

In the
United States Court of Appeals
For the Seventh Circuit

No. 15-3854

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

JESSE D. FEATHERLY,

Defendant-Appellant.

Appeal from the United States District Court for the
Western District of Wisconsin.

No. 0758 3:14-cr-00127-1 — **Barbara B. Crabb**, *Judge.*

ARGUED OCTOBER 5, 2016 — DECIDED JANUARY 17, 2017

Before BAUER, FLAUM, and KANNE, *Circuit Judges.*

PER CURIAM. Jesse Featherly challenges the denial of his motion to quash the search warrant that led to the discovery of child pornography on his computer. Featherly contended that the government secured the warrant by making an intentionally false statement on the warrant application. The district court disagreed, and Featherly pleaded guilty to receiving child pornography. Because the court did not clearly err

in concluding that there was no intentionally false statement and that probable cause supported the warrant, we affirm.

Featherly, then 27, was living in a trailer park in Rice Lake, Wisconsin, when his involvement with child pornography attracted the attention of law enforcement. An agent in Oklahoma discovered that Featherly's Internet-service account was being used to share files containing child pornography. An FBI special agent in Wisconsin, Jon Hauser, applied for a warrant to search Featherly's residence. In an affidavit filed in support of the warrant application, Hauser stated that the agent in Oklahoma, after partially downloading the shared files, "was able to determine the IP address of this [user's] computer to be 68.190.144.255." (An "Internet Protocol address" or "IP address" is defined elsewhere in the affidavit as referring to "a unique number used by a computer to access the Internet" and is assigned by a user's Internet-service provider.) According to Hauser, the agent was able to use this unique "address" and ascertain that an Internet-service provider, Charter Communications, at the time of the download had assigned this IP address to Featherly's service account.

A magistrate judge issued the warrant, concluding that the affidavit established probable cause to search the residence. The warrant was executed and, based on the images found, Featherly was charged with receipt of child pornography, 18 U.S.C. § 2252(a)(2), and possession of it, *id.* § 2252(a)(4).

Featherly then moved for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), seeking to quash the warrant and suppress all evidence obtained during the search because Hauser had falsely stated in his affidavit that the IP address used by the suspect was traced to Featherly's computer. The

No. 15-3854

3

statement was false, Featherly maintained, because an IP address identifies only a modem—the device that connects computers to the Internet—and does not pinpoint the particular computer that uses the modem to access the Internet. If Hauser’s false statement were “excised” from the affidavit, Featherly urged, there would be no evidence to trace the offending Internet user to his residence, and thus no probable cause for the search.

The magistrate judge held an evidentiary hearing to clarify the facts relevant to Featherly’s challenge to the accuracy of the application for the search warrant. An FBI special agent who was based in Eau Claire, Forrest Wilkins, testified that he was the primary investigator in Featherly’s case and had prepared the affidavit which Hauser reviewed and signed. Wilkins elaborated on his understanding of the significance of an IP address. He acknowledged, for instance, that an IP address was associated with a modem at the service residence of the Internet subscriber, but said that a modem could be defined as a “computer,” because it was a “high speed data processing device.”

The magistrate judge concluded that probable cause supported the warrant and recommended that the motion to quash the warrant be denied. This finding of probable cause, the judge explained, was not affected by Wilkins’s view that “computer” could be defined to include modems, but even if this view were not correct, his adoption of a broader definition had not been reckless or with an intent to mislead. The judge dismissed Featherly’s semantic challenge to “computer” as irrelevant (“This court’s response to these arguments is ‘okay, so what?’”), and discounted the significance of any flaw in the affidavit’s wording as “neither material nor

misleading.” Based on the evidence in the affidavit, the court reasonably could infer that a search of Featherly’s residence would turn up evidence of child pornography because the service account of the user sharing the incriminating files had been registered to Featherly’s name and address. Finally, the judge concluded, Wilkins did not perpetrate any knowing or reckless falsehood: He had no reason to falsely attribute the IP address to Featherly’s computer because such a misstatement “did nothing to bolster probable cause.”

Over Featherly’s objection, Judge Crabb adopted the magistrate judge’s report and recommendation, denied the motion to quash the warrant, and reprimanded Featherly for “persist[ing] in tilting at this windmill.” She agreed that the affidavit did not contain an intentionally false statement or material omission and thus did not need to be analyzed under *Franks*; she also agreed that the affidavit supplied sufficient probable cause to support the issuance of a warrant. And even if Wilkins in the affidavit had wrongly referred to the modem as a computer, any mistake was irrelevant because Charter identified the modem as servicing Featherly’s residence, and this identification was sufficient to support an inference that pornography would be found on his computer.

After his motion was denied, Featherly pleaded guilty to receiving child pornography, 18 U.S.C. § 2252(a)(2)—though reserving the right to appeal the denial of his motion—and was sentenced to 144 months’ imprisonment.

On appeal Featherly challenges the conclusion that there was no *Franks* violation requiring suppression of the evidence. Under *Franks*, evidence seized under a warrant must be suppressed when the defendant shows that “(1) the affida-

No. 15-3854

5

vit 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 (7th Cir. 2013); see *Franks*, 438 U.S. at 155–56. Featherly focuses on the first prong and maintains that Hauser’s affidavit falsely stated that an IP address belonged to the user’s computer. In Featherly’s view the IP address was assigned only to his modem, and the identity of the particular device using the modem at the time in question was unknown. This confusion, Featherly continues, kept the warrant-issuing judge from considering the possibility that someone else in the trailer park had connected to his modem wirelessly, without his knowledge, and used his Internet service to share child pornography.

We agree with the district judge that there was no intentional false statement in the affidavit. The statement that the IP address belonged to the user’s computer was not false. As the government points out, Hauser specified in his affidavit that he defined the term “computer” according to the statutory language of 18 U.S.C. § 1030(e)(1), which includes a “communications facility directly related to or operating in conjunction with” a computer. One such “communications facility” is Featherly’s modem since it’s a device that operates in conjunction with a computer to enable communication with others over the Internet. The affidavit could have been more precise, as the magistrate judge and the district judge both noted, but it accurately stated that the Internet user who was sharing child pornography was using an IP address connected to Featherly’s service account.

We also agree with the district judge and the magistrate judge that Hauser's statement about an IP address belonging to a particular computer was not significant to the finding of probable cause because probable cause was sufficiently established by the tracing of the IP address to Featherly's modem. While an unknown user conceivably could connect to another's modem through an unsecured wireless network, the record does not reflect that Featherly had such a network. Further, probable cause requires only "facts sufficient to induce a reasonably prudent person to believe that a search ... will uncover evidence of a crime," *United States v. Gregory*, 795 F.3d 735, 741 (7th Cir. 2015) (quoting *United States v. Roth*, 201 F.3d 888, 892 (7th Cir. 2000)), and the connection between an IP address and a modem at an Internet subscriber's residence is sufficient to justify a search, *see, e.g., United States v. Vosburgh*, 602 F.3d 512, 526–27 (3d Cir. 2010) (agreeing with other circuits that "evidence that the user of a computer employing a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address"); *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) (acknowledging possibility that neighbors could have used unsecured wireless connection but concluding that "it remained likely that the source of the transmissions [of child pornography] was inside [the] residence" to which the IP address was assigned).

AFFIRMED.