APPENDIX

APPENDIX TABLE OF CONTENTS

No. 22-2773

IN THE
UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

PAUL S. OSTERMAN,
Defendant-Appellant.

On Appeal from the United States District Court for the Eastern District of Wisconsin,
No. 1:21-cr-00110 – **William C. Griesbach,** *Judge*.

ARGUED NOVEMBER 29, 2023 — DECIDED AUGUST 1, 2024

AMENDED ON PETITION FOR REHEARING OCTOBER 23, 2024

Before RIPPLE, SCUDDER, JACKSON-AKIWUMI, *Circuit Judges*.

JACKSON-AKIWUMI, *Circuit Judge*. A detective in Oneida County, Wisconsin, applied for a warrant so he could place a GPS tracker on Paul Osterman's truck. After monitoring the truck—a search within the meaning of the Fourth Amendment—authorities prosecuted Osterman for sex trafficking a child. Osterman later learned that some information the

detective included in the affidavit seeking the warrant was in- correct. To Osterman, this meant the affidavit failed to establish probable cause for the search, so he asked the district court to suppress the fruits of the search.

After an evidentiary hearing, the district court held that the affidavit established probable cause despite its inaccuracies. The court therefore denied Osterman's motion to sup- press, and Osterman appeals. We agree with Osterman that the detective acted recklessly when he failed to correct the affidavit. But we have taken an independent look at the affidavit, as we must, and we conclude that it establishes probable cause even without the incorrect information. For that reason, we are compelled to affirm.

I

MeetMe.com is an online-dating website. When the web- site's administrators suspect that MeetMe users are targeting children for sexual exploitation, the administrators must file a "CyberTip" with the National Center for Missing and Exploited Children. *Frequently Asked Questions*, NAT'L CTR. FOR MISSING AND EXPLOITED CHILDREN, https://report.cybertip.org/faqs (last visited July 17, 2024). The center manages a centralized system for reporting online child exploitation, and when a CyberTip involves a child in immediate or impending harm, it forwards the tip to law enforcement for investigation. *Id.*

In this case, Detective Chad Wanta of the Oneida County Sheriff's Office received eight CyberTips. The tips reported strikingly similar instances of misconduct on MeetMe.com between January 2018 and December 2019. All the users had MeetMe

usernames beginning with the letter J, including variations of "Jared," "Jones," and "Jacob." In addition, each user sent messages on the website looking for "a much younger girl" and offering money to meet with one for sexual encounters.

The CyberTips further disclosed that all but one of the messages originated from MeetMe users who used wireless internet signals hosted by companies in Rhinelander, Wisconsin. Specifically, two tips noted the user accessed publicly available wi-fi provided by a McDonalds at 25 S. Stevens Street. Three tips reported the user accessed public wi-fi offered by a laundromat called Modes, Machines & More LLC, at 2100 Lincoln Street. And two other tips explained the user accessed a private wi-fi network hosted by Northwoods Communications Technologies LLC (now "Northwoods Connect – High Speed Internet"), an internet provider then located at 2151 N. Chippewa Drive.

In sum, seven of the eight CyberTips Detective Wanta received involved similar usernames, sexual propositions, locations, and wi-fi access. The eighth tip was different, but not by much: it linked the suspect to a wi-fi hotspot not in Rhine- lander, Wisconsin, but in Hillside, Illinois.

After receiving the CyberTips, Detective Wanta launched an investigation. He targeted the Rhinelander companies listed in the tips. Hoping to identify the MeetMe user who accessed Northwoods Communications' private wi-fi network, Detective Wanta interviewed the owner and operator of Northwoods Communications: Osterman. Osterman told Detective Wanta it was impossible to identify the user by the IP address provided in the CyberTip because the IP address could have been used by any

one of his company's 400 customers.

Undeterred, Detective Wanta shifted his focus to a MeetMe user who called himself Brad Jones. The relevant CyberTip detailed an instant message exchange between Jones and a child that occurred on July 4, 2019. Near the beginning of the exchange, Jones apparently thought the person was older and offered her money to help locate a younger girl. But later, Jones realized he was talking to a twelve-year-old girl who lived in Chicago, Illinois. He told the girl he would drive from Wisconsin to Chicago that night so they could meet. Authorities later learned from the child victim that, when Jones reached Chicago on July 4, he paid her twenty- five dollars in exchange for sex. Law enforcement subsequently subpoenaed a Holiday Inn in Hillside, Illinois, for a list of guests who stayed in the hotel on July 5. Osterman was among them.

By this point in the investigation, Osterman's profile had popped up twice: at the Hillside Holiday Inn and in relation to Northwoods Communications. But his connection to the investigation did not end there. A few months after the Jones incident, someone called the Rhinelander Police Department to report a suspicious man who allegedly had been sitting in a black pickup truck for several hours. Officers who arrived on the scene discovered Osterman sitting in the truck using two tablets and a cell phone within wi-fi range of Modes, Ma- chines & More LLC—the same laundromat whose wi-fi had been accessed by a MeetMe user in the CyberTips. When the officers spoke with Osterman, he told them he owned an internet company and was testing his competitor's internet speed.

Believing these connections to be more than coincidence, Detective Wanta secured a search

warrant to track Osterman's truck by GPS. The GPS data showed Osterman's truck was parked for several hours on different days at the McDonalds and laundromat described in the CyberTips. The data also showed the truck was parked around other public wi-fi locations in northern Wisconsin during the investigation.

These discoveries aided the investigation, but the inaccuracies in the affidavit Detective Wanta submitted to secure the warrant did not. In one paragraph, he wrongly suggested that Jones had messaged the underaged girl through the Hillside Holiday Inn's wi-fi on July 4. In reality, no part of the conversation took place through the hotel's wi-fi; instead, Jones merely connected to it on July 5, not July 4. In another para- graph, Detective Wanta wrote that a suspect accessed a wi-fi hotspot owned by the Rhinelander McDonalds. He failed to add that this suspect was linked to a person based in Texas. Detective Wanta testified that he discovered the Texas association after he submitted the affidavit the first time, but he failed to update the affidavit despite having an opportunity to do so before each of the three times he renewed the war- rant.

These inaccuracies led Osterman to file a motion to sup- press after a grand jury indicted him on three charges: one count of sex trafficking a child in violation of 18 U.S.C. §§ 1591(a)(1), (b)(1), and (c); one count of using a computer to persuade and induce/entice a minor to engage in unlawful sexual activity in violation of 18 U.S.C. § 2422(b); and one count of travel with intent to engage in illicit sexual activity with a minor in violation of 18 U.S.C. § 2423(b).

The district court held a *Franks* hearing on

Osterman's motion to suppress. *See Franks v. Delaware,* 438 U.S. 154 (1978). Detective Wanta appeared as the sole witness. He testified about the Jones investigation and admitted that his affidavit contained errors. When asked about the paragraph describing how Jones sent messages through the Hillside Holiday Inn's wi-fi on July 4, 2019, Detective Wanta admitted that information was incorrect because Jones merely accessed the hotel's wi-fi the next day, on July 5. The more accurate account, he agreed, was that Jones started messaging on July 4, but from a hotspot in Antigo, Wisconsin. The mix-up was inadvertent, Detective Wanta testified. Before receiving the CyberTips, another agent told him Jones communicated with the minor victim through wi-fi signals hosted by the Hillside Holiday Inn. In addition, the CyberTips contained multiple files but Detective Wanta did not look at every single file because, as a Wisconsin officer, he did not expect to investigate a Chicago-area incident. In the end, Detective Wanta conceded that he could have caught the error in the date had he reviewed his records more thoroughly.

The same was true for the second error. Detective Wanta testified that, after submitting the affidavit, he learned one of the MeetMe users linked to Rhinelander was based in Texas. Instead of updating the affidavit with this information, however, he used it—unrevised—to renew the warrant three times. Detective Wanta maintained that he never intentionally lied to or misled anyone.

After the *Franks* hearing, the district court denied Oster- man's motion to suppress. In its ruling, the court credited Detective Wanta's testimony and accepted the detective's assertion that the

misstatements found their way into the affidavit by mistake. The court also weaved certain facts together into a hypothetical affidavit to determine whether probable cause existed, and the court concluded it did. After losing the sup- pression battle, Osterman pled guilty to child sex trafficking and received a sentence of 300 months' imprisonment.

II

"There is a presumption of validity with respect to the affidavit supporting the search warrant." *Franks*, 438 U.S. at 171. But a defendant may overcome this presumption if the defendant can prove a *Franks* violation occurred. *See United States v. Edwards*, 34 F.4th 570, 580 (7th Cir. 2022). A *Franks* violation is established "when the defendant shows by a pre- ponderance of the evidence that (1) the affidavit in support of the warrant contains false statements or misleading omissions, (2) the false statements or omissions were made deliberately or with reckless disregard for the truth, and (3) prob- able cause would not have existed without the false statements and/or omissions." *United States v. Williams*, 718 F.3d 644, 647-48 (7th Cir. 2013) (citing *Franks*, 438 U.S. at 155-56).

When we are asked to review a district court's factual findings in the above inquiry, including findings related to deliberate or reckless disregard for the truth, we evaluate the findings for clear error. *See United States v. Spears*, 673 F.3d 598, 604 (7th Cir. 2012). The factual findings will stand unless we are "left with the definite and firm conviction that a mistake has been committed." *Williams*, 718 F.3d at 649 (quoting *United States v. Sauerwein*, 5 F.3d 275, 278 (7th Cir. 1993)). By contrast, we undertake de novo review of legal determinations, which includes

the question of whether an affidavit establishes probable cause without the false statements or omissions. *Id.* at 649.

The parties do not dispute that the affidavit in this case contained false statements or misleading omissions. So our inquiry focuses on the second and third elements necessary to prove a *Franks* violation. To prove such a violation, and to pre- vail on his suppression motion by extension, Osterman must demonstrate that Detective Wanta knowingly, intentionally, or recklessly made false statements or misleading omissions in the warrant affidavit. *See United States v. Norris*, 640 F.3d 295, 300-01 (7th Cir. 2011). But that is not all. Osterman also must demonstrate that the false statements or misleading omissions are material. *Id.* at 301.

As for the second *Franks* element, we conclude that Detective Wanta knowingly, intentionally, or recklessly left false or misleading information about one of the CyberTips in the warrant affidavit. The district court found the opposite: it held that Detective Wanta "did not knowingly, intentionally, or with reckless disregard for the truth, include a false statement in his search warrant affidavit." On the record before us, this factual finding amounts to clear error because it is evident Detective Wanta acted recklessly in refusing to update the warrant once he knew that one of the MeetMe users was based in Texas. He admitted that one of the suspects was linked to Texas and he could have updated the affidavit since he had the accurate information before renewing the warrant. When an officer continues a course despite having "serious doubts as to the truth" or "obvious reasons to doubt" the ac- curacy of his assertions, that is a reckless disregard for the truth.

Betker v. Gomez, 692 F.3d 854, 860 (7th Cir. 2012) (internal citations omitted). There is no question that Detective Wanta's conduct falls into this category.

By contrast, we affirm the district court's conclusion that Wanta did not include the incorrect information about the Holiday Inn wi-fi (the extent and date of Jones's access) recklessly or intentionally. The record does not clearly support that Wanta had "serious doubts as to the truth" or an "obvious reasons to doubt" the veracity of his report about the Holiday Inn. *See id.* Rather, it appears to have been a negligent mistake. The district court therefore made no error in this regard.

As for the third *Franks* element, our inquiry is whether the inaccuracies in the affidavit are material to the probable cause finding. If they are, as Osterman insists, his suppression motion should have been granted; if they are not, the district court was right to deny the suppression motion. We consider this question of materiality afresh in our de novo review and therefore give no weight to the district court's analysis. *See United States v. Taylor,* 63 F.4th 637, 651-52 (7th Cir. 2023). We are mindful that "the task of the issuing judge is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him," the issuing judge believes "there is a fair probability that contra- band or evidence of a crime will be found in a particular place." *Id.* at 651 (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)) (internal citations omitted). At the end of the day, we will not disturb the issuing judge's probable cause determination so long as the affidavit establishes probable cause after we "eliminate the alleged false statements," *Betker*, 692 F.3d at 862, and add in the exculpatory evidence that

had been omit- ted, *Rainsberger v. Benner*, 913 F.3d 640, 643 (7th Cir. 2019). The resulting hypothetical affidavit then becomes the object of our probable cause analysis. *See id.*

The parties have not provided us any cases that establish whether courts must eliminate non-reckless misstatements, as opposed to only intentional or reckless misstatements, in con- structing the hypothetical affidavit. But that makes no difference here. When we eliminate the false statement about the Holiday Inn wi-fi access and add in the omitted fact that one of the Cyber Tips was linked to a Texas user, the hypothetical affidavit still establishes probable cause. The hypothetical affidavit identifies Osterman not only as a resident of Rhine- lander, Wisconsin, but also as the owner of Northwoods Connect, a Rhinelander company that was used multiple times by the MeetMe users suspected of targeting children for sexual exploitation. The hypothetical affidavit also notes that Detective Wanta interviewed Osterman in connection with the investigation since he owned the company. From there, the affidavit goes on to explain that Rhinelander police officers investigated a suspicious man who had been sitting in his vehicle for hours. The man of course turned out to be Osterman, who was sitting in his vehicle using two tablets and a cell phone within wi-fi range of one of the establishments referenced in the CyberTips. And perhaps most damning of all, Osterman stayed at the Hillside Holiday Inn on July 5, a day after a MeetMe user said he planned to travel from Wisconsin to Chicago for sexual activity with a child in the middle of the night.

This information is enough to support a probable cause finding. It is true that adding the detail about

the user linked to Texas could have suggested there was more than one suspect. But the judge issuing the warrant did not have to be certain Osterman was the *only* suspect; the judge only needed enough information to formulate a substantial belief that *Osterman* had committed a crime and evidence of the crime would be found by monitoring his truck. *See United States v. Parra*, 402 F.3d 752, 764 (7th Cir. 2005) ("So long as the totality of the circumstances, viewed in a common sense manner, reveals a probability or substantial chance of criminal activity on the suspect's part, probable cause exists." (internal citation omitted)). The affidavit provided at least that information if not more absent the misleading omission, thereby establishing probable cause. *See Betker*, 692 F.3d at 862.

Thus, although we agree with Osterman that Detective Wanta acted recklessly when he failed to update the warrant affidavit about the user linked to Texas, suppression of the fruits of the GPS search remains beyond reach to Osterman because the false statement and misleading omission in the affidavit are immaterial. Probable cause existed even without them.

AFFIRMED.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,
Plaintiff,

v. Case No. 21-CR-110

PAUL S. OSTERMAN,
Defendant.

ORDER DENYING MOTION TO SUPPRESS

On May 19, 2021, a federal grand jury returned a three-count indictment charging Defendant Paul S. Osterman with the following: Count 1 – Sex Trafficking of a Child, in violation of 18 U.S.C. §§ 1591(a)(1) and (b)(1); Count 2 – Using a Computer to Persuade and Induce/Entice a Minor to Engage in Unlawful Sexual Activity, in violation of 18 U.S.C. § 2422(b); and Count 3 – Travel with Intent to Engage in a Sexual Act with a Minor, in violation of 18 U.S.C. § 2423(b). Presently before the Court is Osterman's motion to suppress evidence obtained through a warrant authorizing police to install on his truck a GPS tracking device. Osterman requested an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), to establish that the warrant was based on intentional falsehoods. Upon consideration of Osterman's motion and the government's response, the Court concluded that a hearing was warranted and conducted such a hearing on January 20, 2022. Having now considered the evidence

presented and for the reasons that follow, Osterman's motion is denied.

GPS Devices, Search Warrants, and *Franks* Hearings

"[T]he Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *United States v. Jones*, 565

U.S. 400, 404 (2012). Absent exigent circumstances or other exception recognized by the Court, a warrant signed by a judge or magistrate must be obtained to authorize a search. *California v. Acevedo*, 500 U.S. 565, 580 (1991); *see also United States v. Brewer*, 915 F.3d 408, 413 (7th Cir. 2019) (noting "GPS vehicle monitoring generally requires a warrant . . . ."). Law enforcement obtained such a warrant here, but Osterman contends the warrant is invalid because police intentionally or recklessly used false information to obtain it.

In *Franks v. Delaware*, the Supreme Court held that, where a defendant makes a substantial preliminary showing that a false statement was knowingly and intentionally, or with reckless disregard for the truth, included by the affiant in a search warrant affidavit and the statement was necessary to finding probable cause, the Fourth Amendment requires that a hearing, which has become known as a *Franks* hearing, be held at the defendant's request. If at such a hearing the defendant succeeds in proving that the warrant was based on such information, the warrant is deemed invalid and any evidence obtained thereby is suppressed. 438 U.S. at 155–56; *United States v. McMurtrey*, 704 F.3d 502, 508 (7th Cir. 2013).

A *Franks* hearing is not held on the defendant's mere request. 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, and . . . the allegedly false statement is necessary to the finding of probable cause." *Franks*, 438 U.S. at 155–

56. As the court explained in *McMurtrey*, "It is relatively difficult for a defendant to make the 'substantial preliminary showing' required under *Franks*. Allegations of negligent or innocent mistakes do not entitle a defendant to a hearing, nor do conclusory allegations of deliberately or recklessly false information. The defendant must identify specific portions of the warrant affidavit as intentional or reckless misrepresentations, and the claim of falsity should be substantiated by the sworn statements of witnesses." 704 F.3d at 509 (citing *Franks*, 438 U.S. at 171). "To obtain a hearing, the defendant must also show that if the deliberately or recklessly false statements were omitted, or if the deliberately or recklessly misleading omissions included, probable cause would have been absent." *Id.*

The Search Warrant Affidavit

The affidavit submitted in support of the warrant application in this case is signed by Detective Sergeant Chad Wanta of the Oneida County Sheriff's Office. At the time of the application for the warrant, Sergeant Wanta was affiliated with the Internet Crimes Against Children (ICAC) Task Force, which focuses on investigating technology-facilitated child sexual exploitation and internet crimes against children, including trafficking of children. Sergeant

Wanta had been a law enforcement officer for eighteen years and had received training in the investigation of internet crimes against children. He worked cooperatively with agents from the Wisconsin Department of Justice investigating cases within Oneida County. Wanta Aff., Dkt. No. 22-1, ¶¶ 1–3.

In his affidavit, Sergeant Wanta recounts a series of eight CyberTipLine reports from the National Center for Missing and Exploited Children (NCMEC) that had been received by the Wisconsin Department of Justice, the Oneida County Sheriff's Office, and the Federal Bureau of Investigation. Ex. 1, Wanta Aff. at ¶ 6. A CyberTipLine Report is a notification that internet providers are statutorily required to submit to NCMEC regarding suspected online crimes against children. NCMEC then forwards those cyber tips to the appropriate law enforcement agency for investigation. *See* 18 U.S.C. § 2258A.

Sergeant Wanta stated in his affidavit that he had received several CyberTipLine reports that described incriminating messages beginning in January 2018 and continuing to December 2019. The messages all seemed related because of the characteristics they shared. Wanta Aff. at

¶ 6. The affidavit describes eight separate CyberTipLine reports. Each was reported by the electronic service provider MeetMe.com and sought a sexual encounter with a female child. All had screen names using a name starting with the letter J. One used the name "Jared," and the rest used some form of the name "Jacob" and/or "Jones." The contents of the message and verbiage used to convey the offer to pay money to meet with minor females for sexually explicit purposes was also strikingly similar. In each instance, the suspect offered to pay if the recipient

could find him "a much younger girl." Without stating amounts, the suspect continued to promise "serious cash if you could get me a much younger girl" or "I'll pay you lots," frequently using dollar signs, "$$$," to represent money. All but two of the messages were sent using public Wi-Fi locations. All but one of the CyberTipLine reports stated that the Wi-Fi locations used by the sender were associated with businesses located in Rhinelander, a small city (pop. 7,500) in northern Wisconsin. *Id.* ¶¶ 6–10, 12–15. Two of the reports described in the affidavit stated that the IP address used by the sender was determined to be from the public Wi-Fi provided by the McDonald's fast-food restaurant at 25 S. Stevens Street in Rhinelander, and three stated the IP addresses used by the sender were determined to be from the public Wi-Fi of Modes, Machines & More LLC, a laundromat located at 2100 Lincoln Street, Rhinelander. *Id.* ¶¶ 7, 9, 13–15. Two of the reports identified Northwoods Communications Technologies, located at 2151 N. Chippewa Drive, Rhinelander, Wisconsin, as the source of the IP address for the messages, and one of the reports determined that the IP address used by the suspect was from the public Wi-Fi location at the Holiday Inn Express at 200 S. Mannheim Road, Hillside, Illinois. *Id.* ¶¶ 8, 10, 12.

These facts, which Osterman does not challenge, are sufficient to warrant the inference that the messages described in the eight CyberTipLine reports likely shared the same source or originated from the same individual who lived and/or worked in Rhinelander. The inference that Osterman was likely that source arose from several other facts Sergeant Wanta included in his affidavit. As noted, two of the CyberTipLine reports Wanta received

identified the Rhinelander business Northwoods Communications Technologies as the source of the IP address for the messages. Those messages included one sent by Thor Jones on May 28, 2018, and another sent by Jake Jones on August 26, 2018. *Id.* ¶¶ 8, 10. Osterman, a resident of Rhinelander, was the contact person for Northwoods Communications. *Id.* ¶ 8. Sergeant Wanta and Special Agent Theodore Indermuehle of the Wisconsin Division of Criminal Investigation ICAC Task Force interviewed Osterman about the messages the CyberTipLine reports identified as issued through his company. By the time of the interview, the name of Northwoods Communications had been changed to Northwoods Connect—High Speed Internet, which was an internet service provider, and Osterman was identified as an owner. Osterman told Sergeant Wanta and Special Agent Indermuehle that the IP address used on the dates and times in question could have been used by any of Northwoods Connect's approximately 400 customers but there was no way to track one specific customer to the IP address. *Id.* ¶ 11.

In addition, one of the CyberTipLine reports identified a messaging conversation that began on July 4, 2019, between a person with the MeetMe username Brad Jones and a person the government refers to as JV-1. According to Sergeant Wanta's affidavit, Jones initially believed JV-1 to be a 19-year-old female living in Chicago. Jones told JV-1 "I'll give you $$$ if you can get me a much younger girl." *Id.* ¶ 12. JV-1 then told Jones she was only 13. Jones replied, "cool. id love to fuck a 10–12 girl. know any? ill pay you." *Id.* JV-1 asked Jones where he lived, and Jones responded that he lived in Milwaukee but could drive to Chicago. JV-1 told

Jones she was really 12 years old and sent him a picture. Jones then agreed to a sexual encounter with JV-1 and said he would drive down to Chicago that night and be there by midnight. At approximately 11:42 p.m., Jones messaged that he was close, and JV-1 gave him an address. *Id.* According to Sergeant Wanta's affidavit, the IP address used by Jones during the messaging was determined to be a public Wi-Fi location at Holiday Inn Express & Suites located at 200 S. Mannheim Road, Hillside, Illinois. Records from the Holiday Inn obtained by the Wisconsin Department of Justice revealed that Osterman rented a room at the hotel on July 5, 2019. *Id.*

Finally, Sergeant Wanta stated in his affidavit that, on February 21, 2020, the Rhinelander Police Department had received a call for service regarding a suspicious male parked in a vehicle for several hours at 2120 Lincoln Street. Rhinelander Police Officer Benjamin Curtes responded and made contact with a male sitting in a black 2019 Ram 1500 Classic Pickup Truck. The male was identified as Osterman. According to Officer Curtes, Osterman had two electronic tablet devices and a cellular phone operating at the same time. Osterman told Officer Curtes that he was the owner of Northwoods Connect and was testing the internet speed of Northwoods Connect competitors. Sergeant Wanta noted in his affidavit that the location where Osterman was parked was within the range that would allow access to the public Wi-Fi connection of Modes, Machines & More LLC, the public Wi-Fi location identified for three of the eight CyberTipLine reports Wanta was investigating. *Id.* ¶ 16.

Based on this information, Sergeant Wanta

sought and obtained a warrant authorizing him to surreptitiously place a GPS tracking device on Osterman's pickup truck on April 6, 2020. Police then monitored the data retrieved from the device through the summer and fall of 2020. They determined that Osterman's truck was parked at the McDonald's and laundromat at the locations identified in the CyberTipLine reports for multiple hours on multiple days. The GPS data also showed that the truck was parked at other public Wi-Fi locations in northern Wisconsin during this time. Govt.'s Response, Dkt. No. 22 at 6.

Osterman contends in this case that two material false statements appear in the warrant used to authorize the installation of the GPS tracking device on his vehicle. Osterman first contends that Sergeant Wanta's statement that "the IP address used by Jones during the messaging was determined to be a public Wi-Fi location at Holiday Inn Express & Suites, 200 S. Mannheim Road, Hillside, IL 60162," Wanta Aff. at ¶ 12, is false. Instead, he contends, the investigators identified two IP addresses used by "Brad Jones" on July 4, 2019, while messaging JV-1 and that neither of those IP addresses were associated with the Hillside Holiday Inn. Def.'s Mot. to Suppress, Dkt. No. 19, at ¶ 10. The second statement Osterman challenges concerns Sergeant Wanta's description of Rhinelander Police Officer Curtes' interaction with Osterman on February 21, 2020. Wanta Aff. at ¶ 16. Sergeant Wanta stated in his affidavit that Osterman was observed in his truck and that he "had two electronic tablet devices and a cellular phone operating at the same time." *Id.* Osterman contends that the statement that Osterman was using three electronic devices simultaneously is also false. Instead, Osterman

claims that Officer Curtes' report states that he saw Osterman using his cellphone and "there were two tablets stacked on top of each other on the center console." Mot. to Suppress at ¶ 14.

Findings of Fact and Conclusions of Law

At the outset, I find Sergeant Wanta to be a credible and candid witness. The statement in his affidavit that the IP address used by Jones "*during the messaging*" was determined to be a public Wi-Fi location at the Hillside Holiday Inn was false if "during the messaging" was intended to refer to the electronic conversation Jones had with JV-1. Sergeant Wanta testified that that is what he intended to say in his affidavit and conceded that he was mistaken. The CyberTipLine report he viewed actually said that Jones used the Hillside Holiday Inn public Wi-Fi on July 5, 2019, about 12 hours after Jones' last message with JV-1. Although not included in his affidavit, Sergeant Wanta testified that he knew at the time he applied for the warrant that the Brad Jones email account had been created using the public Wi-Fi at the Goodwill store in Antigo, Wisconsin on July 3, 2019. Antigo is also in northern Wisconsin, about 45 miles south of Rhinelander. As the affidavit recounts, the CyberTipLine report stated that Jones' messaging with JV-1 occurred on July 4, 2019. Jones initially believed JV-1 to be a 19-year-old female living in Chicago. Jones told JV-1 he would "give you $$$ if you can get me a much younger girl." Wanta Aff. at ¶ 12. JV-1 then told Jones she was actually 13 years old, and when Jones indicated he wanted someone still younger, JV-1 said she was 12. The conversation continued with Jones eventually agreeing to travel from Milwaukee where he claimed to live to Chicago

that night to have sexual intercourse with JV-1. *Id.*

Sergeant Wanta testified that the electronic CyberTipLine report concerning this incident, along with the attachments showing the internet provider's response to subpoenas, indicated that Jones had used a public Wi-Fi in Antigo and one at a McDonald's in Gurnee, Illinois, just north of Chicago, in his messaging with JV-1. He also used a public Wi-Fi for another McDonald's in Chicago in the early morning hours of July 5, 2019, telling JV-1 to meet him outside at 2:30 a.m. Sergeant Wanta testified that he failed to include the other public Wi-Fi locations in his affidavit because of his focus on the Holiday Inn and the guest list that included Osterman's name and address.

Sergeant Wanta testified that after receiving the CyberTipLine report recounting these messages, agents at the Wisconsin Department of Justice realized that the substance and form of the messages were similar to the Rhinelander messages that he was investigating and issued a subpoena to the Hillside Holiday Inn, approximately 17 miles west of Chicago, for the list of guests who were staying at the hotel on July 5, 2019. Sergeant Wanta recognized Osterman's name on the list as the person whose name had surfaced in connection with Northwoods Communications, which had issued the IP address associated with two of the CyberTipLine reports. As he was preparing his affidavit, he inadvertently omitted the other Wi-Fi locations that were identified in the report. Sergeant Wanta testified that he viewed the other Wi-Fi locations as possibly relevant to the case involving JV-1 but not to the Wisconsin cases he was investigating.

Based on the evidence presented and my review of

the warrant affidavit, I find that Sergeant Wanta did not knowingly, intentionally, or with reckless disregard for the truth, include a false statement in his search warrant affidavit. While it is true that Jones was not using the Hillside Holiday Inn Wi-Fi while messaging with JV-1, he did use it during the general time period in which Jones had apparently traveled to Chicago in order to have a sexual encounter with a child he believed to be 12 or 13 years old. The fact that he connected to the internet using the public Wi-Fi provided by different businesses while specifically messaging JV-1 was not material to the probable cause determination. There was no way to identify who Jones might be from the public Wi-Fi available at the Goodwill Store in Antigo or the McDonald's restaurants in Gurnee or Chicago. People do not generally provide their names in order to use the free Wi-Fi connection that is offered to customers at restaurants or other businesses. The failure to identify the other public Wi-Fi locations from which Jones sent messages to JV-1 thus did not weaken the inference that Osterman was likely the source of the messages. In fact, had the additional information been provided, it would have strengthened the inference tying Osterman to the messages since it would have more clearly linked the messages to JV-1 to the person from northern Wisconsin who Sergeant Wanta believed was trying to arrange sexual encounters with young girls. It would have shown that Jones had traveled from Antigo south to Chicago in order to have a sexual encounter with a child.

Hotels, on the other hand, commonly offer free Wi-Fi to registered guests. By checking the hotel registry, the investigators were able to obtain a list of individuals, one of whom was likely the source of the

Jones messaging. That Jones was sending messages through the Hillside Holiday Inn Wi-Fi system using the same email account he used to set up his sexual encounter with JV-1 only hours earlier and on the same day that Osterman was a registered guest at the same hotel was the key fact that, together with the other information contained in Sergeant Wanta's affidavit, gave rise to the reasonable inference that Osterman was the person responsible for the messages law enforcement was investigating. For these reasons, Sergeant Wanta's identification of the Hillside Holiday Inn as the location from which Jones messaged JV-1 and his failure to identify the locations of the public Wi-Fi Jones actually used for the specific messages he sent to JV-1 was not a materially false statement either intentionally or recklessly made in order to obtain a warrant.

Osterman's argument is even weaker with respect to the second "false statement" he alleges concerning the report of Officer Curtes. The affidavit stated Officer Curtes had reported that Osterman was operating his phone and two electronic tablet devices when Officer Curtes encountered him in response to a call that a suspicious person had been parked outside a business for hours. Osterman had been parked near the laundromat whose public Wi-Fi had been identified as the source for three of the CyberTipLine reports Sergeant Wanta identified in his affidavit. Osterman asserted in his motion that Sergeant Wanta's statement that Officer Curtes reported Osterman was using three electronic devices simultaneously is false and that Officer Curtes actually reported that Osterman was using his phone and the tablets were stacked on top of each other on the center console. In fact, Officer Curtes' report, which was received in evidence at the

hearing, notes that Osterman told Officer Curtes that he was "checking the speed of the connection while using his devices to check email and other applications." Ex. 3. Given the specific language of the report, I find Sergeant Wanta's summary of Officer Curtes' observations in his affidavit was true and accurate.

In sum, Osterman has failed to demonstrate that a false statement was knowingly and intentionally, or with reckless disregard for the truth, included by Sergeant Wanta in the affidavit he submitted in order to obtain the warrant authorizing the placement of a GPS tracking device on Osterman's truck. In addition, neither of the allegedly false statements he identifies were material to the probable cause determination made by the judge who issued the warrant. Osterman's motion to suppress is therefore denied. The Clerk is directed to place this matter on the Court's calendar for a telephone conference to discuss further proceedings.

SO ORDERED at Green Bay, Wisconsin this 26th day of January, 2022.

s/ William C. Griesbach
William C. Griesbach
United States District Judge

UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT
Chicago, Illinois 60604

October 23, 2024

Before

Kenneth F. Ripple, *Circuit Judge*
Michael Y. Scudder, *Circuit Judge*
Candace Jackson-Akiwumi, *Circuit Judge*

No. 22-2773

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

PAUL OSTERMAN,
Defendant-Appellant.

Appeal from the United States District Court for the
Eastern District of Wisconsin,
No. 1:21-cr-00110
William C. Griesbach**,** *District Judge*.

O R D E R

Defendant-Appellant filed a petition for rehearing on August 13, 2024. The petition is GRANTED to the extent that the panel is issuing the attached amended opinion.