FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. ALEXANDER NATHAN NORRIS, *Defendant-Appellant.*	No. 17-10354 D.C. No. 2:11-cr-00188-KJM-1 OPINION

Appeal from the United States District Court
for the Eastern District of California
Kimberly J. Mueller, District Judge, Presiding

Argued and Submitted February 14, 2019
San Francisco, California

Filed November 4, 2019

Before: Mary M. Schroeder, Diarmuid F. O'Scannlain, and Johnnie B. Rawlinson, Circuit Judges.

Opinion by Judge Rawlinson

SUMMARY*

Criminal Law

The panel affirmed a conviction for distribution and possession of material involving the sexual exploitation of minors, in a case in which an FBI agent used wireless-tracking software to detect the signal strength of the address of the defendant's wireless device.

The panel held that because there was no physical intrusion into the defendant's residence to detect the signal strength of his device's media-access-control (MAC) address, the district court correctly applied the factors set forth in *Katz v. United States*, 389 U.S. 347 (1967), and determined that no search occurred under the Fourth Amendment. The panel wrote that the defendant lacked a subjective expectation of privacy in the signal strength of his MAC address emanating from his unauthorized use of a third-party's password-protected wireless router. The panel concluded that society is not, in any event, prepared to recognize as reasonable an expectation of privacy predicated on unauthorized use of a third-party's internet access.

The panel held that the district court did not err in denying the defendant's request for a *Franks* hearing, where the defendant failed to make a substantial preliminary showing that the search warrant affidavit included any knowingly, intentionally, or recklessly made material misrepresentations or omissions; and where a corrected

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

and/or supplemented affidavit would not have affected the probable cause determination.

COUNSEL

John Paul Balazs (argued), Sacramento, California, for Defendant-Appellant.

Matthew G. Morris (argued) and Shelley D. Weger, Assistant United States Attorneys; Camil A. Skipper, Appellate Chief; McGregor W. Scott, United States Attorney; United States Attorney's Office, Sacramento, California; for Plaintiff-Appellee.

OPINION

RAWLINSON, Circuit Judge:

To resolve this case, we must once again venture into the intersection of technology and the Fourth Amendment. Defendant-Appellant Alexander Nathan Norris (Norris) seeks to have us apply the protections of the Fourth Amendment to the use of a wireless tracking program to identify the address of his wireless device. Under the facts of this case, we conclude that no Fourth Amendment search occurred in the course of identifying Norris's wireless device, and we affirm his conviction.

I. BACKGROUND

This case originated in December, 2010, when Federal Bureau of Investigation (FBI) Special Agent Nicholas G.

Phirippidis (Special Agent Phirippidis) initiated an investigation into the possession and distribution of child pornography through a peer-to-peer file-sharing network (P2P network).[1] Special Agent Phirippidis downloaded child pornography from username "boyforboys1," using an Internet Protocol address (IP address)[2] of 67.172.180.130 registered to Comcast Communications (Comcast). Comcast could not determine the physical address for "boyforboys1."

In March, 2011, "boyforboys1" logged into the same P2P network, using a different IP address of 64.160.118.55 registered to AT&T Internet Services (AT&T), and Special Agent Phirippidis again downloaded child pornography from "boyforboys1." In response to a subpoena, AT&T identified the subscriber associated with the IP address as residing in Apartment 242. After conducting a public records search and confirming with the apartment manager that the subscriber still resided at Apartment 242, Special Agent Phirippidis obtained a search warrant for Apartment 242.

Upon execution of the search warrant, Special Agent Phirippidis discovered that the password-protected wireless internet router (router) located in Apartment 242 used an IP address of 69.105.80.128 rather than the 64.160.118.55 IP

---

[1] P2P file-sharing software "allows network computer users, connected to the Internet, to share many types of files; these files typically include music, graphics, images, movies, and text. In this way, [P2P network] users are able to collect large numbers of files, including child pornography."

[2] An IP address "refers to a unique number used by a computer to access the Internet." IP addresses can be dynamic (the number changes each time the computer accesses the Internet) or static (the number remains the same each time the computer accesses the Internet).

address connected to "boyforboys1." The search revealed that no devices in Apartment 242 contained any evidence of child pornography or of the P2P file-sharing program used by "boyforboys1."

FBI agents identified all the devices that had recently connected to the router located in Apartment 242 and pinpointed two unknown devices, "bootycop" (media access control [MAC] address unknown) and "CK" (with a MAC address of 00.25:d3:d4:c4:73).[3] Because the apartment residents could not identify either unknown device, Special Agent Phirippidis concluded that "CK" and "bootycop" accessed the router in Apartment 242 without permission. Neither computer was connected to the router when Special Agent Phirippidis executed the search warrant, but agents attempted to identify the location of the "CK" device using Moocherhunter software (Moocherhunter)[4] and the 00.25:d3:d4:c4:73 MAC address.

With Moocherhunter in passive mode and using a wireless antenna, Special Agent Phirippidis and his colleagues captured signal strength readings to locate the 00.25:d3:d4:c4:73 MAC address. Specifically, Moocherhunter was installed on a laptop computer and connected to a directional antenna. The Moocherhunter

[3] A MAC address is "a unique identifier assigned to a network device for communication on a physical network. A MAC address is most often assigned by the manufacturer of a network device," and differs from an IP address.

[4] As its name implies, Moocherhunter is an open-source wireless tracking software program designed to identify computers trespassing on wireless computer networks. Moocherhunter enables the detection of wireless traffic without directly accessing any device.

program was provided the 00.25:d3:d4:c4:73 MAC address, and approximately seventeen location readings were taken in the vicinity of Apartment 242. The readings were significantly higher when the antennae was aimed in the direction of Apartment 243. As a result, the agents concluded that Apartment 243 housed the "CK" device. After identifying the target apartment, Special Agent Phirippidis waited for "boyforboys1" to log on to the P2P network.

A week later, "boyforboys1" logged onto the P2P network and distributed child pornography from the 69.105.80.128 IP address linked to the wireless router in Apartment 242. Special Agent Phirippidis downloaded child pornography files from "boyforboys1," and went to Apartment 242 to confirm whether "boyforboys1" utilized "CK" or "bootycop" devices to distribute the child pornography. With the consent of a resident of Apartment 242, Special Agent Phirippidis and his colleagues determined that "CK" (with the 00.25:d3:d4:c4:73 MAC address) and "bootycop" (with a MAC address of 00:1f:1f:49:d3:11) were logged into the wireless router belonging to the residents of Apartment 242.

After a period of time, "CK" disconnected from the router, leaving only "bootycop" connected to the router. Again using the Moocherhunter software and a wireless antenna, Special Agent Phirippidis measured the signal strength of MAC address 00:1f:1f:49:d3:11, taking readings from Apartment 242 and from a nearby vacant apartment (with permission from the apartment manager). He concluded that: (1) "CK" and "bootycop" exhibited similar signal strengths; (2) "CK" and "bootycop" were associated with each other; (3) Apartment 243 housed both devices; and (4) both had gained unauthorized access to the password-protected router in Apartment 242.

Based on the Moocherhunter data, Special Agent Phirippidis obtained a search warrant for Apartment 243. When Special Agent Phirippidis and his colleagues executed the search warrant, they discovered evidence of child pornography.

II. PROCEDURAL HISTORY

The government indicted Norris on one count of distribution of material involving the sexual exploitation of minors, in violation of 18 U.S.C. § 2252(a)(2), and one count of possession of material involving the sexual exploitation of minors, in violation of 18 U.S.C. § 2252(a)(4)(B). Norris subsequently moved to suppress the evidence obtained as a result of the search warrant, alleging that use of the Moocherhunter software amounted to a warrantless search in violation of the Fourth Amendment. Norris also moved for a *Franks*[5] hearing on the basis that the search warrant affidavit contained misrepresentations and omissions that materially misled the magistrate judge and negated any probable cause determination. The district court denied both motions.

Addressing the motion to suppress, the district court held that no Fourth Amendment search occurred, because, unlike in *Florida v. Jardines*, 569 U.S. 1 (2013), the agents did not encroach upon Norris's curtilage to determine the location of contraband inside the house. *See id.* at 3, 11–12 (holding that a Fourth Amendment search occurred when police brought a drug-sniffing dog to defendant's porch to determine the presence of drugs inside the residence). In *Jardines*, the Supreme Court clarified that the focus in a Fourth

[5] *Franks v. Delaware*, 438 U.S. 154 (1978).

Amendment inquiry should be on "the traditional property-based understanding of the Fourth Amendment." *Id.* at 11. Thus, if "the government gains evidence by physically intruding on constitutionally protected areas," such as the curtilage of a home, a search has occurred, and no further inquiry is required, including whether the defendant had a reasonable expectation of privacy. *Id.*

Having found that the agents did not physically intrude upon Norris's property as in *Jardines*, the district court proceeded to analyze whether Norris could nevertheless establish that a search occurred under the analysis set forth by the Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967). The *Katz* test has been described as encapsulating two questions. The first question "is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citation and internal quotation marks omitted). The second question measures the objective reasonableness of an individual expectation of privacy by inquiring "whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable." *Id.* (citation and internal quotation marks omitted). The district court answered both questions in the negative as applied to Norris.

The district court concluded that Norris lacked a subjective, reasonable expectation of privacy, because he connected to a third-party's router without authorization and assumed the risk that his signal would reveal the MAC address to authorities. The district court distinguished *Kyllo v. United States*, 533 U.S. 27 (2001), involving the use of thermal-imaging devices to scan the residence to determine the existence of fluorescent lights used in growing marijuana.

The district court also ruled that society was not prepared to recognize an expectation of privacy for an individual who gains unauthorized access to a third-party's password-protected router.

Finally, the district court ruled that Norris failed to meet the standard for a *Franks* hearing. Although the alleged misrepresentations and omissions would likely provide a more complete picture of the reliability of the software, the district court concluded that the alleged misrepresentations and omissions did not invalidate the probable cause finding.

Following trial, the jury convicted Norris on both counts. The district court sentenced Norris to 72 months' imprisonment and 180 months' supervised release. The district court entered final judgment, and Norris timely appealed.

III. JURISDICTION AND STANDARD OF REVIEW

The district court had subject matter jurisdiction under 18 U.S.C. § 3231, and we have jurisdiction under 28 U.S.C. § 1291. We review denial of a motion to suppress *de novo*, and the district court's factual findings for clear error. *See United States v. Zapien*, 861 F.3d 971, 974 (9th Cir. 2017). We also review *de novo* the denial of a *Franks* hearing. *See United States v. Kleinman*, 880 F.3d 1020, 1038 (9th Cir. 2018), *as amended*.

IV. DISCUSSION

A. Fourth Amendment Search

It is undisputed that there was no actual physical intrusion into Norris's apartment. Therefore, we apply the *Katz* test to determine if the agents engaged in a search under the Fourth Amendment. *See Jardines*, 569 U.S. at 11.

1. *Subjective Expectation of Privacy*

To connect to the internet, Norris's devices sent a wireless signal transmitting the MAC address of the devices to the password-protected wireless router in Apartment 242. Once connected, Norris accessed the router to utilize the internet connection without authorization.

Although physically located in his home, Norris's wireless signal reached outside his residence to connect to the wireless router in Apartment 242. The FBI captured Norris's wireless signal strength outside Norris's residence to determine the source of the signal. The FBI's actions may be likened to locating the source of loud music by standing and listening in the common area of an apartment complex. Although the music is produced within the apartment, the sound carries outside the apartment. Just as no physical intrusion "on constitutionally protected areas" would be required to determine the source of the loud music, no physical intrusion into Norris's residence was required to determine the strength of the wireless signal emanating from the devices in his apartment. *Jardines*, 569 U.S. at 11.

We conclude that no subjective expectation of privacy exists under these circumstances, where information is openly

available to third parties. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351 (citations omitted); *see also California v. Ciraolo*, 476 U.S. 207, 213–14 (1986) (holding that use of an aircraft in public airspace to view marijuana plants in the backyard of a home did not violate the Fourth Amendment); *California v. Greenwood*, 486 U.S. 35, 40–41 (1988) (concluding that search of publicly exposed garbage did not violate the Fourth Amendment); *United States v. Borowy*, 595 F.3d 1045, 1047–48 (9th Cir. 2010) (upholding search of computer files using file-sharing software available to the public).

We agree with the district court that *Kyllo* does not dictate the conclusion that a Fourth Amendment search occurred in this case. In *Kyllo*, police officers utilized thermal-imaging technology to scan the inside of a house to detect the presence of heat in amounts consistent with the presence of high-intensity lights used to grow marijuana. *See* 533 U.S. at 29–30. The Supreme Court ruled the scan a search under the Fourth Amendment because the government used "sense-enhancing" technology to obtain information from the *inside* of a home that the police could not otherwise obtain "without physical intrusion into a constitutionally protected area." *Id.* at 34. Unlike in *Kyllo*, where the defendant confined his illegal activities to the interior of his home and relied on the privacy protections of the home to shield these activities from public observation, Norris's activities reached beyond the confines of his home, thereby negating any expectation of privacy. *See Katz*, 389 U.S. at 351.

United States v. Karo, 468 U.S. 705 (1984), is equally distinguishable. In *Karo*, the United States Supreme Court held that the government's monitoring of a beeper inside a

private residence violated the Fourth Amendment because the beeper provided location information that could not have been obtained from outside the curtilage of the house. *See id.* at 708, 714; *see also Silverman v. United States*, 365 U.S. 505, 506, 509–12 (1961) (holding that a Fourth Amendment search occurred when police inserted a "spike mike" into a house to overhear conversations of the house next door); *Jardines*, 569 U.S. at 4 (concluding that a Fourth Amendment search occurred when police used a drug-sniffing dog along the front porch (the curtilage) to establish the location of marijuana inside a house). Unlike in *Karo*, *Silverman*, and *Jardines*, the agents in this case collected information from non-constitutionally protected areas, and they collected no information from inside Norris's residence. Thus, Norris lacked any expectation of privacy in the emission of the signal strength of the MAC address emanating from outside his apartment. *See Borowy*, 595 F.3d at 1047–48.

2. *Societal Recognition of Expectation of Privacy as Reasonable*

Even if Norris harbored a subjective expectation of privacy, that expectation was not one society is prepared to recognize as reasonable. The concept of society's recognition of an expressed expectation of privacy is consistent with the overall focus in Fourth Amendment jurisprudence on reasonableness. *See Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness . . .") (citations and internal quotation marks omitted). If society is not prepared to recognize an expectation of privacy as reasonable, intrusion upon that expectation does not violate the Fourth Amendment's overall reasonableness requirement. *See Kyllo*, 533 U.S. at 33. As the Supreme Court articulated in *Rakas v.*

Illinois, 439 U.S. 128, 143 n.12 (1978), "[o]ne of the main rights attaching to property is the right to exclude others, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy." (citation omitted). Conversely, one has no legitimate expectation of privacy in property for which he lacks any possessory or ownership interest. *See United States v. Wong*, 334 F.3d 831, 839 (9th Cir. 2003).

We have also generally concluded that society is not prepared to recognize as reasonable a subjective expectation of privacy in the content of property obtained through unauthorized means. In *United States v. Caymen*, 404 F.3d 1196, 1197–98 (9th Cir. 2005), Caymen used a third-party's credit card to fraudulently purchase a laptop. The police obtained a search warrant for Caymen's residence and discovered the laptop. *See id.* The police contacted the store owner for approval to review the contents of the laptop. *See id.* at 1198. Once the police discovered child pornography, they immediately ceased their search and obtained another warrant to search for child pornography. *See id.* Caymen was indicted for possession of child pornography and moved to suppress seized photographs on the basis that the police conducted an illegal search. *See id.*

On appeal, we rejected Caymen's challenge of the search, ruling that the Fourth Amendment "does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that society is prepared to accept as reasonable." *Id.* at 1200 (internal quotation marks omitted).

We also find instructive the Third Circuit's decision in *United States v. Stanley*, 753 F.3d 114 (3d Cir. 2014). *Stanley* also involved use of the Moocherhunter software to detect the signal strength of a MAC address from outside the suspected residence. *See id.* at 116. As in our case, the defendant accessed child pornography via a neighbor's wireless service. *See id.* at 115–16. The only difference is that in *Stanley*, the neighbor's wireless service was not password-protected. *See id.* at 116. Under these similar circumstances, the Third Circuit determined that "Stanley's expectation of privacy [in his MAC address signal] is not one that society is prepared to recognize as legitimate." *Id.* at 119 (footnote reference omitted). The Third Circuit concluded that "while Stanley may have justifiably expected the path of his invisible radio waves to go undetected, society would not consider this expectation legitimate given the unauthorized nature of his transmission." *Id.* at 120. Although we do not adopt the entire reasoning espoused by the Third Circuit, we agree that even if a person in Norris's position had a subjective expectation of privacy in the wireless signal transmitted outside his residence, society is not prepared to recognize this expectation as legitimate, given the unauthorized access used to generate the wireless transmission. *See id.* Indeed, it strains credulity to suggest that society would be prepared to recognize an expectation of privacy as reasonable when an individual gains access to the internet through the unauthorized use of a third-party's password-protected router located outside his residence. *See id.*

In sum, we affirm the district court's application of the *Katz* factors to conclude that no Fourth Amendment search occurred. Even if Norris had a subjective expectation of

privacy, it was not one society was prepared to accept as reasonable.

B. *Franks* hearing

A *Franks* hearing determines "the validity of the affidavit underlying a search warrant." *Kleinman*, 880 F.3d at 1038 (citation omitted). To obtain a *Franks* hearing, a defendant must make a substantial preliminary showing that: (1) "the affiant officer intentionally or recklessly made false or misleading statements or omissions in support of the warrant," and (2) "the false or misleading statement or omission was material, *i.e.*, necessary to finding probable cause." *United States v. Perkins*, 850 F.3d 1109, 1116 (9th Cir. 2017) (citation, alteration, and internal quotation marks omitted). Once the defendant makes that showing, to prevail at the subsequent hearing, he must establish both prongs by a preponderance of the evidence. *See United States v. Martinez-Garcia*, 397 F.3d 1205, 1214–15 (9th Cir. 2005).

Norris failed to satisfy the first requirement because he did not present any evidence that Special Agent Phirippidis acted knowingly, intentionally, or with reckless disregard for the truth in preparing the affidavit.

In any event, Norris also failed to satisfy the second requirement for a *Franks* hearing because none of the alleged false statements or omissions materially affected the probable cause determination. "Probable cause to search a location exists if, based on the totality of the circumstances," a "fair probability" exists that the police will find evidence of a crime. *Perkins*, 850 F.3d at 1119 (citation omitted). The key inquiry in resolving a *Franks* motion is whether probable cause remains once any misrepresentations are corrected and

any omissions are supplemented. *See id.* If probable cause remains, the defendant has failed to establish a material omission. *See id.*

Norris argues that the FBI falsely identified Moocherhunter as open-source software rather than proprietary software. Norris also alleges that the following omissions were material: (1) the FBI used a free version of Moocherhunter instead of the law enforcement version; (2) the FBI did not authorize its agents to use Moocherhunter in criminal investigations; (3) the FBI did not train its agents to use Moocherhunter; (4) the FBI did not formally test the software; (5) the FBI disregarded any reading believed to be anomalous or not of value; (6) the FBI agents used an incomplete method; (7) the FBI agents did not provide the magistrate judge with location information in relation to the signal strength; (8) the Moocherhunter developer did not subject the software to any objective or peer-review testing; and (9) Moocherhunter will give false readings when a party changes the MAC address to conceal identity.

If the alleged misrepresentations and omissions were corrected and supplemented, the probable cause determination would not be affected, as a "fair probability" remained that Apartment 243 housed devices containing child pornography. *Id.* (citation omitted). The district court did not err in denying the requested *Franks* hearing. *See id.*

V. CONCLUSION

Because there was no physical intrusion into Norris's residence to detect the signal strength of the MAC address of his device, the district court correctly applied the *Katz* factors and determined that no search occurred under the Fourth

Amendment. Norris lacked a subjective expectation of privacy in the signal strength of his MAC address emanating from his unauthorized use of a third-party's wireless router. In any event, we conclude that society is not prepared to recognize as reasonable an expectation of privacy predicated on unauthorized use of a third-party's internet access. Finally, Norris failed to make a substantial preliminary showing that the search warrant affidavit included any knowingly, intentionally, or recklessly made material misrepresentations or omissions. Moreover, a corrected and/or supplemented affidavit would not have affected the probable cause determination. The district court did not err in denying Norris a *Franks* hearing.

AFFIRMED.