PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 13-1910

UNITED STATES OF AMERICA

v.

RICHARD STANLEY,
Appellant

On Appeal from the United States District Court
for the Western District of Pennsylvania
District Court No. 2-11-cr-00272-001
District Judge: The Honorable Joy Flowers Conti

Argued January 7, 2014

Before: SMITH, SHWARTZ, and SCIRICA,
Circuit Judges

(Filed: June 11, 2014)

Donovan J. Cocas [ARGUED]
Rebecca R. Haywood
Office of United States Attorney
700 Grant Street
Suite 4000
Pittsburgh, PA 15219
Counsel for Appellee

Lisa B. Freeland
Peter R. Moyers [ARGUED]
Office of Federal Public Defender
10001 Liberty Avenue
1500 Liberty Center
Pittsburgh, PA 15222
Counsel for Appellant

OPINION

SMITH, *Circuit Judge.*

Richard Stanley appeals from an order of the United States District Court for the Western District of Pennsylvania denying his motion to suppress evidence that he was in possession of child pornography. Specifically, Stanley argues that a Pennsylvania State Police officer conducted a warrantless search when he used a device called the "MoocherHunter" to trace

Stanley's wireless signal from a neighbor's unsecured wireless router to its source inside Stanley's home. For the reasons that follow, we conclude that the use of the MoocherHunter was not a search within the meaning of the Fourth Amendment. Accordingly, we will affirm the judgment of the District Court.[1]

I.

On November 11, 2010, Corporal Robert Erdely ("Erdely"), the head of the computer crime unit of the Pennsylvania State Police ("PSP"), was investigating the online distribution of child pornography when he discovered a computer on the Gnutella peer-to-peer network[2] sharing 77 files that he suspected contained child pornography. Based on information available to any Gnutella user, Erdely determined that this computer was using file-sharing software with a globally unique identification number of "8754E6525772BA0134C4C6CACF12E300" ("300 GUID") and was connected to the Internet via an Internet

[1] Judge Shwartz joins Parts I through IV.A of this Opinion.

[2] Peer-to-peer networks allow users to share files by connecting to other individual computers directly, without using a centralized administrative system. Gnutella is a particularly large peer-to-peer network and is utilized by a number of popular file sharing programs.

protocol address ("IP address") of "98.236.6.174" ("174 IP Address").

Through a search of publicly available records, Erdely determined that the 174 IP Address was registered to a Comcast Cable ("Comcast") subscriber, and he obtained a court order requiring Comcast to disclose this individual's subscription information. In response, Comcast informed Erdely of the subscriber's name ("the Neighbor") and his home address in Pittsburgh, Pennsylvania.

On November 18, 2010, Erdely executed a search warrant for the Neighbor's home. The search revealed that none of the Neighbor's computers contained either child pornography or the file-sharing software with the 300 GUID. The search also revealed that the Neighbor's wireless Internet router was not password-protected. From this information, Erdely deduced that the computer sharing child pornography was connecting wirelessly to the Neighbor's router from a nearby location without the Neighbor's knowledge or permission.[3] In other words,

[3] To establish a wireless connection, an Internet user selects the desired wireless network from a list of available options displayed on his wireless-enabled device. This causes a wireless card inside the user's device to transmit radio waves to the wireless router, which then transmits radio waves back to the device. This exchange of radio waves

Erdely determined that the computer in question was "mooching" off the Neighbor's Internet connection.

With the Neighbor's permission, Erdely connected a police computer to the router in order to determine the media access control address ("MAC address") and private IP address of any other devices that were connected wirelessly at the time.[4] From this data, Erdely determined that the mooching computer was not connected at that time. With the Neighbor's permission, Erdely left the police computer attached to the router so it could be accessed remotely from Erdely's office in Harrisburg, Pennsylvania.

On January 19, 2011, while working in Harrisburg, Erdely learned that the computer associated with the 300 GUID was again sharing child pornography on the IP address assigned to the Neighbor. By remotely accessing the police computer he had left in the Neighbor's home, Erdely determined that the mooching computer had a private IP address of "192.168.2.114" (the "114 Private IP Address") and a MAC address of "mac=00-1C-B3-B4-48-95" (the "95 MAC Address"). Erdely searched online for the "mac" prefix in the 95 MAC address and discovered that it belonged to an Apple wireless card.

---

comprises the "wireless signal" that connects the device to the router.

[4] This information was available to any computer connected to the Neighbor's router.

Because Erdely had not discovered any Apple wireless devices in the Neighbor's home, this information reinforced his conclusion that the 95 MAC Address and the 114 Private IP Address belonged to the mooching computer. Erdely decided to travel to Pittsburgh so that he could use a "MoocherHunter" device to attempt to determine this computer's location.

The aptly-vernacularized MoocherHunter is a mobile tracking software tool that can be downloaded for free from the manufacturer's website and used by anyone with a laptop computer and a directional antenna.[5] This device can be used in either "active mode" or "passive mode." In "passive mode," the user enters the MAC address of the wireless card he wishes to locate and the program measures the signal strength of the radio waves emitted from this card.[6] These signal strength readings increase as the user aims the antenna in the direction of the mooching computer and moves closer to its location.

Before using the MoocherHunter, Erdely contacted an Assistant United States Attorney in the Western District of Pennsylvania to discuss the propriety of

---

[5] Though MoocherHunter is the name of the software, for the sake of convenience this opinion will refer to this software and the equipment using it collectively as "the MoocherHunter."

[6] The mechanics of "active mode" are not relevant to this appeal.

obtaining a search warrant.[7] Erdely and the AUSA had a "lengthy discussion" in which they decided that the MoocherHunter was "completely different" from the infrared technology used in *Kyllo v. United States*, 537 U.S. 27 (2001). J.A. 271. They also discussed the practical impossibility of obtaining a search warrant without knowing which one of the many nearby residences the signal was being transmitted from. Ultimately, Erdely determined that he needed to proceed without a warrant.

On the evening of January 19, 2011, Erdely arrived at the Neighbor's home and entered the 95 MAC Address into the MoocherHunter. From the residence, he found that the MoocherHunter's readings were strongest (67) when he aimed the antenna at a six-unit apartment complex across the street. From the public sidewalk in front of this building, the MoocherHunter's readings were strongest (100) when Erdely aimed the antenna directly at Stanley's apartment.

That night, Erdely used this information to obtain a search warrant for Stanley's home. Shortly thereafter, Erdely and other PSP officers executed this warrant. When these officers arrived, Stanley initially fled through a back door. He soon returned, however, and confessed

[7] Ederly reached out to the AUSA after unsuccessfully attempting to contact an attorney at the Allegheny County District Attorney's Office.

that he had connected to the Neighbor's router to download child pornography. Erdely seized Stanley's Apple laptop and later recovered 144 images and video files depicting child pornography.

II.

As a result of Erdely's meticulous investigation, a federal grand jury in the Western District of Pennsylvania returned a one-count indictment charging Stanley with possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). Stanley was arrested and initially pled not guilty.

On April 13, 2012, Stanley filed a motion to suppress his statements to Erdely and the evidence obtained from his home and computer. His primary argument was that Erdely conducted a warrantless search under *Kyllo v. United States*, 533 U.S. 27 (2001), when he used the MoocherHunter to obtain information about the interior of his home that was unavailable through visual surveillance.[8]

On November 14, 2012, the District Court denied Stanley's motion. Citing *Smith v. Maryland*, 442 U.S.

[8] Stanley also argued that Erdely's search warrant was not supported by probable cause and that the MoocherHunter was a "mobile tracking device" which required a warrant under 18 U.S.C. § 3117. He has abandoned these arguments on appeal.

735 (1979), the District Court held that Stanley lacked a reasonable expectation of privacy in his wireless signal because he "exposed his wireless signal to a third party and assumed the risk that the signal would be revealed to authorities." J.A. 23. The District Court also rejected Stanley's *Kyllo* argument, explaining that "although the defendant [in *Kyllo*] caused the heat by using high-intensity lamps, he did not send it to a third party and to the extent he could, he contained the heat in his garage." *Id.* at 27. Stanley, on the other hand, "had to . . . initiate contact" with the Neighbor's router and therefore "did not have a reasonable expectation of privacy in that wireless signal simply because it emanated from a computer located inside of his home." *Id.* Finally, the District Court noted that if Stanley had shared child pornography through his own Internet subscription, Erdely could have discovered his location the same way he discovered the Neighbor's: by subpoenaing his Internet service provider for subscription information. *Id.* at 28. "That [Stanley] established an unauthorized connection," the District Court reasoned, "does not convert his subjective expectation of privacy into a reasonable one." *Id.*

Thereafter, Stanley entered into an agreement with the government, under which he would plead guilty but reserve the right to appeal the District Court's order denying his motion to suppress. After his guilty plea was entered, the District Court sentenced Stanley to 51

months in prison. This timely appeal followed.

III.

The District Court had subject matter jurisdiction pursuant to 18 U.S.C. § 3231. We have jurisdiction under 28 U.S.C. § 1291.

"With respect to a suppression order, we review the District Court's factual findings for clear error and exercise plenary review over its legal determinations." *United States v. Ritter*, 416 F.3d 256, 261 (3d Cir. 2005) (internal citations omitted).

IV.

"There are two ways in which the government's conduct may constitute a 'search' implicating the Fourth Amendment." *Free Speech Coal., Inc. v. Att'y Gen. of U.S.*, 677 F.3d 519, 543 (3d Cir. 2012). First, a search occurs when the government "unlawfully, physically occupies private property for the purpose of obtaining information." *Id.* (citing *United States v. Jones*, 132 S.Ct. 945, 949–52 (2012)). Alternatively, a search occurs when the government violates an individual's expectation of privacy that "society recognizes as reasonable." *Kyllo*, 533 U.S. at 33 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

Stanley does not contend that Erdely physically trespassed on his property at any point during his investigation. Nor would that argument have been successful; Erdely did not physically enter Stanley's property until after he obtained a search warrant for the apartment. Instead, Stanley argues that Erdely violated his reasonable expectation of privacy when he used the MoocherHunter to trace Stanley's wireless signal back to the interior of his home.

Determining whether this second type of search occurred involves two questions: "(1) whether the individual demonstrated an actual or subjective expectation of privacy in the subject of the search or seizure; and (2) whether this expectation of privacy is objectively justifiable under the circumstances." *Free Speech Coal., Inc.*, 677 F.3d at 543. To be objectively justifiable, a defendant's expectation of privacy must be more than rational; society must be willing to recognize it as legitimate. *See United States v. Jacobsen*, 466 U.S. 109, 122 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities."); *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("Obviously, however, a 'legitimate' expectation of privacy by definition means more than a subjective expectation of not being discovered.").

A.

The thrust of Stanley's argument on appeal is that Erdely's use of the MoocherHunter was an unlawful search under *Kyllo*. We disagree, and hold that Stanley's expectation of privacy is not one that society is prepared to recognize as legitimate.[9]

In *Kyllo*, police officers suspected that the defendant was growing marijuana inside of his home. 533 U.S. at 29. Without obtaining a warrant, these officers parked across the street and scanned the defendant's home using a thermal imager. *Id.* at 29–30. This device revealed that certain portions of the home's exterior were unusually warm, leading police to believe that the defendant was using high-powered halide lamps inside. *Id.* at 30. The Supreme Court held that this scan was a search, and established a rule 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 in question is not in

[9] The Government argues that Stanley did not proffer any evidence of a subjective expectation of privacy. Because we find that any such expectation would not have been objectively justifiable, we need not reach the question of whether Stanley adequately demonstrated that he subjectively held it.

general public use." *Id.* at 34 (internal quotation marks and citation omitted).

One could argue that this language, considered in the abstract, encompasses Erdely's use of the MoocherHunter. The MoocherHunter, like the thermal imager in *Kyllo*, is surely "sense-enhancing technology," as it detects radio waves which cannot be perceived by unaided human senses. Further, Erdely used this sense-enhancing technology to obtain "information regarding the interior of [Stanley's] home that could not otherwise have been obtained without physical intrusion": the fact that a wireless card associated with particular Internet activity was located there. *Id*. *See also United States v. Karo*, 468 U.S. 705, 714–18 (1984) (holding that the government's use of a tracking device to discover that a particular barrel was located inside the defendant's home was a search for purposes of the Fourth Amendment). Finally, the government does not contend that the MoocherHunter is technology that is "in general public use."

Critical to *Kyllo*'s holding, however, was the fact that the defendant sought to confine his activities to the interior of his home. He justifiably relied on the privacy protections of the home to shield these activities from public observation. *See Kyllo*, 533 U.S. at 34 (characterizing the thermal imaging scan as a "search of the interior of [Kyllo's] home[]," which it considered to be "the prototypical . . . area of protected privacy"). *See*

also id. at 37 ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.") (emphasis in original). Stanley can make no such claim.

Stanley made no effort to confine his conduct to the interior of his home. In fact, his conduct—sharing child pornography with other Internet users via a stranger's Internet connection—was deliberately projected *outside* of his home, as it required interactions with persons and objects beyond the threshold of his residence. In effect, Stanley opened his window and extended an invisible, virtual arm across the street to the Neighbor's router so that he could exploit his Internet connection. In so doing, Stanley deliberately ventured beyond the privacy protections of the home, and thus, beyond the safe harbor provided by *Kyllo*. *See United States v. Broadhurst*, No. 3:11-cr-00121-MO-1, 2012 WL 5985615, at *5 (D. Or. Nov. 28, 2012) (distinguishing the use of a MoocherHunter-like device from the thermal scan in *Kyllo* because "in *Kyllo*, the heat signals were not being intentionally sent out into the world to connect publicly with others."); *United States v. Norris*, No. 2:11-cr-00188-KJM, 2013 WL 4737197, at *7 (E.D. Cal. Sept. 3, 2013) ("In this case the agents used Moocherhunter to pick up signals the defendant was voluntarily transmitting to [his neighbor's router], not information confined to the private area of defendant's home.").

Stanley cannot avail himself of the privacy protections of his home merely because he initiated his transmission from there. *See Smith*, 442 U.S. at 743 ("The fact that [Smith] dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would."). Most importantly, 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. *Rakas*, 439 U.S. at 143 n.12.

As noted in *Rakas*, "[a] burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate.'" *Id.* The defendant's presence in those circumstances "is wrongful; his expectation is not one that society is prepared to recognize as reasonable." *Id.* (internal quotation marks and citation omitted). Similarly, in *United States v. Kennedy*, 638 F.3d 159, 165 (3d Cir. 2011), we held that an unauthorized driver in a rental car lacks a reasonable expectation of privacy in the vehicle in part because he "not only acts in contravention of the owner's property rights, but also deceives the owner of the vehicle."

Here, the presence of Stanley's unauthorized signal was itself "wrongful." When Stanley deliberately connected to the Neighbor's unsecured wireless network, he essentially hijacked the Neighbor's router, forcing it to relay data to Comcast's modem and back to his computer, all without either the Neighbor's or Comcast's knowledge or consent. Stanley was, in effect, a virtual trespasser. As such, he can claim no "legitimate" expectation of privacy in the signal he used to effectuate this trespass—at least where, as here, the MoocherHunter revealed only the path of this signal and not its contents.

The presence of Stanley's signal was likely illegal. A large number of states, including Pennsylvania, have criminalized unauthorized access to a computer network.[10] A number of states have also passed statutes penalizing theft of services,[11] which often explicitly

---

[10] *See, e.g.*, Cal. Penal Code § 502; Colo. Rev. Stat. Ann. § 18-5.5-102; Del. Code Ann. tit. 11, § 932; Fla. Stat. Ann. § 815.06; Ind. Code Ann. § 35-43-2-3; Iowa Code Ann. § 716.6B; La. Rev. Stat. Ann. § 14:73.8; Mo. Ann. Stat. § 569.099; N.H. Rev. Stat. Ann. § 638:17; N.J. Stat. Ann. § 2C:20-25; Okla. Stat. Ann. tit. 21, § 1953; S.C. Code Ann. § 16-16-20; 18 Pa. Cons. Stat. Ann § 7611; Tex. Penal Code Ann. § 33.02; Vt. Stat. Ann. tit. 13, § 4102; W. Va. Code Ann. § 61-3C-5.

[11] *See, e.g.*, Ala. Code § 13A-8-10; Ariz. Rev. Stat. Ann. § 13-1802; Del. Code Ann. tit. 11, § 845; 720 ILCS 5/16-14; Ky. Rev. Stat. Ann. § 514.060; Mont. Code Ann. § 45-6-305;

include telephone, cable, or computer services.[12] We need not decide here whether these statutes apply to wireless mooching,[13] but the dubious legality of Stanley's conduct bolsters our conclusion that society would be unwilling to recognize his privacy interests as "reasonable." This is particularly so where the purpose

---

N.H. Rev. Stat. Ann. § 637:8; N.J. Stat. Ann. § 2C:20-8; 18 Pa. Cons. Stat. Ann. § 3926; Utah Code Ann. § 76-6-409.3; Vt. Stat. Ann. tit. 13, § 2582.

[12] *See, e.g.*, Ariz. Rev. Stat. Ann. § 13-1801; Del. Code Ann. tit. 11, § 857; N.J. Stat. Ann. § 2C:20-8; Or. Rev. Stat. Ann. § 164.125; Wash. Rev. Code Ann. § 9A.56.010; 18 Pa. Cons. Stat. Ann. § 3926. *See also* Alaska Stat. Ann. § 11.46.200 ("A person commits theft of services if . . . the person obtains the use of . . . a computer network . . . with reckless disregard that the use by that person is unauthorized."); Iowa Code Ann. § 714.1 ("A person commits theft when the person . . . [k]nowingly and without authorization accesses . . . a . . . computer network . . . for the purpose of obtaining computer services.").

[13] Some commentators consider the legality of wireless mooching to be an open question. *See, e.g.*, Grant J. Guillot, *Trespassing Through CyberSpace; Should Wireless Piggybacking Constitute a Crime or Tort Under Louisiana Law?*, 69 La. L. Rev. 389, 399 (2009); Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of WI-FI and the Law*, 21 Santa Clara Computer & High Tech. L.J. 101, 145 (2004); Matthew Bierlein, Note, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 Ohio St. L.J. 1123, 1165 (2006).

of Stanley's unauthorized connection was to share child pornography.[14]

To recognize Stanley's expectation of privacy as "legitimate" would also reward him for establishing his Internet connection in such an unauthorized manner. As the District Court recognized, had Stanley shared child pornography using his own, legitimate Internet connection, Erdely could have obtained Stanley's address from his Internet service provider—just as he obtained the Neighbor's address from Comcast. *See United States v. Christie*, 624 F.3d 558, 573–74 (3d Cir. 2010) ("Federal courts have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.") (internal quotation marks and citations omitted). Stanley cannot conceal his location by establishing an unauthorized connection and at the same time ask society to validate his expectation of privacy in the signal-strength information that police used to determine that location in a more roundabout manner. *See Broadhurst*, 2012 WL 5985615 at *5 (refusing to allow the defendant to "serendipitously receive Fourth Amendment protection because he hijacked another person's Internet connection to share child pornography

[14] *Cf.* La. Rev. Stat. Ann. § 14:73.8 (penalizing "accessing . . . of any . . . computer network . . . for purposes of uploading, downloading, or selling of pornography involving juveniles").

files").

Although the analogy is imperfect, we believe that the MoocherHunter is akin to a drug sniffing dog in that it was only able to detect a signal that was itself unauthorized and likely illegal. The use of a drug sniffing dog, which allows police to detect odors that they could not perceive with their human senses, is not a search under the Fourth Amendment because it "discloses only the presence or absence of narcotics, a contraband item." *United States v. Place*, 462 U.S. 696, 707 (1983). *See also id.* ("[A drug sniffing dog] does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage."). In this way, "the manner in which information is obtained through this investigative technique is much less intrusive than a typical search." *Id.* Thus, "[t]he legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from [a defendant's] hopes or expectations concerning the nondetection of contraband." *Illinois v. Caballes*, 543 U.S. 405, 410 (2005).

Here, the MoocherHunter detected only a signal that was itself unauthorized, and as we have characterized it, likely illegal. At the time Erdely used the MoocherHunter, Stanley was connecting to the Neighbor's router without his knowledge or consent.

Without that contemporaneous unauthorized connection, the MoocherHunter would have been unable to function. And the MoocherHunter revealed only the path of the signal establishing this connection. It revealed nothing about the content of the data carried by that signal. Accordingly, Stanley's privacy expectations concerning the path of his unauthorized signal are "categorically distinguishable" from expectations he would have had concerning the path of a lawful, legitimate signal. *Caballes*, 543 U.S. at 410.

B.

While we conclude that Stanley lacked a reasonable expectation of privacy in the path of his unauthorized signal, we believe the able District Judge went too far when she held that "Stanley exposed his signal to a third party and assumed the risk that the signal would be revealed to the authorities." J.A. 23. Other district courts have embraced this theory as well. *See Norris*, 2013 WL 4737197 at *7–8; *Broadhurst*, 2012 WL 5985615 at *5. Because of that, we believe it appropriate to address why we consider this a flawed approach.[15]

[15] Because we hold that Stanley lacked a reasonable expectation of privacy, Judge Shwartz finds it unnecessary to discuss the third-party doctrine and *Smith v. Maryland*. In addition, Judge Shwartz has a different view concerning the doctrine's applicability to the facts of this case. From her

In *Smith*, a robbery victim told police that she was receiving harassing phone calls from a man identifying himself as the robber. 442 U.S. at 737. Suspecting this man to be Michael Smith, police asked Smith's telephone company to install a pen register that would record the phone numbers he dialed from his home phone. *Id.* When the register confirmed that Smith had dialed the victim's number, police obtained a search warrant for his home and discovered additional incriminating evidence. *Id.* After he was indicted, Smith moved to suppress this evidence on the basis that police officers conducted an unconstitutional warrantless search. *Id.*

---

perspective, even though Stanley's transmissions to the Neighbor's router did not specifically disclose his location, he voluntarily disclosed information to surreptitiously obtain his neighbor's internet service that his neighbor could use to find him. A cybertrespasser like Stanley assumes the risk that his neighbor (the trespassed upon party) would take steps to discover his whereabouts and share whatever clues he has with the police, including those that provide a link that leads to his location. Like a footprint, the information that Stanley conveyed to the neighbor's router may not in and of itself disclose his location, but it did provide a lead and by leaving it behind, Stanley assumed the risk it would be pursued. Thus, to the extent it is necessary to discuss the third-party doctrine, Judge Shwartz would conclude that, on the facts of this case, it provides another ground on which to affirm the District Court's ruling that the use of the MoocherHunter here did not violate the Fourth Amendment.

In upholding Smith's conviction, the Supreme Court acknowledged that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" because that person "assume[s] the risk" that this third party will convey this information to the police. *Id.* at 743–44 (internal citations omitted). As an example, the Court cited its prior holding that "a bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to banks and exposed to their employees in the ordinary course of business." *Id.* at 744 (internal quotation marks and citation omitted). The Court then explained that "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 744. Accordingly, "petitioner assumed the risk that the company would reveal to police the numbers he dialed." *Id.*

In Stanley's case, the District Court held that "[b]ased upon *Smith*'s rationale, . . . Stanley did not have a legitimate expectation of privacy in the wireless signal he caused to emanate from his computer to the Kowikowski wireless router." J.A. 20. The District Court explained:

> The information logged on that wireless router was accessible to [the Neighbor] and

> through his consent, to Erdely. This information showed the private IP address of Stanley's computer. Stanley, therefore, could have no reasonable expectation of privacy in the signal he was sending to or receiving from [the Neighbor]'s wireless router in order to connect to the internet.

J.A. 21. Accordingly, the District Court held that "Stanley exposed his wireless signal to a third party and assumed the risk that the signal would be revealed to the authorities." J.A. 23.

We regard the District Court's reasoning as flawed because Stanley's wireless signal was not itself "information" that could be "conveyed" to authorities. *Smith*, 442 U.S. at 744. Rather, 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. Specifically, Stanley, through transmission of his wireless signal, disclosed to the Neighbor his MAC address, his private IP address, and the fact that his wireless card was communicating with Stanley's router at particular points in time. Stanley, therefore, assumed the risk that the Neighbor would convey this information to Erdely.

Erdely, however, did not simply take this information to a magistrate and obtain a search warrant. Rather, Erdely used this information to conduct an additional investigative step that revealed additional information. Specifically, Erdely entered Stanley's MAC address into a sense-enhancing device, which he then used to obtain additional information about the strength of Stanley's signal at different physical locations. It was this additional information that Erdely used to obtain a warrant for Stanley's home. Yet Stanley did not "assume the risk" that the Neighbor would divulge this information because the Neighbor never possessed it. And if the Neighbor had possessed it, Erdely would not have needed the MoocherHunter in the first place.[16]

Were we to hold that Stanley exposed his "signal" under *Smith* by transmitting it to a third-party router, we might open a veritable Pandora's Box of Internet-related

[16] The District Court also appears to have erroneously equated Stanley's wireless signal with the private IP address assigned to that signal. *See* J.A. 21 ("An internet subscriber does not have a reasonable expectation of privacy in his IP address . . . , and likewise, a person connecting to another person's wireless router does not have an expectation of privacy in that connection, i.e. the private IP address, when it is available to that third person and anyone with whom that person shares the information."). Just as a home is more than the address assigned to it, a wireless signal, as discussed above, is more than just its private IP address.

privacy concerns. The Internet, by its very nature, requires *all* users to transmit their signals to third parties. Even a person who subscribes to a lawful, legitimate Internet connection necessarily transmits her signal to a modem and/or servers owned by third parties. This signal carries with it an abundance of detailed, private information about that user's Internet activity. A holding that an Internet user discloses her "signal" every time it is routed through third-party equipment could, without adequate qualification, unintentionally provide the government unfettered access to this mass of private information without requiring its agents to obtain a warrant. We doubt the wisdom of such a sweeping ruling, and in any event, find it unnecessary to embrace its reasoning.

V.

We conclude that Stanley lacked a reasonable, legitimate expectation of privacy in the wireless signal. While Stanley is neither sheltered by *Kyllo* nor defeated by *Smith*, the unauthorized nature of his connection to the Neighbor's router eliminates the possibility that society would recognize his privacy expectations as legitimate. Accordingly, we will affirm the judgment of the District Court.