No._____

IN THE SUPREME COURT OF THE UNITED STATES

_____

ALEXANDER NATHAN NORRIS,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

_____

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

_____

PETITION FOR A WRIT OF CERTIORARI

_____

JOHN BALAZS
COUNSEL OF RECORD
Attorney at Law
916 2nd Street, Suite F
Sacramento, CA 95814
(916) 447-9299
john@balazslaw.com

QUESTION PRESENTED

In *Kyllo v. United States*, the Court held that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where (as here) the technology is not in general public use." 533 U.S. 27, 30 (2011). In this case, the court of appeals held that an FBI agent's use of sophisticated software technology not in general public use to obtain information from inside petitioner's residence is not a "search" within the meaning of the Fourth Amendment because it did not invade petitioner's "reasonable expectation of privacy." *United States v. Norris,* 9th Cir. No. 17-10354, 938 F.3d 1114 (9th Cir. 2019) (App. 1-17).

The question presented is whether a law enforcement officer's warrantless use of Moocherhunter software and a directional antenna to locate a computer in petitioner's apartment is a "search" within the meaning of the Fourth Amendment.

LIST OF PARTIES

The parties to the proceedings below were Petitioner, Alexander Nathan Norris, and Respondent, United States of America.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

No._____

IN THE SUPREME COURT OF THE UNITED STATES

_____

ALEXANDER NATHAN NORRIS,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

_____

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

_____

PETITION FOR A WRIT OF CERTIORARI

Petitioner Alexander Nathan Norris respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit in case number 17-10354.

OPINIONS BELOW

The opinion of the court of appeals (App. 1-17) is reported at 938 F.3d 1114. The district court's order denying petitioner's motion to suppress evidence is at App. 18-30.

JURISDICTION

The judgment of the court of appeals was entered on November 4, 2019. App. 1-17. A timely petition for rehearing and rehearing en banc was denied on February 4, 2020. App. 54. This Court has jurisdiction over this petition pursuant to 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL PROVISION

U.S. Constitution, Amendment IV:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

STATEMENT

On April 28, 2011, the government filed an Indictment charging petitioner with one count of distribution of materials containing visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2) (count 1) and one count of possession of materials containing visual depictions of minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(4)(B) (count 2).

Petitioner moved to suppress evidence obtained during execution of a search warrant at his apartment in Davis, California. In his motion, he argued that the warrant was invalid because the affidavit relied on material information obtained through a prior unconstitutional search, that is, the affidavit relied on federal agents' warrantless use of "Moocherhunter" software and a directional antenna to locate a computer within petitioner's home in violation of the Fourth Amendment.

Moocherhunter is a Singapore-made software program with a free version that can be downloaded from its website. App. 125, 127. In the "passive mode" that agents reported using in this case, Moocherhunter works by looking for MAC addresses connected to a router and then

searching for the signal emanating from the device with the MAC address. App. 134-35. By aggregating readings in a manner similar to the way submarines use sonar to locate objects, an individual can use Moocherhunter to find a device that has been connected to a router or has the MAC address that had been entered in the software. App. 134.[1]

After further briefing (dockets 43, 44), the district court held argument on the motion to suppress. App. 31-53. After supplemental briefs were filed, the district court denied the motion. App. 18-30.

At trial, the parties stipulated that the government's undercover agent downloaded visual depictions from petitioner's desktop computer and that at the time of the downloads petitioner knew that the depictions showed one or more real minors engaged in sexually explicit conduct. Docket 212, Reporter's Transcript (RT) 457-58. The jury returned a guilty verdict on both counts. The district court sentenced

---

[1] Although not at issue in this petition, petitioner also argued that the warrant was invalid under *Franks v. Delaware,* 438 U.S. 154 (1976), because the affidavit misled the magistrate judge by omitting, among other things, material information about the unreliability of the software.

Norris to 72 months imprisonment and 180 months supervised release. Docket 189.

On appeal, the Ninth Circuit concluded that the FBI agents' use of Moocherhunter software with a wireless antenna to locate petitioner's computer within his apartment was not a search under the Fourth Amendment because it did not violate a "reasonable expectation of privacy." App. 10-15; *see Katz v. United States,* 389 U.S. 347 (1967). The court first held that Norris lacked any subjective "expectation of privacy in the emission of the signal strength of the MAC address emanating from outside his apartment." App. 10-12. The court then concluded that even if petitioner had a subjective expectation of privacy, there is no Fourth Amendment violation because his expectation is not "one that society is prepared to recognize as 'reasonable'" since he accessed his neighbor's router without authorization. App. 12-15.

The Court should grant certiorari because the Ninth Circuit's decision denigrates Fourth Amendment protections and violates this Court's precedents on an important question in an evolving area of constitutional law. This case also provides a good opportunity for the Court to reevaluate the continuing viability of the *Katz* "reasonable

expectation of privacy test" for determining whether a "search" has occurred under the Fourth Amendment.

REASONS FOR GRANTING THE PETITION

1. The Ninth Circuit's opinion conflicts with *Kyllo v. United States* and other Supreme Court cases in holding that petitioner lacked Fourth Amendment protection where federal agents used sophisticated technology not in general public use (Moocherhunter software) to locate a computer in his residence.

In *Kyllo v. United States,* a federal agent suspected that the defendant was growing marijuana inside his home using high-intensity lamps. 533 U.S. 27, 29 (2001). The agent "used an Agema Themovision 210 thermal imager to scan the triplex" where Kyllo's residence was located. *Id.* at 29-30. "Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye." *Id.* at 29. By detecting infrared radiation, "[a] thermal imager reveals the relative heat of various rooms in the house." *Id.* at 35 n.2. A thermal imager "emits no rays or beams and shows a crude visual image of the heat being radiated from outside [a] house." *Id.* at 30. Thermal imagers "are entirely passive" and measure the infrared

radiation emanating from a building that reaches its sensors. *Id.* at 36 n.3.

In holding that officers violated Kyllo's Fourth Amendment rights, the Court emphasized that "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Id.* at 31. The Court held that where "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40.

Government agents' use of Moocherhunter in this case and the thermal imager used in *Kyllo* made virtually-identical intrusions into a private home. Moocherhunter measures the radio waves, emanating from the wireless card inside Norris's apartment. App. 44. The thermal imager in *Kyllo* measured infrared radiation emitted by the lamps inside the home and received on the street outside the triplex. 533 U.S. at 29. Both the radio waves measured here and the infrared radiation

measured in *Kyllo* are types of electromagnetic radiation.[2] The thermal imager and Moocherhunter each detected electromagnetic radiation emanating from a residence. *Id.* at 35.

As a result, petitioner's case fits squarely within the holding of *Kyllo* that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where (as here) the technology is not in general public use." *Id.* at 30. The government searched petitioner's apartment by using sense-enhancing technology that is not in general

---

[2] Electromagnetic radiation are "waves of electric and magnetic energy moving together (i.e., radiating) through space." Office of Eng'g & Tech., Fed. Commc'n Comm'n, OET Bulletin 56, Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields 1 (4th ed. Aug. 1999). The electromagnetic spectrum

> includes all the various forms of electromagnetic energy from extremely low frequency (ELF) energy, with very long wavelengths, to X-rays and gamma rays, which have very high frequencies and correspondingly short wavelengths. In between these extremes are radio waves, microwaves, infrared radiation, visible light, and ultraviolet radiation, in that order.

Id. at 2.

public use (Moocherhunter software with a directional antenna) to glean information about the interior of his apartment that otherwise could not be obtained without physically intruding into his home.[3] Thus, as in *Kyllo,* agents' use of sense-enhancing technology to measure the electromagnetic radiation emanating from petitioner's apartment should be deemed a search under the Fourth Amendment.

The Ninth Circuit distinguished petitioner's case from *Kyllo*, and other Supreme Court Fourth Amendment cases, namely, *United States v. Karo,* 468 U.S. 705 (1984), and *Silverman v. United States,* 365 U.S. 505 (1961), on the ground that petitioner's "activities reached beyond the confines of his home, thereby negating any expectation of privacy." 938 F.3d at 1120. This distinction ignores critical factual information and sweeps too broadly legally.

---

[3] The record contains no evidence that Moocherhunter was generally used by the public at the time agents used it in this case. *See also United States v. Stanley,* 753 F.3d 114, 119 (3d Cir. 2014) ("the government does not contend that the MoocherHunter is technology that [was] 'in general public use'" when agents used it in 2011); *United States v. Broadhurst,* No. 3:11-CR-00121-MO, 2012 U.S. Dist. Lexis 168893, at * 19 (D. Or. 2012) ("it is worth noting that there is a difference between a device that can be purchased by the public and 'general public use'" as used in *Kyllo*).

Norris did expose certain signal information to his neighbor, including his MAC and IP addresses, by connecting to the router. But in doing so, he did not show either his neighbors or the public the *location* of his laptop computer. *Cf. Bond v. United States,* 529 U.S. 334, 338-39 (2000) ("A bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. . . . We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.") Instead, agents measured radio energy in the area surrounding both apartments, which never reached the neighbor's router, and cannot properly be considered part of the signal. The energy is essentially waste and is unintentional, like the heat energy information that officers collected through a thermal imager in *Kyllo.* 533 U.S. at 30 ("Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye."). Government agents learned the location of petitioner's computer's only through advanced sense-enhancing technology using information that was not sent to his neighbor's router to determine the signal's strength at other locations. *See United States v. Stanley,* 753

F.3d 114, 123 (3d Cir. 2014) ("his wireless signal was composed of radio waves that were associated with a plethora of information, some of which the Neighbor could convey to authorities, but most of which he could not").[4]

By accessing a neighbor's Wi-Fi network without permission, one would expect that the neighbor's router would learn his device's MAC address, but not that the router (or government agents) would be able to search for and locate his computer inside a private residence using that MAC address. Like the beeper placed in a can of ether and taken into a residence in *Karo*, the search for the electronic device here "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing about and that it could not have obtained without a warrant." 468 U.S. at 715; *see also Silverman,* 365

[4] Although the Third Circuit reached the same result in *Stanley* as the Ninth Circuit did here, the Ninth Circuit's opinion here is more expansive. In *Stanley,* the Third Circuit rejected a defendant's claim that officers' use of Moocherhunter technology to conduct a warrantless search of a residence violated the Fourth Amendment. The Third Circuit held that because the defendant did not have an expectation of privacy that society was prepared to accept as reasonable, it need not reach the question of whether he had a subjective expectation of privacy against the government's use of Moocherhunter technology to locate a computer within the defendant's residence. 753 F.3d at 119 n.9.

U.S. at 509 (finding search occurred where government listened in to a residence using a "spike mike," a microphone attached to a spike inserted into the walls of a house). Petitioner therefore maintained an expectation of privacy against government use of sophisticated technology not available to the public to locate a computer that was in his private residence.

The Ninth Circuit also held 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." App. 14; *accord Stanley,* 753 F.3d at 120 ("while [the defendant] 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 the transmission"). The government argued that petitioner fits the example given in *Rakas v. Illinois* of "a burglar plying his trade in a summer cabin during the offseason," who may have a subjective expectation of privacy in the cabin, but "not one that society is prepared to recognize as reasonable." Ans. Brief, at 19, quoting *Rakas v. Illinois,* 439 U.S.

128, 143 n.12 (1978); *Stanley,* 753 F.3d at 120 (citing same example). The Ninth Circuit reasoned that courts have "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." App. 13.

But the comparison would be more apt if petitioner had challenged the search of his neighbor's computer onto which he had surreptitiously downloaded computer files rather than, as in this case, a search into his own apartment. The summer burglar may not have a reasonable expectation of privacy in the summer cabin he broke into, but society would still recognize as reasonable the burglar's expectation of privacy in his own home. Officers who located the stolen property in the burglar's own home using some type of advanced technology not in general public use would thus still be conducting a search for Fourth Amendment purposes.

Likewise, the Ninth Circuit failed in its attempt to analogize this case to one where there is no reasonable expectation of privacy in property because the property was obtained through fraud, robbery, or trespass. App. 13, citing *United States v. Caymen,* 404 F.3d 1196, 1201

(9th Cir. 2005).[5] But again, the analogy does not fit because petitioner did not challenge a search of the neighbor's router that he accessed by trespass or fraud; he moved to suppress a search of his own apartment. Even if he lacked a reasonable expectation of privacy in the transmissions sent to a neighbor's computer by unlawfully accessing it, petitioner stills maintains a reasonable expectation of privacy in his own apartment.

For these reasons, the Court should grant certiorari and hold that the government's use of Moocherhunter in this case constitutes a "search" under the *Katz* reasonable expectation of privacy test.

2. This case also presents an ideal vehicle for the Court to reconsider the *Katz* "reasonable expectation of privacy" test for determining when law enforcement engages in a "search" within the meaning of the Fourth Amendment.

Alternatively, the Court should use this case to reconsider the "reasonable expectation of privacy" test in *Katz* for determining when a

---

[5] The presence of radio waves in the surrounding area or even in the neighbor's apartment does not constitute a trespass as the radio waves would exist in the same places even if Norris had connected to his own router. It is only the signal itself (the information communicated to the neighbor's router) that should be considered a trespass.

Fourth Amendment search occurs. The Fourth Amendment states, in relevant part, that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV.

The Court has generally held that a Fourth Amendment "search" occurs where officers' conduct violates a person's subjective "expectation of privacy" that "society is prepared to recognize as 'reasonable.'" *Katz,* 389 U.S. at 361; *see Carpenter v. United States,* 138 S. Ct. 2206, 2219 (2018) ("when the Government accessed [cell-site location information] from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy"); *see also United States v. Jones,* 565 U.S. 400 (2012) (applying a trespass test to the government's installation of a GPS device on a vehicle, as supplementing the *Katz* privacy-based test). This standard is inconsistent with the ordinary meaning of the word "search" and the history of the Fourth Amendment. As Justice Thomas, among others, has explained, the *Katz* test is without a basis in the text or history of the Fourth Amendment and improperly "invites courts to make judgments about policy, not law." *Carpenter,* 138 S. Ct. at 2236 (Thomas, J., dissenting); *see id.* at 2264 ("*Katz*'s problems start with the

text and original understanding of the Fourth Amendment") (Gorsuch, J., dissenting); *Minnesota v. Carter,* 525 U.S. 83, 97 (1998) (contending that since *Katz,* the determination of what law enforcement conduct interferes with a reasonable expectation of privacy "bear[s] an uncanny resemblance to those expectations of privacy that this Court considers reasonable") (Scalia, J., concurring); Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 Sup. Ct. Rev. 67, 90 (2012) ("The Supreme Court's cases have treated the phrase 'reasonable expectation of privacy' as a term of art.").

The Court should replace the *Katz* test with one more faithful to the ordinary meaning of the word "search" and the history of the Fourth Amendment. "[T]he ordinary meaning of 'search' has remained unchanged since the people ratified the Fourth Amendment over two hundred years ago." *Morgan v. Fairfield City,* 903 F.3d 553, 568 (6th Cir. 2018) (Thapar, J., concurring in part and dissenting in part), *cert. denied,* 139 S. Ct. 1377 (2019). "When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo,*

533 U.S. at 32 n.1 (quoting N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989)). "In other words, officers conduct a search when they engage in a purposeful, investigative act." *Morgan,* 903 F.3d at 568. The history of the Fourth Amendment also "shows that when the Framers used the word 'search,' they meant something specific: investigating a suspect's property with the goal of finding something." *Id.* at 570 (Thapar, J., concurring in part and dissenting in part), and authorities cited therein. "In this way, the original meaning of the term matches the ordinary one." *Id.*

On the other hand, jurists and commentators have criticized the Court's *Katz* jurisprudence as improperly "conflating the [Fourth Amendment's] search inquiry with the reasonableness one." *Id.*; *see also* Akhil R. Amar, *Fourth Amendment First Principles,* 107 Harv. L. Rev. 757, 769 (1994) ("[I]n the landmark *Katz* case, the Court, perhaps unconsciously, smuggled reasonableness into the very definition of the Amendment's trigger . . . ."); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment,* 129 Harv. L. Rev. 1821, 1871 (2016) ("The structure of the doctrine is especially puzzling in the *Katz* regime, which creates a separate reasonableness analysis at the

first step of the Fourth Amendment framework prior to evaluating the reasonableness of the government's conduct at the second step."). "[R]easonableness determines the legality of a search, not 'whether a search . . . within the meaning of the Constitution has *occurred*.'" *Carpenter,* 138 S. Ct. at 2243 (Thomas, J., dissenting) (quoting *Minnesota v. Carter,* 525 U.S. 83, 97 (1998) (Scalia, J., concurring)). "Smuggling both questions into one is not faithful to the Amendment's text and ends up narrowing the scope of the coverage." *Morgan,* 903 F.3d at 571; *Carpenter,* 138 S Ct. at 2246 (Thomas, J., dissenting) (noting that the *Katz* test "threatened to narrow the original scope of the Fourth Amendment").

This case is an excellent one to reconsider *Katz* and replace its test with one more consistent with the ordinary meaning and historical understanding of "search," that is, whether law enforcement officers purposefully engaged in conduct to gather evidence. Under Sixth Circuit Judge's Thapar's proposed test, for example, the FBI agent's use of Moocherhunter software is a "search" because it is a purposeful, investigative act to locate a computer than officers believed contained child pornography. *See Morgan,* 903 F.3d at 572 ("The officers

conducted a search in *Kyllo* because using a thermal imager to determine whether heat is emanating from a house is a purposeful, investigative act."). The *search* into a private residence was unreasonable because it was performed with neither a warrant nor any legitimate justification to excuse one. Without the results of the warrantless Moocherhunter search, there is no question the warrant affidavit lacked probable cause to search petitioner's apartment. Thus, the court of appeals erred in affirming the denial of petitioner's motion to suppress.

CONCLUSION

For these reasons, the Court should grant the petition for a writ of certiorari.

Respectfully submitted,

Dated: March 30, 2020

JOHN BALAZS
Counsel of Record

Attorney for Petitioner
ALEXANDER NATHAN NORRIS