed child pornography (hereinafter, "CSAM").[2] NCMEC reviewed the submission and flagged 50 files as CSAM. The CyberTip identified AT&T IP address 162.234.188.43, which geolocated[3] to West Columbia, SC. The South Carolina Attorney General's Office referred the tip to the Lexington County Sheriff's Department (LCSD) for investigation.

On June 27, 2024, the LCSD obtained a state search warrant compelling AT&T to produce subscriber information for the IP address. AT&T identified May as the subscriber, with the service address at his West Columbia residence.

That same day, the LCSD obtained a state warrant for the "joebidennnn69" Kik account. On July 12, 2024, Kik produced records confirming that the account was created on March 30, 2024, using a Samsung SM-G781U1 Android[4] phone and an unverified email address. Registration

---

[1] MediaLab/Kik is a social media company based out of Los Angles, California, that operates the Kik Messenger Application. Kik Messenger is a chat application that allows users to communicate and share videos and photographs both in group and person-to-person settings with other Kik users.

[2] Outside the legal system, NCMEC chooses to refer to child pornography images as Child Sexual Abuse Material (CSAM) to most accurately reflect what is depicted – the sexual abuse and exploitation of children.

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

[4] Kik Messenger stores the phone's make and model information using device identifiers and system information. When the 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 possibly IMEI), 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.

and subsequent activity were tied to the AT&T IP address at May's residence. Kik's production further showed that the account contained 265 CSAM videos and exchanged approximately 1,147 messages between March 30 and April 4, 2024, many involving the trade of CSAM.

Agents conducted surveillance of May's residence. They confirmed that the residence's Wi-Fi network was password-protected, meaning that any CSAM activity using that IP address required prior access to May's secure home network.

On August 1, 2024, United States Magistrate Judge Paige J. Gossett issued a federal search warrant to search May's residence. On August 5, 2024, HSI and the South Carolina Law Enforcement Division (SLED) executed the warrant. During the search, May identified his personal Samsung SM-G781U1 smartphone, located on his nightstand next to a CPAP machine.[5] It was the same make and model as the phone used to register the joebidennnn Kik account. On August 6, 2024, Judge Gossett issued a federal search warrant to search the contents of May's phone.

Forensic analysis of May's phone yielded several items of evidentiary value. First, the user dictionary included the term "joebidennnn" and the same email used to register the Kik account. Additionally, artifacts showed the installation and deletion of Kik, as well as Telegram, Mega, and Loki[6]—all applications referenced in Kik messages. All were deleted on April 4, 2024, within seconds of each other. Also, there were hundreds of Kik notifications received by May's device while the "joebidennnn69" account was active. Although May deleted the Kik application, Kik's

---

[5] An identical phone belonging to his wife was found on the opposite nightstand, but unlike May's phone, forensic analysis revealed no activity related to the CSAM scheme on her device.

[6] Loki Messenger, which re-branded as Session, is a decentralized anonymous messaging app that uses Signal's end-to-end encryption, Lokinet's onion routing or proxy requests, and the Loki Storage Server infrastructure. *See* https://loki.network/2019/12/13/rebranding-loki-messenger/.

records preserved 265 CSAM videos in the cloud. Analysis of Kik logs confirmed that the account connected 958 times via May's home Wi-Fi, 67 times via his Verizon account, and 48 times via a VPN. May had a VPN application installed on his phone.

On June 10, 2025, a federal grand jury indicted May on ten counts of distribution of child pornography, 18 U.S.C. § 2252A(a)(2), each tied to separate instances of distribution. In total, May distributed 479 CSAM videos over five days.

At his June 12, 2025, arraignment before United States Magistrate Judge Shiva V. Hodges, May requested a detention hearing under 18 U.S.C. § 3142(f). The Court ordered May detained pending trial. (ECF No. 20).

II. ARGUMENT

A. May is not entitled to a *Franks* hearing because he failed to make a substantial preliminary showing that law enforcement made a false statement, that the false statement was made knowingly and intentionally or with reckless disregard of the truth, or that the false statement was necessary to a finding of probable cause.

Franks hearings are "the exception, not the rule." *United States v. Allen*, 631 F.3d 164, 171 (4th Cir. 2011). A defendant must show (1) a false statement, (2) made knowingly and intentionally or with reckless disregard for the truth, and (3) necessary to the probable cause finding. *Moody*, 931 F.3d at 370. May fails on all three prongs.

To be entitled to relief or to even receive a *Franks* hearing, a defendant must make "a dual showing…which incorporates both a subjective and an objective threshold component." *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990). In other words, "*Franks*… has two distinct prongs, 'requir[ing] proof of both intentionality and materiality.'" *United States v. Pulley*, 987 F.3d 370, 376 (4th Cir. 2021) (quoting *United States v. Wharton*, 840 F.3d 163, 168 (4th Cir. 2016)).

To obtain a *Franks* hearing, a defendant must first carry a "heavy burden." *United States v. Haas* 986 F.3d 467, 474 (4th Cir. 2021).

1. No false statement was made.

May has not met his burden of showing the affidavit is objectively false. The required falsity showing "cannot be conclusory and must rest on affidavits or other evidence." *Moody*, 931 F.3d at 370. "As a result, the defendant cannot rely on a purely subjective disagreement with how the affidavit characterizes the facts." *Id*. There must be evidence showing the statement at issue is "objectively false." *Id*. Such evidence does not exist here.

In this motion, one nearly identical to a previous motion (ECF No. 64) filed related to the search of his residence, May's false-statement claim hinges on paragraph 11(e) of the affidavit and May's reading of a portion of SA Lorenzen's testimony during the detention hearing. Paragraph 11(e) states:

> 11. Based on my training, experience, and consultation with experienced agents assigned to investigate child sexual exploitation and child pornography, I know the following:
> …..
>
> 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 collections 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.

(ECF No. 72-1 at 10-11).

SA Lorenzen testified, consistent with her affidavit, that CSAM offenders often use multiple usernames, delete applications, and rely on cloud storage:

> 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).

She acknowledged that no CSAM or artifacts of CSAM were found on any of the devices seized from May's home; instead, she testified, "everything is related to, essentially, the Kik app in this case[.]" (*Id*. at 44). She added that it is not unusual "to find files that have been deleted." (*Id.* at 57). And she clarified that while it is common not to find CSAM *on the local storage of devices*, offenders typically retain access *through cloud accounts*:

> Q. All right. As far as you talk about some generalities a little bit about general cases of these things occur, how often is it that you prefer -- 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 that 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.

(*Id*. at 62-64).

SA Lorenzen's broad description of her training and experience investigating collectors of child pornography in paragraph 11(e) is neither false, nor contradicted by her subsequent testimony at May's detention hearing. Paragraph 11(e) of her affidavit states that "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 collections of illicit

materials." (ECF No. 72-1 at 11 (emphasis added)). "Dispose of" means to "to get rid of," "to deal with conclusively," or "to transfer to the control of another." *See* Merriam-Webster at https://www.merriam-webster.com/dictionary/dispose (Last Accessed Sept. 15, 2025). So when SA Lorenzen wrote that child pornographers rarely "dispose of" child pornography, she wrote that child pornographers rarely if ever conclusively get rid of, or completely lose access to or control over, the child pornography they consume.

That statement is not false. It is supported by SA Lorenzen's 20 years of training and experience. It is validated by a well-developed body of case law acknowledging "the tendency of individuals who possess or access with intent to view child pornography to collect such material and hoard it for a long time." *See, e.g.*, *United States v. Bosyk*, 933 F.3d 319, 331 (4th Cir. 2019) (quotation marks omitted); *United States v. Krueger*, 145 F.4th 460, 465 (4th Cir. 2025). It is consistent with SA Lorenzen's testimony at the detention hearing that "[w]ith the technology of cloud-based systems, . . . commonly there are not items actually saved on the camera roll of a phone." (ECF No. 64-2 at 63). And incidentally, it is consistent with what occurred here: no CSAM was found in the local storage of May's devices, but May's Kik account preserved 265 CSAM videos.

Child pornographers rarely completely get rid of their access to child pornography. One of the ways they retain it is by leaving the child pornography accessible through apps like Kik rather than saving the files on the internal storage of their phones. Contrary to May's claims, SA Lorenzen's testimony at the detention hearing does not show her affidavit is false.

Attempting to meet his burden, May assigns disproportionate weight to the final question and the final answer on re-cross, neither of which are a model of clarity:

> 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.

(ECF No. 64-2 at 63-64). His attempt to manufacture a falsity by divorcing SA Lorenzen's answer from the balance of her testimony should be rejected. Throughout the exchange, the agent repeatedly pointed defense counsel back to Kik and similar cloud-based platforms as a place where May and child pornographers like him store and maintain child pornography. (*Id*. at 63 ("With the technology of cloud-based systems, yes, you are going to find that there -- commonly there are not items actually saved on the cameral roll of a phone."); *id.* ("Well, we can connect the Kik accounts with him, which is essentially a cloud-based storage system for their photos and their content."); *id.* ("All of his CSAM and his child pornography was still in his Kik account")). Taken in context, her final answer, at the end of 53 pages of questioning, is at most imprecise. And "[m]ere imprecision does not, by itself, show falsity." *Moody*, 931 F.3d at 372.

May has failed to show SA Lorenzen made an objectively false statement in the affidavit. For that reason alone, the motion should be denied.

2. May has made no showing of intentionality or recklessness.

Even assuming that paragraph 11(e) was inaccurate, May offers no evidence that it was knowingly or recklessly false. "An innocent or even negligent mistake by the officer will not suffice" to make the required intentionality showing. *Moody*, 931 F.3d at 371. Instead, "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." *Id*. May has again failed to meet his burden.

There is no evidence that SA Lorenzen intentionally or recklessly misled the U.S. Magistrate Judge. On the contrary, SA Lorenzen was honest and candid in both the affidavit and at the detention hearing. Paragraph 11 is a broad summary of SA Lorenzen's experience investigating CSAM offenses over a 20-year career. Paragraph 11(e) described how individuals who collect child pornography protect their CSAM using a variety of methods, including using electronic devices and "send[ing] it to third party image storage sites via the Internet." (ECF No. 72-1 at 11). As explained above, there is no inconsistency between the affidavit and SA Lorenzen's testimony. At most, there is a lack of precision in one answer to a question at the end of 53 pages of testimony. "Given the lack of precision" in that single statement, the Court "cannot reasonably infer that [SA Lorenzen] acted with intent to mislead or with reckless disregard of whether the statements would mislead." *See Moody*, 931 F.3d at 372. May failed to make a substantial showing to prove intentionality and he is not entitled to a *Franks* hearing. The motion should be denied.

3. Probable cause to search May's phone did not depend on paragraph 11(e).

May has not shown the allegedly false statement was material because the removal of paragraph 11(e) neither diminishes a finding of probable cause, nor renders the information stale. A defendant seeking a *Franks* hearing "must show materiality—that is, that the false statements were necessary to the finding of probable cause." *Moody*, 931 F.3d at 371 (quotation marks omitted). "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." *Id.* "This limitation reflects the ultimate purpose of *Franks*: to prevent the admission of evidence obtained pursuant to warrants that were issued only because the issuing magistrate was misled into believing that there existed probable cause." *Id.* (quotation marks omitted).

Even without paragraph 11(e), the affidavit established probable cause to search May's phone:

- Cell phones have advanced capabilities, including internet browsing, text and email, photography, video, and data file storage, all of which are relevant to a Kik distribution scheme. (*See* ECF No. 72-1 at ¶ 12).

- Cell phones are used to communicate with others by voice, direct connect, text message, and email. (*Id.* ¶ 12).

- Cell phones store data such as names and addresses, search the internet, and capture audio, image, and video files. (*Id.* ¶ 12).

- Kik is a social media platform that allows users to communicate over a chat application and to share photographs and videos. (*Id.* ¶ 13, fn. 2).

- Kik is an application utilized on mobile phones that stores information about the phone to optimize the performance of the application. (*Id.* ¶ 17, fn. 4).

- Kik sent a CyberTipline Report to NCMEC stating that a user located at IP address 162.234.188.43 uploaded child pornography on March 31, 2024. (*Id.* ¶ 13, 15).

- The account used to traffic in the CSAM bore the name of a politician, and the owner of the account was also a politician. (*Id.* ¶ 13, 20, 25).

- The conduct was repeated and persistent. In the CyberTip, NCMEC identified 50 CSAM distributions from the user sent on the Kik platform to other users. (*Id.* ¶ 14).

- The videos shared by the user included a CSAM video showing an eight-year-old female victim being made to perform oral sex on an adult male. Another video showed an adult male using his penis to penetrate a toddler girl who appeared to be about three years old. (*Id.* ¶ 14, 17).

- Over a five-day period, the target Kik user sent 1,147 messages online through the Kik application. That content included at least 265 CSAM videos. Texts of the conversations were included in the affidavit, which showed the user's repeated interest in collecting CSAM. (*Id.* ¶ 18, 19).

- The IP address used to share the CSAM was geolocated to West Columbia, South Carolina. (*Id.* ¶ 15).

- A state search warrant served on AT&T revealed that the billing party for the IP address account was May and that the service address was May's home address. (*Id.* ¶ 16).

- A cell phone was also used to facilitate the offense. Kik records showed that a Samsung SM-G781U1 Android smartphone was used to register the account. The same IP address

registered to May's home was used to register the joebidennnn69 Kik account that uploaded CSAM on March 31, 2024. (*Id.* ¶ 17).

- Property records corroborated that May, the subscriber of the IP address, owned the house. (*Id.* ¶ 23).
- DMV records also corroborated that the same person, May, was associated with the house. (*Id.* ¶ 24).
- Law enforcement surveillance on multiple occasions confirmed that May owned the home and open-source information confirmed he lived there with his wife and two minor children. (*Id.* ¶ 20, 21, 25).
- The cell phone sought to be searched matched the phone that was used to register the Kik account. When searching May's house on August 5, 2024, agents located a Samsung SM-G781U1 smartphone, which matched the make and model number used to register the Kik account. (*Id.* ¶ 17, 29, 30).
- The Samsung smartphone was recovered from May's nightstand next to a CPAP machine, and May acknowledged that it was his personal phone. (*Id.* ¶ 30).
- Child pornographers often collect and keep material that show interest in minor children and are relevant to 404(b) and Rule 414 evidence. (*Id.* ¶ 11(a)).
- Child pornographers often maintain evidence of peer-to-peer communications, chats, and file share activity with others who share such files. (*Id.* ¶ 11(b)).
- Child pornographers often collect written material that relates to child erotica or an interest in children. (*Id.* ¶ 11(c)).
- Child pornographers often maintain lists of others, including online, who they may be able to contact to collect additional CSAM material. (*Id.* ¶ 11(d)).

Even without paragraph 11(e), the magistrate judge still knew that someone used May's home IP address to register a Kik account using the same make and model of phone that May owned that was then used to upload child pornography to the internet via the same IP address. She knew a phone matching that make and model was found on May's nightstand next to his CPAP machine. She knew that a smartphone application was used through May's home internet to facilitate the child pornography scheme, that more than 1,147 messages were exchanged over a five-day period, and that it is well accepted in child pornography investigations "that digital media

files persist for a long time." *Bosyk*, 933 F.3d at 331. And she could infer that May, the owner of the phone, was a person "involved with child pornography" who "collect[s] child pornography," and was therefore likely to possess "other sexually explicit materials related to [his] interest in children"; communicate with like-minded individuals through peer-to-peer communications, chats, and emails that might be saved on digital storage media; produce or collect written material on sexual activity with minors; and maintain names and contact information of others he may be able to contact to collect additional CSAM. (*See* ECF No. 72-1 at 10-11). This "collector inference" provided a "substantial basis" for concluding that the search of the phone would uncover evidence of wrongdoing, notwithstanding the several months that had elapsed since the CSAM distribution in March and April 2024. *See Krueger*, 145 F.4th at 466 (reasoning the collector inference applied because the conduct described in the affidavit, like here, occurred across multiple days).

Assuming May can show the challenged portion of paragraph 11(e) is false, it would not undermine the probable cause supporting the search of his phone for evidence tying May to the possession of child pornography such as text messages, peer-to-peer messages, or emails. The evidence contained in the affidavit, even absent paragraph 11(e), created more than a fair probability that contraband, or evidence that May's phone was used to store and send contraband and evidence of that storage, would be found inside the phone, satisfying the "low bar" of probable cause. *See Nazario v. Gutierrez*, 103 F.4th 213, 229 (4th Cir. 2024).

May also seems to acknowledge the limited significance of paragraph 11(e) in determining probable cause when he argues that it "is boilerplate language…not based on the facts and circumstances at hand." (ECF No. 72 at 3-4). The single paragraph at issue cannot be both merely "boilerplate," yet necessary to establish probable cause. It was a summary description of how, in

SA Lorenzen's training and experience, child pornographers protect their CSAM. And its removal does not destroy probable cause that evidence of possessing child pornography would be found within May's phone. Any falsity was therefore immaterial, and the motion should be denied.

B. May is not entitled to a *Franks* hearing because he failed to make a substantial showing that material information was intentionally omitted from the affidavit.

"*Franks* protects against omissions that are designed to mislead, or that are made in reckless disregard of whether they would mislead, the magistrate." *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990) (emphasis omitted). But "[a] defendant requesting a *Franks* hearing based on claims of omissions faces an even higher evidentiary burden than when he bases his claims on false statements." *Moody*, 931 F.3d at 374. In that case, the defendant "must provide a substantial preliminary showing that (1) law enforcement made an omission; (2) law enforcement made the omission 'knowingly and intentionally, or with reckless disregard for the truth,' and (3) the inclusion of the omitted evidence in the affidavit would have defeated its probable cause." *Haas*, 986 F.3d at 474.

1. May fails to show *evidence* was intentionally omitted from the affidavit.

May alleges SA Lorenzen made the following omissions:

> (1) "As for staleness concerns, it is very, very common to execute a search warrant on a suspected possessor of child CSAM and discover no CSAM or CSAM artifacts in his home, on his electronics or in his cloud storage accounts."

(ECF No. 72 at 8). His *Franks* claim fails twice-over at a threshold level. First, "*Franks* concerns omissions of fact." *United States v. Fritzinger*, No. 4:20-cr-81, 2024 WL 2868987, at *9 (E.D.N.C. June 6, 2024). And second, it asks whether "the inclusion of the omitted *evidence* would defeat the probable cause in the affidavit." *Haas*, 986 F.3d at 474. But May's purported omission is

neither facts nor evidence. It is a manufactured mischaracterization of SA Lorenzen's testimony about her training and experience.

May's argument misrepresents SA Lorenzen's testimony and ignores the nuanced distinction she consistently drew between finding child pornography saved on a local device and finding it in a cloud-based system such as Kik. The alleged "omission" was omitted from the affidavit because it is not a true statement. As discussed above, SA Lorenzen testified that CSAM may not be found on "the camera roll of a phone," but it is often found in cloud-based storage systems, as it was here. (ECF No. 64-2 at 63). While SA Lorenzen acknowledged no CSAM was found in a search of a "Google Drive" or "Dropbox" account, she clarified CSAM was "still in [May's] Kik account," "which is essentially a cloud-based storage system." (ECF No. 64-2 at 63). That, SA Lorensen testified, is a common pattern with child pornographers, one that happened to bear out in May's own conduct.

But even if the Court were to remove SA Lorenzen's answer to the last question from its context and construe her entire testimony to be 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," May would still fail to show that she omitted facts or evidence relating to probable cause from the affidavit. SA Lorenzen's answer to that question was related to her experience in similar cases; she did not testify about whether "a search of the May home" or "of any cloud storage associated with Mr. May" would result in the discovery of CSAM or CSAM artifacts. May fails to show evidence was intentionally omitted from the affidavit.

2. Even if information was intentionally omitted, it was not material to a finding of probable cause.

In assessing materiality, courts "insert the facts recklessly or intentionally omitted, and then determine whether or not the corrected warrant affidavit would establish probable cause."

Wharton, 840 F.3d at 169 (quotation marks and alteration omitted). "If the corrected warrant affidavit establishes probable cause, there is no *Franks* violation." *Id.* (quotation marks omitted). May argues that the portion of SA Lorenzen's testimony that was omitted from her affidavit should be added to the affidavit to determine whether the omission was material. In doing so, May suggests that paragraph 11(e) should be read to say that it is "very, very common to execute a search warrant on a suspected possessor of CSAM and discover no CSAM or CSAM artifacts in his home, on his electronics or in his cloud storage accounts." As previously noted, this misrepresents SA Lorenzen's testimony and deprives it of necessary context and the balance of the agent's responses at the hearing. But even if this information was deliberately omitted from the search warrant, her testimony in its entirety should be inserted into the warrant to determine materiality, not merely May's preferred mischaracterization of her testimony. Therefore, if the affidavit were to be supplemented with SA Lorenzen's entire testimony, paragraph 11(e) would include at the end: "Although it is common in today's age of cloud-based storage systems not to find child pornography saved on local devices, it can often be found in a cloud-based storage system or other digital location."

The amended affidavit would not preclude a magistrate judge from finding probable cause to believe that evidence of child pornography possession aside from the CSAM files themselves could be found in May's phone. Even if the issuing judge were notified that evidence related to child pornography may not be found on the camera roll of a phone, as set forth above, the affidavit amply establishes a fair probability that May's phone would contain evidence of communications related to the possession of child pornography; records related to the ownership, operation, or creation of the Kik account at issue and similar evidence related to cloud-based platforms like Kik;

as well as evidence of user attribution for May's phone during the time period described in the affidavit.

Even if the first sentence of paragraph 11(e) were removed and the new sentence were added, the substantial basis for probable cause would remain the same.

III. CONCLUSION

For the above reasons, the Government respectfully requests that this Court deny May's motion to suppress evidence seized from his phone and for a *Franks* hearing.

Respectfully submitted,

BRYAN P. STIRLING
UNITED STATES ATTORNEY

By: s/Scott Matthews
J. Scott Matthews (Fed. ID # 13779)
Elliott B. Daniels (Fed. ID # 11931)
Assistant United States Attorneys
United States Attorney's Office
1441 Main Street, Suite 500
Columbia, SC 29201
Telephone 803-929-3000
Facsimile 803-256-0233
Email: Jonathan.Matthews2@usdoj.gov
Email: Elliott.Daniels@usdoj.gov

Austin M. Berry
Trial Attorney
Child Exploitation & Obscenity Section
Criminal Division
United States Department of Justice
1301 New York Ave. NW
Washington, D.C. 20005
Email: Austin.Berry2@usdoj.gov

September 23, 2025