[DO NOT PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 14-14506
Non-Argument Calendar

D.C. Docket No. 1:14-cr-20243-KMM-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

ALEXANDER ROUSSEAU,

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of Florida

(October 19, 2015)

Before HULL, JORDAN and JILL PRYOR, Circuit Judges.

PER CURIAM:

After a jury trial, Alexander Rousseau appeals his convictions on five counts of receiving materials depicting a minor engaged in sexually explicit conduct, in

violation of 18 U.S.C. § 2252(a)(2). On appeal, Rousseau challenges the district court's denial of his motion to suppress evidence found during the execution of a search warrant at the fire station where Rousseau worked. During the search, federal agents found Rousseau's laptop, which contained over 100 videos of child pornography and, at the time of the search, was actively downloading child pornography using an unsecured wireless network. Rousseau argues that the district court: (1) should have held a Franks[1] hearing to determine whether the search warrant application contained material misrepresentations about who could access the wireless network; and (2) should have suppressed the evidence found during the search because the search warrant was unconstitutionally broad. After review, we affirm.

I. FRANKS CLAIM

A. General Principles

A defendant seeking a Franks hearing must make a "substantial preliminary showing" that (1) an affiant applying for a search warrant made intentionally false or recklessly misleading statements, and (2) those statements were necessary to the finding of probable cause. United States v. Barsoum, 763 F.3d 1321, 1328 (11th Cir. 2014), cert. denied, 135 S. Ct. 1883 (2015). The defendant's substantiality requirement "is not lightly met." United States v. Arbolaez, 450 F.3d 1283, 1294

[1]Franks v. Delaware, 438 U.S. 154, 155-56, 98 S. Ct. 2674, 2676 (1978).

(11th Cir. 2006). Allegations of deliberate falsehood or reckless disregard for the truth "must be accompanied by an offer of proof." Id.

In addition, the defendant must show that, if the misrepresentations were removed from, or the omitted facts were included in, the warrant affidavit, then probable cause would be lacking. United States v. Mathis, 767 F.3d 1264, 1275 (11th Cir. 2014) (involving omissions), cert. denied, 135 S. Ct. 1448 (2015); Barsoum, 763 F.3d at 1329 (involving misstatements). If the warrant would still support probable cause, then no Franks hearing is necessary. United States v. Capers, 708 F.3d 1286, 1296 (11th Cir. 2013). In the search warrant context, probable cause exists when, under the totality of the circumstances, "there is a fair probability of finding . . . evidence [of a crime] at a particular location." United States v. Brundidge, 170 F.3d 1350, 1352 (11th Cir. 1999). [2]

B. Warrant Affidavit

FBI Special Agent Alexis Carpinteri's warrant affidavit stated, inter alia, that her investigation had identified a computer with the user name "anon_ae3d4aee@Ares" and an IP address assigned to "Miami Fire Station 6" that

[2]We review for an abuse of discretion a district court's denial of a Franks hearing. Barsoum, 763 F.3d at 1328. Because the district court's denial of the motion to suppress is a mixed question of law and fact, we review the district court's factual findings for clear error, and its application of the law to the facts de novo. Id. We review de novo whether a search warrant affidavit established probable cause, taking care "both to review findings of historical fact only for clear error and to give due weight to the inferences drawn from those facts by resident judges and local law enforcement officers." United States v. Jiminez, 224 F.3d 1243, 1248 (11th Cir. 2000) (quotation marks omitted).

was using the ARES peer-to-peer ("P2P") file sharing network to share files containing child pornography. Surveillance of the Station revealed one open (i.e., not secured by a password) wireless Internet network with limited geographic scope.

Specifically, Agent Carpinteri's affidavit stated that "[a] check for open wireless networks was conducted," which revealed "one open wireless network labeled 'WiFi-Repeater1.'" That wireless network "could only be detected while pulled up directly to the front of the building," and "[t]he only area for a vehicle to pull up to the building was directly in front of the four (4) bay garage doors where the emergency vehicles for the station were housed." There was no visitor parking, and the employee parking behind the building was secured by a gated entrance. Further, "[i]t did not appear that any area along the perimeter of the [Station] was viable to access and utilize the unsecured network that was observed at the [Station]."

The investigation further revealed that the IP address had shared files containing child pornography on the P2P network "on a consistent basis, starting on June 1, 2013," with the majority of the time on the P2P network observed "after 8:00 p.m., often after 10:00 p.m., and ending before 4:00 a.m." Agents also learned that individual firefighters assigned to the Station worked in 24-hour shifts

beginning at 7:30 a.m., and that each firefighter worked one day on-duty, followed by two days off-duty, with some flexibility for contractual days off.

C. Rousseau's Claim of Misrepresentation in Affidavit

Rousseau identifies as false or misleading Agent Carpinteri's statements that the wireless network could only be accessed directly in front of the Station and did not appear to be accessible around the Station's perimeter. Rousseau argues that Agent Carpinteri did not accurately describe the area around the Station, which included a sidewalk on the east side of the Station and a public park on the west side of the Station, and that, in fact, the unsecured wireless network "can be easily accessed by any member of the public" from these omitted areas.

Even assuming arguendo that Agent Carpinteri's affidavit misrepresented the accessibility of the wireless network to people outside the Station, the district court did not abuse its discretion in declining to hold a Franks hearing. This is so because, even if the wireless network could conceivably be accessed from either the sidewalk or the park, the other information in Agent Carpinteri's affidavit showed a fair probability that it was someone inside the Station who was using the wireless network to download and share the child pornography. [3] In particular, as

[3]Because we, like the district court, conclude that the unchallenged portions of the warrant affidavit provide probable cause to believe someone inside the Station was downloading the child pornography, we do not address the government's other arguments that Rousseau failed to submit affidavits or other evidence in support of his factual assertions and thus failed to offer

the district court explained, Agent Carpinteri's affidavit stated that the illegal downloads from the IP address under that username were done "on a consistent basis" for over six months and mostly at night between 10:00 p.m. and 4:00 a.m., making it more likely the user was someone inside the Station than someone outside on the sidewalk or in the public park.

For the first time on appeal, Rousseau contends that Agent Carpinteri's affidavit also omitted that Rousseau was the sole target of the investigation. To the contrary, the trial record shows that Rousseau was not the sole target. Specifically, Agent Carpinteri testified that, from comparing the records of employees' shifts, she identified Rousseau as the only employee on duty at all the relevant times. But, Carpinteri also explained that this fact did not necessarily tell her that Rousseau was the individual downloading and sharing files, because she still did not know who was on the computer and "who [was] doing what at any given time." Therefore, Rousseau was "not the only one" targeted by the FBI investigation. See United States v. Smith, 459 F.3d 1276, 1294 n.16 (11th Cir. 2006) (explaining this Court may consider evidence subsequently introduced at trial in reviewing a motion to suppress). Accordingly, Rousseau has not shown error, much less plain error.

---

proof that Agent Carpinteri made any misrepresentations, much less ones that were intentional or reckless.

In sum, because Rousseau failed to make a substantial preliminary showing of a material misrepresentation in Agent Carpinteri's affidavit, the district court was not required to hold a Franks hearing.

II. PARTICULARITY OF THE SEARCH WARRANT

A. General Principles

The Fourth Amendment requires that a search warrant particularly describe the place to be searched and the things to be seized. U.S. Const. amend. IV. "A warrant which fails to sufficiently particularize the place to be searched or the things to be seized is unconstitutionally over broad." United States v. Travers, 233 F.3d 1327, 1329 (11th Cir. 2000). The particularity requirement, however, does not require "elaborate specificity." United States v. Betancourt, 734 F.2d 750, 754 (11th Cir. 1984). "The standard is one of practical accuracy rather than technical nicety." Id. at 755 (quotation marks omitted).

With regard to the place to be searched, the warrant's description need only have "sufficient particularity to direct the searcher, to confine his examination to the place described, and to advise those being searched of his authority." United States v. Burke, 784 F.2d 1090, 1092 (11th Cir. 1986). As to the materials to be seized, "a description is sufficiently particular when it enables the searcher reasonably to ascertain and identify the things to be seized." United States v. Santarelli, 778 F.2d 609, 614 (11th Cir. 1985). If the applicant for the warrant

cannot give an exact description, but has probable cause to believe that such materials exist, the warrant is sufficiently particular if it is as specific as the circumstances and nature of the activity under investigation permit. Id. Further, where it is not feasible at the time the warrant is issued to give an exact description of the materials to be seized, the warrant satisfies the Fourth Amendment's particularity requirement if it limits the seizure of items to only those items that constitute evidence of criminal activity. Id. at 615.[4]

B. Search Warrant

The search warrant described the property to be searched as any computers, including, among other things, data storage devices, cellular telephones, tablets, and external hard drivers, found in the Station. The search warrant described the items to be seized as, among other things, any visual depictions of child pornography, any records of communication relating to sharing child pornography, communications with an Internet service provider, communications relating to ownership or use of computers at the Station, computer software, computer passwords, and any computers and cameras that may be used to view or store child pornography.

[4]We review de novo a district court's determination that a search warrant satisfied the Fourth Amendment's particularity requirement. United States v. Bradley, 644 F.3d 1213, 1258-59 (11th Cir. 2011).

Agent Carpinteri's affidavit provided general information about the typical behavior of persons involved in child pornography, including how they use computers and other electronic devices to store and transmit images. Among other things, the affidavit explained that "[v]irtually any type of computer," including "cellular telephones, smartphones, tablets, and other such electronic mobile devices" can access the Internet and P2P networks using certain "apps" and wireless networks and that "[a]ny of these computers, if connected to the internet through a home network, would be associated with the IP address assigned to that home network . . . , just the same as would a laptop or desktop computer."

Agent Carpinteri's affidavit also provided information about how computers are seized and searched by forensic analysts for child pornography in a laboratory. The affidavit explained that ordinarily agents must "seize most or all computer items . . . to be processed later" in the laboratory. In this case, however, "[i]n order to narrow down which computers need to be seized [from the Station] for further examination," agents would conduct "on-site evidentiary previews" that would "identify which computers contain evidence of criminal activity and require seizure and which computers are unrelated to the possession, receipt, and distribution of child pornography."

C. Rousseau's Claim That Warrant Was Overbroad

The district court properly denied Rousseau's motion to suppress on particularity or overbreadth grounds. The warrant sufficiently described the places to be searched as the Station—including the address and a description of the building—and any "computers" and "data storage devices" found in the Station. The warrant further contained a very detailed list of the items to be seized, including visual depictions of child pornography; digital and paper documents pertaining to, inter alia, the possession, receipt, or transmission of child pornography, Internet service provider accounts, or online or remote electronic storage; computer software, including P2P file sharing software; and photographic equipment containing child pornography. These descriptions were sufficient to enable a searcher to confine the search to the places described and to reasonably ascertain and identify the things to be seized.

To the extent the descriptions did not identify a specific location within the Station or specific item (such as a particular computer or cell phone), they were as specific as the circumstances and nature of the activity being investigated would permit.[5] The agents were investigating the downloading and sharing of child pornography using an IP address registered to the Station and an open wireless

[5]We find no merit to Rousseau's argument that the warrant application failed to show a nexus between the places to be searched and the items to be seized and the criminal activity being investigated. See United States v. Kapordelis, 569 F.3d 1291, 1310 (11th Cir. 2009) (explaining that the warrant affidavit should establish a connection between the place searched and the criminal activity). Based on the information in the warrant application, there existed a fair probability that evidence of the possession, receipt or distribution of child pornography would be found on one or more computers and storage devices inside the Station.

network accessible inside the Station. The investigators did not know which or how many Station employees might be involved in the activity, much less which computers or electronic storage devices in the Station were being used. The warrant made clear that a search of the computers required the seizure of "most or all computer items" to perform the search thoroughly, and that "on-site evidentiary previews" would be conducted to minimize the burden on individuals and devices that were not involved in the illegal activity. The warrant also only authorized the seizure of items that were "[e]vidence of possession, receipt, and distribution of child pornography."

Contrary to Rousseau's assertion, agents did not conclude that a desktop computer was the only device associated with the anon_ae3d4aee@Ares username. The warrant application stated that any type of computer, including mobile devices such as cell phones, smartphones, and tablets, could use a home wireless network, access P2P networks using certain apps, and store large amounts of electronic data. Dr. Sam Malek's trial testimony—that a P2P network is essentially "just computers," such as personal laptops and desktops, communicating with each other—does not contradict the warrant application on this point. Dr. Malek did not testify that a P2P network can be accessed using only a desktop or laptop computer.

Again, and also contrary to Rousseau's contention, the record does not show that agents identified Rousseau as the only suspect. Agent Carpinteri testified that, although Rousseau was the only Station employee on duty every time child pornography was shared via the P2P network, this did not necessarily mean that he was the only one using a computer to do so. Moreover, even if Rousseau had been confirmed as the only target, the record does not show that the search could have been limited to his quarters or computers. Firefighters at the Station did not have individual quarters, and it was not known that Rousseau had his own laptop at the Station until the warrant was executed.

Under the circumstances, the warrant was as specific as it could be and it was not feasible for the agents to identify ahead of time a particular computer or storage device inside the Station to be seized and searched. For all these reasons, the district court did not err in denying Rousseau's motion to suppress.

AFFIRMED.