

In the
United States Court of Appeals
For the Seventh Circuit

No. 22-2773

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

PAUL S. OSTERMAN,

Defendant-Appellant.

Appeal from the United States District Court for the
Eastern District of Wisconsin,
No. 1:21-cr-110 — **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 incorrect. 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 suppress, 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 website'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 Rhinelander, 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, Machines & 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 paragraph, 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 warrant.

These inaccuracies led Osterman to file a motion to suppress 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 Osterman'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 suppression 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 preponderance 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) probable 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 prevail 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 accuracy 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 contraband 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 omitted, *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 constructing 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 Rhinelander, 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.