

No. 14-3576

**UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT**

FILED
May 28, 2015
DEBORAH S. HUNT, Clerk

UNITED STATES OF AMERICA,)
)
Plaintiff-Appellee,)
)
v.)
)
PAUL C. SCHUMACHER,)
)
Defendant-Appellant.)
)
)
)

ON APPEAL FROM THE UNITED
STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF OHIO

BEFORE: DAUGHTREY, GIBBONS, and GRIFFIN, Circuit Judges.

MARTHA CRAIG DAUGHTREY, Circuit Judge. Following his arrest and indictment for receipt and possession of child pornography, Paul Schumacher moved to suppress all evidence acquired in the search of his residence and computer. He argued that the warrant authorizing the search lacked probable cause because the affidavit filed in support of the warrant failed to establish the scientific reliability of the investigative software used to support the affidavit's allegations or to sufficiently detail the software's operations. He also requested a hearing on the motion. The district court denied both his request for a hearing and the motion on its merits. Schumacher now appeals this denial on the grounds that the district court abused its discretion by denying the motion without first providing him the opportunity to examine the reliability of the software in a hearing. We find no reversible error and affirm.

FACTUAL AND PROCEDURAL BACKGROUND

The challenged search warrant was based on an affidavit in which Jeffrey M. Casey, a special agent of the Secret Service, asserted that his investigation of the activities of the internet account registered to 17 Hop Drive in Lowellville, Ohio, established probable cause to believe that someone at that address had received, possessed, and/or distributed child pornography over a peer-to-peer network. Agent Casey swore that on June 19, 2013, he signed into “automated software which operates on the Phex platform” while covertly connected to the internet protocol (IP) address in question. The affidavit’s explanation of how this “automated software” operated was limited to the following:

The software automates the process of browsing and downloading files from a single source. The downloaded files are shared by a user over the Gnutella network. The software searches the Gnutella network for files with hash values of suspected child pornography.

The terms “Gnutella network” and “hash values” were defined in the affidavit, which also asserted that an individual using the IP address assigned to the internet account at 17 Hop Drive was sharing over 4,000 unique files with hash values corresponding to videos and images of child pornography. From these shared files, the automated software used by Agent Casey downloaded five image files; screen captures of the downloaded files showed images of child pornography. A search of various public records revealed that one of the two individuals associated with 17 Hop Drive was defendant Paul Schumacher.

The search warrant application was granted on July 30, 2013. Following the execution of the warrant, Schumacher was indicted and arrested on charges of one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and one count of possessing a computer containing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B).

Schumacher moved to suppress the evidence acquired in the search of his home and computer, on the ground that the search warrant affidavit “contain[ed] unreliable information, in violation of the Fourth Amendment.” He requested an evidentiary hearing on the motion, which was opposed by the government. After finding that Schumacher had both failed to meet the preliminary showing requirements for a suppression hearing and failed to show that the search warrant affidavit lacked probable cause, the district court denied his motion to suppress.

Schumacher pleaded guilty to one count of receiving child pornography and was sentenced to 97 months imprisonment. As a condition of the plea agreement, Schumacher reserved the right to appeal the district court’s denial of his motion to suppress.

DISCUSSION

We review a district court's decision whether to hold an evidentiary hearing on a motion to suppress for an abuse of discretion. Factual findings made in denying an evidentiary hearing on a motion to suppress are reviewed for clear error; conclusions of law are reviewed *de novo*. See *United States v. Rose*, 714 F.3d 362, 369-70 (6th Cir.), *cert. denied*, 134 S. Ct. 272 (2013).

Schumacher argues that the district court erred in denying his motion to suppress without first holding an evidentiary hearing because, in doing so, it left unresolved a genuine issue of fact regarding the existence of probable cause for the search of his property. Specifically, he contends that the search warrant affidavit lacked probable cause because it failed to establish the scientific reliability of the software on which the affidavit’s allegations were based.

The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation” U.S. Const. amend. IV. “A warrant will be upheld if the affidavit provides a ‘substantial basis’ for the issuing magistrate to believe [that] ‘there is a fair probability that contraband or evidence of a crime will be found in a particular place.’” *United*

States v. Smith, 510 F.3d 641, 652 (6th Cir. 2007) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). When a defendant alleges that a statement in an affidavit filed in support of issuing a warrant is false or that information was omitted from the affidavit, he is entitled to an evidentiary hearing if he: (1) makes a substantial preliminary showing that the affiant knowingly, intentionally, or with reckless disregard for the truth included the false statement or omitted information, and (2) establishes that the false statement or omission is material to a finding of probable cause. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978); *Rose*, 714 F.3d at 370. No hearing is required if probable cause exists absent the false statement, or if probable cause exists despite the inclusion of the omitted statement. *United States v. Fowler*, 535 F.3d 408, 415 (6th Cir. 2008).

The district court did not err in denying Schumacher's motion to suppress without first providing a hearing. Though Schumacher now insists that the search warrant affidavit "lacked probable cause due to deliberate and/or reckless omissions and misstatements regarding the investigative software," in the district court he failed to identify any false statements within the affidavit or provide any evidence that information material to the existence of probable cause was omitted from the affidavit. Schumacher asserts that the veracity of the entire affidavit is in doubt because the affidavit "provides no information relative to the accuracy or reliability of the government's method of investigation." He takes particular offense at the affidavit's failure to describe how the investigative software works, name the software, or "cite actual statistics or a single report verifying [its] claims . . . as to the reliability and accuracy" of it. He fails to establish, however, any way in which the omission of this information was actually material to a finding of probable cause. Inclusion in the affidavit of a more detailed account of how the software at issue operated, its name, and statistics or reports verifying its reliability and accuracy

would not, in fact, have decreased the probability that a search of Schumacher's property would turn up images of child pornography; such information arguably would have only strengthened the affidavit by showing that the software was reliable. *See United States v. Chiaradio*, 684 F.3d 265, 279 (1st Cir. 2012).

Furthermore, Schumacher's argument implies that a warrant affidavit that relies on information acquired by software lacks probable cause unless it also establishes the scientific reliability of that software. But Schumacher offers no precedent, from this circuit or any other, in support of this proposition. Notably, the First Circuit has flatly rejected it. *See Chiaradio*, 684 F.3d at 278-79 (upholding denial of motion to suppress that argued for suppression, on the ground that the search warrant affidavit was based on "largely untested" software and did not sufficiently demonstrate the software's reliability, because "probable cause does not require scientific certainty").

Schumacher observes that other district courts have held hearings "to allow presentation of evidence and cross-examination of witnesses regarding . . . the reliability of investigative software utilized by the government." But the lower court decisions he cites are not only binding on this court; they are also completely unpersuasive. None of these cases holds or otherwise supports Schumacher's claim that blanket challenges to the reliability of investigative software entitle a defendant to a *Franks* hearing.¹

¹ *See, e.g., United States v. Dennis*, No. 3:13-cr-10-TCB, 2014 WL 1908734, at * 3, *5 (N.D. Ga. May 12, 2014) (noting that evidentiary hearing was held, where defendant argued that law enforcement's use of file sharing software to access his computer violated his Fourth Amendment right to privacy); *Mahan v. Bunting*, No. 1:13-cv-00165, 2014 WL 1154054, at *1-*2, *4 (N.D. Ohio Mar. 20, 2014) (acknowledging that state court conducted suppression hearing after defendant filed a motion to suppress that argued that the search warrant affidavit failed to provide sufficient information on investigative software); *United States v. Thomas*, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484, at * 1 (D.Vt. Nov. 8, 2013) (reviewing the findings of an evidentiary hearing held after defendants filed motions to suppress that made specific challenges to the reliability of investigative software); *United States v. Gabel*, No. 10-60168, 2010 WL 3927697, at *1, *2 (S.D.Fla. Sept. 16, 2010) (noting that evidentiary hearing was held, where defendant argued, *inter alia*, that the search warrant affidavit was invalid

Schumacher's reliance on *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012), is similarly misguided. As Schumacher himself acknowledges, *Budziak* recognized that the functionality of investigative software used in child pornography cases was "material [to the defense] under the rules of discovery." But the dispositive question in *Budziak* was whether the defendant was entitled to information regarding the functionality of investigative software as a discovery matter, not whether a search-warrant affidavit must provide such information. 697 F.3d at 1111-12. Thus, it is of no relevance here.

Schumacher additionally argues that the denial of his motion to suppress without first providing a hearing was erroneous because it deprived him of the opportunity to "investigate and cross-examine" the software. He suggests that an evidentiary hearing should have been held to allow him to gather evidence that the software was unreliable. In this regard, Schumacher appears to have confused the purpose of a *Franks* hearing, which is to permit the court to determine whether law enforcement agents made deliberate falsehoods to secure a search warrant, not to provide discovery for the defendant. *See Franks*, 438 U.S. at 170 (noting that the preliminary showing requirement "prevent[s] the misuse of a veracity hearing for purposes of discovery."). Further, "[t]o mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Id.* at 171. The district court's refusal to provide Schumacher a hearing on his motion to suppress, then, did not deprive him of his right to investigate the reliability of the software, because he was not entitled to any such right under *Franks*.²

because it omitted the fact that law enforcement used file sharing software that was only available to law enforcement to access his computer).

² Schumacher cursorily asserts that the district court violated his Fifth Amendment right to due process and his Sixth Amendment right to confrontation by denying his suppression motion without a hearing. But he provides no case law or argument in support his apparent claim that these rights extend to a defendant challenging whether a search

Lastly, Schumacher incorrectly asserts that the district court ran afoul of this court's precedent by denying his motion and "blindly accept[ing] the reliability" of the software. He provides no precedent holding that a court must assess the reliability of investigative software used to support a search warrant's affidavit before finding that probable cause for the warrant exists. He instead cites two cases that concern the irrelevant issue of the competency and credibility of evidence offered at suppression hearings. *See United States v. Stepp*, 680 F.3d 651, 668 (6th Cir. 2012); *Fields v. Bagley*, 275 F.3d 478, 485 n.5 (6th Cir. 2001) (*per curiam*).

Because Schumacher has failed to show that the search warrant affidavit included false statements or omitted information material to a finding of probable cause, he cannot meet the preliminary showing required for an evidentiary hearing on a motion to suppress. The district court thus did not abuse its discretion in denying Schumacher's motion to suppress without first holding a *Franks* hearing, and should be affirmed.

CONCLUSION

For the reasons set out above, we AFFIRM the district court's judgment.

warrant affidavit provided probable cause for a search, or that they entitle such a defendant to a *Franks* hearing even if that defendant cannot make the preliminary showing required for such a hearing.