Boston College Law Review

Volume 56
Issue 6 *Electronic Supplement*

Article 2

5-13-2015

Everybody's Going Surfing: The Third Circuit Approves the Warrantless Use of Internet Tracking Devices in *United States v. Stanley*

Emily W. Andersen
Boston College Law School, emily.andersen@bc.edu

EVERYBODY'S GOING SURFING: THE THIRD CIRCUIT APPROVES THE WARRANTLESS USE OF INTERNET TRACKING DEVICES IN *UNITED STATES v. STANLEY*

Abstract: On June 11, 2014, in *United States v. Stanley*, the U.S. Court of Appeals for the Third Circuit held that the warrantless use of a tracking device to detect the location of a wireless signal was not a search in violation of the Fourth Amendment. The court reasoned that because the defendant was using his neighbor's open wireless network, the defendant did not have a reasonable expectation of privacy. The court's reasoning was based on a belief that the use of an open wireless network, which is not password protected, is "likely illegal." This comment argues that the Third Circuit erred in refusing to recognize the applicability of the test for "sense-enhancing devices" derived from the 2001 U.S. Supreme Court decision *Kyllo v. United States*. Further, the Third Circuit's holding imperils an activity that many law-abiding citizens engage in daily.

INTRODUCTION

The rapid pace of technological innovation presents a constant challenge for law enforcement, legislatures, and the legal system to keep pace with criminal use of technology.[1] Determined individuals continue to find creative new ways to use technology to engage in criminal activity, while equally determined law enforcement officials seek to thwart them.[2] Legislators and courts are left to face these innovations as they arise, often without fully understanding the consequences to the general public.[3]

---

[1] *See, e.g.*, Matthew Bierlein, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 OHIO ST. L. J. 1123, 1125 (2006) (reflecting on the difficulty of applying the law to new technologies while keeping in mind potential ramifications); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487–88 (2011) (arguing that the Supreme Court's application of the Fourth Amendment evolves as technology changes); Amy E. Wells, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 99 (2000) (arguing that the Internet has made such rapid advances that the law can no longer keep pace).

[2] *See* Kerr, *supra* note 1, at 486 (noting that as criminals find new ways to commit crimes, police likewise make use of new methods to solve those crimes). *See generally* U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER NETWORKS (2007), *available at* https://www.ncjrs.gov/pdffiles1/nij/210798.pdf, *archived at* https://perma.cc/CCA9-EVBX (identifying various methods of using technology to detect computer and online criminal activity).

[3] *See* Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 COMMLAW CONSPECTUS 63, 70 (1995) (stating that legislators cannot fashion adequate laws

In June 2014, in *United States v. Stanley*, the U.S. Court of Appeals for the Third Circuit faced a question regarding the legality of tracking technology used by the Pennsylvania State Police.[4] Law enforcement used this technology to locate the defendant, Richard Stanley, who was suspected of transmitting child pornography by "mooching" off of his neighbor's unprotected wireless Internet signal.[5] The technology traced the source of the defendant's wireless signal using an antenna and software called "Moocherhunter™."[6] The Third Circuit held that use of this technology by the police, which located Stanley while he was using his computer within his home, was not an unlawful search.[7] The Third Circuit, therefore, affirmed the lower court's ruling that a warrant was not required to use the technology.[8]

This Comment argues that the Third Circuit should have applied the test for sense-enhancing devices and should not have applied the expectation of privacy test to reach its holding.[9] Part I of this Comment reviews the current state of Fourth Amendment jurisprudence in regard to unreasonable searches and discusses the facts and procedural posture of *Stanley* in the district court.[10] Part II explores the reasoning behind the Third Circuit's holding that Stanley did not have a reasonable expectation of privacy when using the unprotected wireless signal emanating from his neighbor's wireless router.[11] In

---

until they understand the technology they are regulating); Eli R. Shindelman, *Time for the Court to Become "Intimate" with Surveillance Technology*, 52 B.C. L. REV. 1909, 1911 (2011) (arguing that surveillance technology has advanced faster than Fourth Amendment jurisprudence).

[4] *See* United States v. Stanley (*Stanley II*), 753 F.3d 114, 115–16 (3d Cir. 2014) (describing the technology), *cert. denied*, 135 S. Ct. 507 (2014).

[5] *See id.* at 116–17.

[6] *Id.* at 116. Mirroring the Third Circuit's opinion, future references to Moocherhunter encompass the software as well as the computer and directional antenna that are used with the software. *See id.* at 116 n.5.

[7] *See id.* at 115.

[8] *See id.* Other circuits have not yet ruled on whether a warrant is required before using similar technology to locate individuals suspected of computer and/or Internet crimes. *See* Response Brief for the United States at 41, *Stanley II*, 753 F.3d 114 (No. 13-1910), 2013 WL 5427843, at *41. District courts have applied the third party doctrine from *Smith v. Maryland*, 442 U.S. 735 (1979), to the same or similar technology. *See Stanley II*, 753 F.3d at 122. In 2013, in *United States v. Norris*, the U.S. District Court for the Eastern District of California cited the lower court's opinion in *Stanley* and found that use of the same technology, Moocherhunter, to locate the defendant did not require a warrant. *See* No. 2:11–cr–00188–KJM, 2013 WL 4737197, at *8 (E.D. Cal. Sept. 3, 2013). The court reached that decision by applying the third party doctrine. *See id.* In 2012, in *United States v. Broadhurst*, the U.S. District Court for the District of Oregon found that evidence obtained after police used similar technology to locate defendant and obtain a search warrant was not admissible because police trespassed on defendant's property in order to use the technology. *See* No. 3:11–cr–00121–MO–1, 2012 WL 5985615, at *6 (D. Or. Nov. 28, 2012). Apart from police error, the court applied the third party doctrine and found that use of the technology would not have required a warrant. *See id.* at *4.

[9] *See infra* notes 75–111 and accompanying text.

[10] *See infra* notes 13–57 and accompanying text.

[11] *See infra* notes 58–74 and accompanying text.

closing, Part III argues that the Third Circuit's holding misapplies U.S. Supreme Court precedent and exposes law-abiding Internet users to an unreasonably limited protection of their Fourth Amendment rights.[12]

I. (UN)REASONABLE SEARCHES: EXTENDING PROTECTION FROM THE HOME TO THE INDIVIDUAL

In response to the exponential growth in technological innovation that began in the mid-twentieth century, Fourth Amendment jurisprudence has shifted from its singular focus on a property-based conception of protecting the home.[13] The U.S. Supreme Court has recognized the Fourth Amendment's applicability to an individual's privacy interests outside of the home.[14] Section A reviews the property-based focus of Fourth Amendment jurisprudence and discusses the shift towards protecting privacy outside of the home.[15] Section B discusses the Supreme Court's recent insistence that privacy protections have not usurped the essential Fourth Amendment protection of the home.[16] Section C reviews the facts and procedural posture of *Stanley*.[17]

A. Fourth Amendment Protection Begins at Home

Fourth Amendment jurisprudence traditionally emphasized the sanctity of the home.[18] The Fourth Amendment prohibits law enforcement from conducting unreasonable searches of "persons, houses, papers, and effects."[19] Generally, a search requires a court-issued warrant that identifies probable

---

[12] *See infra* notes 75–111 and accompanying text.

[13] *See* Katz v. United States, 389 U.S. 347, 353 (1967) (overruling precedent that required a physical trespass to invoke Fourth Amendment protection against a search); Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1294 (1981) (noting the *Katz* court's shift from focusing on property rights when applying the Fourth Amendment).

[14] *See Katz*, 389 U.S. at 353 (holding that recording defendant's conversation from the exterior of a telephone booth was a violation of his Fourth Amendment right to privacy).

[15] *See infra* notes 18–32 and accompanying text.

[16] *See infra* notes 33–39 and accompanying text.

[17] *See infra* notes 40–57 and accompanying text.

[18] *See* U.S. CONST. amend. IV; Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."); Boyd v. United States, 116 U.S. 616, 630 (1886) (noting the Fourth Amendment's protection of an individual's personal property and security).

[19] *See* U.S. CONST. amend. IV. Fourth Amendment protections also apply to state actors through the Fourteenth Amendment. *See* Mapp v. Ohio, 367 U.S. 643, 660 (1961) (holding that the exclusion of evidence obtained without a warrant in federal courts extends to state courts by virtue of the Fourteenth Amendment).

cause and specifies the location of the proposed search.[20] Because the Fourth Amendment provides protection against *unreasonable* searches, reasonable searches do not require a warrant.[21] Fourth Amendment jurisprudence simultaneously protects individuals from unreasonable government intrusion and seeks to incentivize state and federal law enforcement to work within the boundaries of the law.[22] Accordingly, the Supreme Court has held that evidence obtained in an unlawful search cannot be used to establish a criminal defendant's guilt.[23]

Until the late 1960s, the Fourth Amendment was limited to protection against physical trespass of the home or property.[24] In 1967, in *United States v. Katz*, the U.S. Supreme Court—recognizing the increasing threat to privacy from advancing technology—extended the scope of Fourth Amendment protections to privacy interests outside of the home.[25] This change was initiated when the Supreme Court held that unlawful searches are not limited to physical intrusions.[26] In short, the Supreme Court held that the Fourth Amendment protects "people, not places."[27]

---

[20] *See* U.S. CONST. amend. IV ("[N]o 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.").

[21] *See* Warden v. Hayden, 387 U.S. 294, 298 (1967) (holding that the search of a home without a warrant was reasonable because police were in pursuit of an armed robber known to have entered the premises); United States v. Rabinowitz, 339 U.S. 56, 60 (1950) (holding that the Framers reserved the government's power to conduct reasonable searches without a warrant); Carroll v. United States, 267 U.S. 132, 147, 149, 162 (1925) (holding that police had probable cause for suspicion of illegal activity by defendant so that evidence obtained from defendant's car without a warrant was admissible).

[22] *See Mapp*, 367 U.S. at 647–48 (citing Weeks v. United States, 232 U.S. 383, 393 (1914)) (stating that the well-intentioned efforts of police to gather evidence against guilty parties cannot be pursued outside the scope of individuals' constitutional rights); McDonald v. United States, 335 U.S. 451, 455–56 (1948) (emphasizing the necessity of interposing a neutral judge between police and their ability to search a home); Ashdown, *supra* note 13, at 1289 (arguing that law enforcement is unlikely to regulate itself by sacrificing crime prevention in order to protect individual rights).

[23] *See Mapp*, 367 U.S. at 644–45, 655 (holding that evidence obtained after police forcibly entered defendant's home without a warrant was inadmissible).

[24] *See Katz*, 389 U.S. at 353 (focusing Fourth Amendment protection on privacy rather than just property); Derek T. Conom, *Sense-Enhancing Technology and the Search in the Wake of* Kyllo v. United States*: Will Prevalence Kill Privacy?*, 41 WILLAMETTE L. REV. 749, 756 (2005) (noting the *Katz* Court's shift from protecting property rights to privacy interests when applying the Fourth Amendment).

[25] *See* 389 U.S. at 353 (holding that the Fourth Amendment is not limited to physical intrusions of the home); *Silverman*, 365 U.S. at 509 (noting that in future cases the Court may be required to consider "the Fourth Amendment implications of . . . frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society"); Shindelman, *supra* note 3, at 1914 (stating that the decision in *Katz* expanded the scope of Fourth Amendment protection by including privacy).

[26] *See Katz*, 389 U.S. at 353. In *Katz*, FBI agents recorded the defendant's conversations by placing a recording device on the exterior of a telephone booth. *Id.* at 348. The Supreme Court

The Supreme Court articulated a two-part test for privacy interests that courts use today: whether (1) a defendant has a subjective expectation of privacy; and (2) society would recognize the defendant's expectation of privacy as reasonable.[28] The Fourth Amendment provides protection against a warrantless search when both conditions are met.[29]

An individual's reasonable expectation of privacy was subsequently diminished through the holdings in a series of cases that developed the "third party doctrine."[30] For example, the Court held that because numbers dialed from a defendant's home telephone were voluntarily transmitted to the telephone company, the defendant did not have a reasonable expectation of privacy.[31] By transmitting these numbers to a third party—a telephone company—customers "assume the risk" of having those numbers shared with others, such as law enforcement.[32]

---

held that although the recording device was not placed within the telephone booth, the defendant had entered the booth with the expectation that his conversation would be private. *See id.* at 352–53.

[27] *See id.* at 351.

[28] *See id.* at 361 (Harlan, J., concurring) (restating the expectation of privacy test in the form courts use today); *see also* United States v. Jones, 132 S. Ct. 945, 952 (2012) (referring to "the *Katz* reasonable-expectation-of-privacy test").

[29] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[30] *See* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 567–70 (2009) (tracing the development of the third party doctrine through case law). The U.S. Supreme Court first developed the doctrine in 1952, in *On Lee v. United States*, when the Court held that there was no Fourth Amendment violation when the government recorded a conversation where one party to the conversation had consented to wearing a wire. *See* 343 U.S. 747, 753–54 (1952). In 1976, in *United States v. Miller*, the U.S. Supreme Court held that police did not need a warrant to subpoena the defendant's bank records. *See* 425 U.S. 435, 443 (1976) (holding that there is no Fourth Amendment violation when the government obtains documents from a third party even when a defendant believes the third party will keep the information in confidence). By 1979, the Court had fully formulated the third party doctrine in *Smith v. Maryland*, holding that police did not need a warrant to ask a telephone company to record a list of telephone numbers dialed by the defendant. *See* 442 U.S. at 745–46; Kerr, *supra*, at 570.

[31] *See Smith*, 442 U.S. at 743. In *Smith*, police asked a telephone company to utilize a pen register to remotely track and share with police the numbers dialed from the defendant's home telephone. *Id.* at 737. Although the content of telephone conversations are protected from being recorded without a warrant, the Court noted that telephone companies openly disclose their ability to record the numbers each customer dials. *See id.* at 741–42. The Court provided two examples of this disclosure: (1) customers' monthly bills included a list of calls made to long-distance numbers; and (2) phone books distributed by telephone companies included a notice to customers, which offered to help authorities trace unwanted (harassing) phone calls. *See id.* at 742–43.

[32] *See id.* at 744. Justice Marshall dissented, arguing that to find an assumption of the risk requires an element of choice that is absent given the necessity of telephones in everyday life. *See id.* at 749–50 (Marshall, J., dissenting). Further, Justice Marshall challenged the majority's contention that the average consumer has notice of a telephone company's ability to trace phone numbers. *See id.* at 749. He argued that even if such notice was present, most consumers would not then make the leap to understand that a telephone company can share those numbers with police. *See id.* at 743. The 1986 Pen Register statute circumscribed the holding in *Smith* by requiring a warrant to track phone numbers dialed. *See* 18 U.S.C. § 3121 (2012). It was amended under the

B. No Place Like Home: Privacy Within the Home Is Not Diminished by Protections Without

The Supreme Court has been careful to ensure that new interpretations of the Fourth Amendment's applicability outside the home do not diminish or replace the fundamental right to protection against government intrusion within the home.[33] The Court has reinforced that precept by addressing the potential of technology to procure information about the interior of the home without a physical intrusion.[34] To that end, the Court has interpreted the Fourth Amendment to protect against non-physical searches of the home.[35]

For example, in 2001, in *Kyllo v. United States*, the U.S. Supreme Court held that the use of an infrared thermal sensor to detect heat being emitted from the defendant's home was an unreasonable search that required a warrant.[36] The sensor was capable of detecting both legal and illegal activity within the home, leading the Court to hold that all activity within the home, no matter how trivial, should be protected from government intrusion absent a warrant.[37] Consequently, the Court held that the use of "sense-enhancing

---

Patriot Act in 2001 to require a warrant to obtain Internet routing and addressing data. *See* Patriot Act of 2001, Pub. L. No. 107-56, § 216(a), 115 Stat. 272, 288 (codified as amended at 18 U.S.C. § 3121 (2012)). Some scholars defend the controversial third party doctrine, arguing that it closes a loophole that would allow criminals to escape detection by communicating through third parties. *See* Kerr, *supra* note 30, at 564 (arguing that the third party doctrine is necessary to keep criminals from abusing Fourth Amendment protection by using third parties to circumvent law enforcement). *But see* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) (arguing that the third party doctrine poses a threat to personal privacy by creating the potential for unfettered government surveillance).

[33] *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (noting that the Fourth Amendment primarily protects the home); *Jones*, 132 S. Ct. at 952 (stating that privacy protections supplement rather than replace traditional Fourth Amendment protections); Soldal v. Cook Cnty., 506 U.S. 56, 64 (1992) (stating that the shift in focus to privacy protection has not "snuffed out" protection of the home); Alderman v. United States, 394 U.S. 165, 180 (1969) (denying that *Katz* removed Fourth Amendment protection of the home).

[34] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of a device to gain information about the interior of a home, even absent a physical intrusion into the home, was a search).

[35] *See id.*

[36] *See id.* at 34–35. Police suspected that the defendant was growing marijuana in his garage with the use of special lamps that produce higher than average temperatures. *See id.* at 29. Police officers used a thermal sensor from within their car, which was located across the street from the defendant's home. *Id.* at 30.

[37] *See id.* at 37 (stating that Fourth Amendment protection does not depend on the quality or quantity of information obtained during a search). In a dissenting opinion, Justice Stevens argued that a warrant was not required because the defendant was knowingly emitting heat from his home and simple observation may have provided police with the same information. *See id.* at 42 (Stevens, J., dissenting). As an example, Justice Stevens suggested that snow melting from the roof of the garage at a faster rate than that of neighboring roofs would have provided the same insight into the temperature of the defendant's garage. *See id.* at 43.

technology" that is not in use by the public and is able to gather information about activity within the home that, absent the technology, could not be gathered without entering the home, constitutes a search of the home within the scope of the Fourth Amendment.[38] When a device combines these characteristics, law enforcement is required to obtain a warrant before using the device to conduct a search.[39]

C. United States v. Stanley in the District Court

In November 2010, the routine investigations of the Pennsylvania State Police led to the discovery of a computer sharing child pornography through a peer-to-peer file-sharing network.[40] After tracing the activity to Stanley's neighbor's router, law enforcement obtained a search warrant and performed a search of the neighbor's home.[41] Law enforcement found two computers in the neighbor's home, though neither contained the files in question.[42] Law enforcement also found a wireless router in the home.[43] Stanley's neighbor had not password-protected his router, leading law enforcement to infer that a third computer within range of the router had accessed it from outside the neighbor's home.[44] Law enforcement located the third computer and the like-

---

[38] *Id.* at 34, 40 (majority opinion); *see* April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 693 (2005) (discussing the *Kyllo* Court's development of this new test).

[39] *Kyllo*, 533 U.S. at 34, 40; *see* Conom, *supra* note 24, at 765 (2005) (stating that few courts have used the *Kyllo* test because of the difficulty in applying the test to new technology).

[40] *See* United States v. Stanley (*Stanley I*), No. 11–272, 2012 WL 5512987, at *2–3 (W.D. Pa. Nov. 14, 2012), *aff'd*, 753 F.3d 114 (3d Cir. 2014). Law enforcement discovered the file-sharing user's public IP address and identified it as a Comcast IP address. *Id.* Police then obtained a court order to compel Comcast to share information regarding the name and address of the subscriber with that public IP address. *Id.* This led police to Stanley's neighbor, the Comcast subscriber. *Id.*

[41] *See id*. at *3.

[42] *Id.*

[43] *See id.* Wireless routers assign unique IP addresses to each computer that accesses the Internet through the router. *Id.* at *4. Upon inspection of the neighbor's wireless router, law enforcement discovered that the router had assigned three unique IP addresses, yet the neighbor's computers used only two of those numbers. *See id.* at *5. Law enforcement determined that their suspect must have been assigned the third unique IP address associated with the router. *See id.*

[44] *See Stanley II*, 753 F.3d at 115–16. The neighbor confirmed that he had not given anyone explicit permission to access his router. *See Stanley I*, 2012 WL 5512987, at *3. Wireless routers typically transmit and receive radio signals from a radius of 300 feet. Reply Brief for Appellant at 24, *Stanley II*, 753 F.3d 114 (No. 13-1910), 2013 WL 5869880, at *24. Law enforcement searched the settings on the wireless router and identified the MAC address of the computer (a unique number) associated with the third IP address, yet law enforcement was unable to locate the computer with this information alone. *See Stanley I*, 2012 WL 5512987, at *5–6; *see also Broadhurst*, 2012 WL 5985615, at *6 (noting that the defendant's wireless signal could have been transmitted to the router in question from anywhere, making use of tracking technology necessary to locate the defendant). Law enforcement was, however, able to confirm that the third computer had accessed the file-sharing network. *See Stanley II*, 753 F.3d at 117; *Stanley I*, 2012 WL 5512987, at *5–6.

ly suspect by using tracking technology available to the Pennsylvania State Police—Moocherhunter.[45]

Moocherhunter tracks the location of unauthorized wireless users, or "moochers," by utilizing a directional antenna to trace a computer or device transmitting signals to and from a wireless router.[46] Using Moocherhunter, law enforcement tracked the unauthorized user by following the signal the third computer was transmitting to and from the router.[47] The signal was strongest when law enforcement stood on the sidewalk outside of Stanley's apartment door.[48]

After identifying Stanley's address, law enforcement was able to obtain a search warrant.[49] During the search of his apartment, Stanley confessed to using his neighbor's wireless signal to access child pornography.[50] Stanley was indicted on one count of possession of child pornography under 18 U.S.C. § 2252(a)(4)(B).[51] Stanley pled not guilty to the charge and filed a motion to suppress evidence gathered by police and statements he made during the search.[52] Stanley argued that law enforcement's use of Moocherhunter to locate his laptop computer within his home constituted a search that required a warrant.[53] On November 14, 2012, the U.S. District Court for the Western District of Pennsylvania denied Stanley's motion.[54] Stanley then appealed to the U.S. Court of Appeals for the Third Circuit, which affirmed the lower court's decision on June 11, 2014.[55] The Third Circuit held that Stanley did not have a "legitimate" expectation of privacy in transmitting child pornography through his neighbor's wireless router.[56] The U.S. Supreme Court denied Stanley's petition for writ of certiorari on November 10, 2014.[57]

---

[45] *See Stanley I*, 2012 WL 5512987, at *7–8. Pennsylvania State Police were unsure as to whether or not use of the software required a search warrant, and called the U.S. Attorney's Office for advice. *See id.* at *6. Based on that conversation, law enforcement decided a search warrant was unnecessary. *See Stanley II*, 753 F.3d at 117.

[46] *Stanley I*, 2012 WL 5512987, at *6. Pennsylvania State Police used Moocherhunter in "passive mode" in order to locate Stanley's computer. *Id.* Moocherhunter can also be used in "active mode" in order to trace any wireless signal transmitted to any wireless router. *Id.*

[47] *See id.* at *7–8. Law enforcement entered the MAC address for the suspect's computer into the police-owned laptop with Moocherhunter installed and attached a directional antenna to track the signal. *See id.* at *7.

[48] *See id.* at *8.

[49] *See id.*

[50] *Stanley II*, 753 F.3d at 117. Law enforcement found 144 files containing images and videos of child pornography on Stanley's laptop computer. *Id.*

[51] 18 U.S.C. § 2252(a)(4)(B) (2012); *Stanley I*, 2012 WL 5512987, at *1.

[52] *Stanley I*, 2012 WL 5512987, at *1.

[53] *See Stanley II*, 753 F.3d at 119.

[54] *Stanley I*, 2012 WL 5512987, at *22.

[55] *Stanley II*, 753 F.3d at 114–15.

[56] *See id.* at 124.

[57] *See* Stanley v. United States, 135 S. Ct. 507 (2014) (denying petition for writ of certiorari).

II. THE THIRD CIRCUIT SEEKS LEGITIMACY IN REASONABLE EXPECTATIONS OF PRIVACY

On appeal, the U.S. Court of Appeals for the Third Circuit affirmed the U.S. District Court for the Western District of Pennsylvania's finding while clarifying the district court's reasoning.[58] The Third Circuit agreed that the expectation of privacy test was appropriate but rejected the district court's application of the third party doctrine to the facts of the case.[59] This Part reviews the Third Circuit's holding, beginning with its rejection of the third party doctrine.[60] This Part then reviews the Third Circuit's application of the expectation of privacy test.[61] Lastly, this Part discusses why the Third Circuit rejected the test developed in *Kyllo v. United States*.[62]

The Third Circuit rejected the lower court's application of the third party doctrine.[63] The district court found that because Stanley transmitted information to his neighbor's router, Stanley had assumed the risk of that information being given to police.[64] The Third Circuit held that this application of the third party doctrine was too broad, as all Internet traffic requires sharing information with third parties, such as servers.[65] Because the information transmitted to these third parties includes much beyond the basic data of telephone numbers dialed from a home telephone, the Third Circuit feared

---

[58] *See* United States v. Stanley (*Stanley II*), 753 F.3d 114, 124 (3d Cir. 2014), *cert. denied*, 135 S. Ct. 507 (2014).

[59] *See id.* at 122.

[60] *See infra* notes 63–66 and accompanying text.

[61] *See infra* notes 67–70 and accompanying text.

[62] *See infra* notes 71–74 and accompanying text.

[63] *See Stanley II*, 753 F.3d at 122; *supra* notes 30–32 and accompanying text (discussing the third party doctrine). The Third Circuit's holding is also counter to the lower court findings in *United States v. Norris* and *United States v. Broadhurst*. *See Stanley II*, 753 F.3d at 122; United States v. Norris, No. 2:11–cr–00188–KJM, 2013 WL 4737197, at *8 (E.D. Cal. Sept. 3, 2013) (holding that defendant did not have a reasonable expectation of privacy in Internet data transmitted to a third party); United States v. Broadhurst, No. 3:11–cr–00121–MO–1, 2012 WL 5985615, at *5 (D. Or. Nov. 28, 2012) (holding that defendant did not have a reasonable expectation of privacy because he transmitted information to a third party).

[64] *See* United States v. Stanley (*Stanley I*), No. 11–272, 2012 WL 5512987, at *12 (W.D. Pa. Nov. 14, 2012), *aff'd*, 753 F.3d 114 (3d Cir. 2014). The Third Circuit corrected the technological leap made by the lower court regarding exactly what Stanley transmitted to a third party. *See Stanley II*, 753 F.3d at 123–24. The lower court seemed to suggest that Stanley had transmitted his physical address to his neighbor's router, which the neighbor was then able to give to police. *See id.* Instead, police were only able to obtain discrete data from the neighbor's router—Stanley's IP and MAC addresses—that police then input into Moocherhunter to locate Stanley. *See id.*

[65] *See Stanley II*, 753 F.3d at 124; Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) (noting that third parties like Internet Service Providers and websites have access to a broad range of data transmitted by Internet users).

providing law enforcement with "unfettered access" to individuals' Internet data without adequate Fourth Amendment protection.[66]

After eliminating the third party doctrine from its analysis, the Third Circuit applied the expectation of privacy test and held that Stanley did not have a reasonable expectation of privacy because of the "dubious legality" of using his neighbor's wireless signal.[67] In so holding, the Third Circuit relied on a piece of analysis that the U.S. Supreme Court added to the expectation of privacy test.[68] In 1978, in *Rakas v. Illinois*, the U.S. Supreme Court added a requirement that a reasonable expectation of privacy must also be "legitimate," or lawful.[69] Therefore, in addition to Stanley's mode of access to the Internet, the Third Circuit held that given the illegality of Stanley's transmission of child pornography, society would not recognize Stanley's expectation of privacy as reasonable.[70]

Finally, the Third Circuit held that the test set out in *Kyllo* was inadequate given Stanley's use of a "virtual arm" to extend his activities outside of his home.[71] The Third Circuit addressed the similarities between law enforcement's use of Moocherhunter and law enforcement's use of a thermal

---

[66] *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) (holding that customers do not have an expectation of privacy in telephone numbers dialed from their home telephone); *Stanley II*, 753 F.3d at 124 (indicating reluctance to apply the third party doctrine to all signals sent to third parties).

[67] *See Stanley II*, 753 F.3d at 120–22 (reviewing case law to arrive at the conclusion that Stanley lacked a reasonable expectation of privacy); *supra* notes 28–29 and accompanying text (discussing the expectation of privacy test). Under the expectation of privacy test, in order to enjoy Fourth Amendment protection, an expectation of privacy must be both subjectively and objectively reasonable. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Third Circuit held that although Stanley may have had a subjective expectation of privacy, he did not have an objective expectation of privacy because of his "likely illegal" use of his neighbor's router. *See Stanley II*, 753 F.3d at 120–22.

[68] *See Stanley II*, 753 F.3d at 120–22. This addition was explained in 1978, in *Rakas v. Illinois*, when the U.S. Supreme Court stated that the reasonable expectation of privacy inquiry is necessarily negated when society would view the activity in question as "wrongful." 439 U.S. 128, 143–44 n.12 (1978) (quoting United States v. Jones, 362 U.S. 257, 267 (1960)) (internal quotations omitted).

[69] 439 U.S. at 143–44 n.12; *see Stanley II*, 753 F.3d at 120–22. The Third Circuit, citing to a footnote in *Rakas*, compared Stanley's expectation of privacy to a burglar's unreasonable expectation of privacy while stealing items from an unoccupied summerhouse. *Stanley II*, 753 F.3d at 120 (citing *Rakas*, 439 U.S. at 143–44 n.12). The Court described Stanley as a "virtual trespasser" who had "hijacked" his neighbor's wireless router. *Id.* The Third Circuit noted that Pennsylvania, like several other states, has statutes that might possibly apply to wireless mooching. *See* 18 PA. CONS. STAT. §§ 3926 ("Theft of services"), 7611 ("Unlawful use of computer and other computer crimes") (2014); *Stanley II*, 753 F.3d at 120–21 nn.10–11.

[70] *See Stanley II*, 753 F.3d at 121, 124.

[71] *See id.* at 119–20; *supra* notes 36–39 and accompanying text (discussing the holding in *Kyllo*). In 2001, in *Kyllo v. United States*, the U.S. Supreme Court held that a warrant is required for devices that can sense activity within the home that would not be detectable without entering the home. *See* 533 U.S. 27, 40 (2001).

sensor to scan the interior temperature of a home in *Kyllo*.[72] Although the Third Circuit acknowledged that Moocherhunter met the requirements of the *Kyllo* test for sense-enhancing devices, the court stated that *Kyllo* only applies to activities that are confined within the home.[73] Because Stanley sent data outside of his home to his neighbor's router, the Third Circuit held that his actions were removed from the "safe harbor" of *Kyllo*, defeating the objective prong of the expectation of privacy test.[74]

III. *KYLLO* HAS THE HOME COURT ADVANTAGE

The U.S. Court of Appeals for the Third Circuit should not have reached the question of whether Stanley had a reasonable expectation of privacy in transmitting data from his laptop using an open wireless network.[75] Instead, the Third Circuit should have recognized that, similar to the device used in *Kyllo v. United States*, use of Moocherhunter to detect Stanley's activity within his home was an unreasonable search.[76] Although the Third Circuit was laudable in limiting the potentially Orwellian reach of the third party doctrine into the realm of Internet data, the court otherwise overlooked essential facts

---

[72] *See Kyllo*, 533 U.S. at 40; *Stanley II*, 753 F.3d at 119.

[73] *See Kyllo*, 533 U.S. at 40; *Stanley II*, 753 F.3d at 119. Moocherhunter was held to be sense-enhancing technology that is not in general use and can gather information about activity within the home that, absent use of the technology, could not be obtained without entering the home. *See Kyllo*, 533 U.S. at 34; *Stanley II*, 753 F.3d at 119.

[74] *See Stanley II*, 753 F.3d at 120. The court acknowledged that Moocherhunter met the requirements for sense-enhancing devices that require a warrant. *See id.* at 119. The Third Circuit distinguished the facts in *Kyllo* by stating that the defendant in *Kyllo* had confined his activities within the home. *See Kyllo*, 533 U.S. at 34; *Stanley II*, 753 F.3d at 119. The Third Circuit held that *Kyllo* did not apply because Stanley transmitted data outside of his home. *See Stanley II*, 753 F.3d at 119–20. In addition, in *Kyllo*, the Supreme Court was particularly concerned with the fact that the thermal sensor police used could detect any activity, legal or illegal, taking place within the home. *See* Illinois v. Caballes, 543 U.S. 405, 409–10 (2005) ("Critical to that decision [in *Kyllo*] was the fact that the *device was capable of detecting lawful activity*—in that case, intimate details in a home, such as 'at what hour each night the lady of the house takes her daily sauna and bath.'" (citing *Kyllo*, 533 U.S. at 38) (emphasis added)); 533 U.S. at 38. The Third Circuit focused only on the possible illegality of Stanley's actions. *See Stanley II*, 753 F.3d at 119–20. The Third Circuit determined that Stanley lacked a "legitimate" expectation of privacy when engaging in the "likely illegal" activity of accessing an unprotected wireless signal. *See id.*

[75] *See* United States v. Stanley (*Stanley II*), 753 F.3d 114, 119–24 (3d Cir. 2014), *cert. denied*, 135 S. Ct. 507 (2014). Although the U.S. Supreme Court denied Stanley's certiorari petition, the Court will need to clarify this area of the law soon given the uncertainty of the application of Fourth Amendment protections to this type of Internet use. *See* Stanley v. United States, 135 S. Ct. 507 (2014) (denying petition for certiorari); Bierlein, *supra* note 1, at 1125–26 (observing the ambiguity regarding the applicability of state and federal laws to open wireless networks).

[76] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001); *Stanley II*, 753 F.3d at 119–24. In 2001, in *Kyllo*, the U.S. Supreme Court held that a warrant is required for use of a sense-enhancing device that is not in general public use to detect activity within the home that otherwise could not be detected without entering the home. *See* 533 U.S. at 34.

and precedent in order to reach its holding.[77] The remainder of this Part outlines the Third Circuit's flawed reasoning.[78] First, this Part argues that the Third Circuit misapplied U.S. Supreme Court precedent regarding sense-enhancing devices and the applicability of the expectation of privacy test to activity within the home.[79] This Part then argues that courts should abandon the reasonable expectation of privacy test as applied to open wireless networks.[80] Finally, this Part calls on Congress to clarify the legality of the everyday activity of open wireless Internet use.[81]

As a threshold issue, the Third Circuit predicates its focus on Stanley's lack of a legitimate expectation of privacy on a misapplication of the U.S. Supreme Court's holding in *Kyllo*.[82] The Third Circuit distinguished the facts in *Stanley* by arguing that, unlike the defendant in *Kyllo*, Stanley had not confined his activities to his home.[83] Yet in *Kyllo*, the Supreme Court focused on the fact that the device used was capable of detecting activity within the home, regardless of whether or not the defendant had exposed that activity to

---

[77] *See Stanley II*, 753 F.3d at 124 (noting reluctance to provide the government with unfettered access to personal metadata); *infra* notes 82–93 and accompanying text (discussing the Third Circuit's decision to ignore Supreme Court precedent articulated in *Kyllo*). This is consistent with detractors of the third party doctrine who are increasingly concerned about the repercussions of the doctrine at a time when Internet users transmit and store large amounts of personal data through and with third parties. *See* Shindelman, *supra* note 3, at 1937 (arguing that the Supreme Court has allowed the government to achieve Orwellian capabilities through its Fourth Amendment jurisprudence); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1531 (2010) (asserting that application of the third party doctrine in the online context could expose massive amounts of data stored online); Tokson, *supra* note 65, at 585 (arguing that the doctrine is incompatible with the Internet age). Widespread government surveillance of private citizens has come under fire in recent years, most recently through publicity surrounding the National Security Agency (NSA) leaks. *See* Jennifer Stisa Granick & Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES, June 27, 2013, *available at* http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html, *archived at* http://perma.cc/53AV-HE52?type=pdf (arguing that the NSA's collection of massive amounts of metadata on private citizens was criminal). The Third Circuit was likely chastened by the resulting public outrage over these revelations. *See Stanley II*, 753 F.3d at 124; Granick & Sprigman, *supra*.

[78] *See infra* notes 82–111 and accompanying text.

[79] *See infra* notes 84–93 and accompanying text.

[80] *See infra* notes 94–98 and accompanying text.

[81] *See infra* notes 99–111 and accompanying text.

[82] *See* Illinois v. Caballes, 543 U.S. 405, 409–10 (2005) (stating that, in *Kyllo*, the fact that the thermal sensor was able to detect lawful and unlawful activity was central to the Court's holding that use of the device required a warrant); *Kyllo*, 533 U.S. at 34 (holding that the use of sense-enhancing devices requires a warrant when the device can detect activity within the home that could not otherwise be obtained without entry into the home); *Stanley II*, 753 F.3d at 119–20 (recognizing that Moocherhunter meets the requirements of the *Kyllo* test but refusing to apply the test in *Stanley* because defendant sent information outside of his home).

[83] *See Stanley II*, 753 F.3d at 119–20 (holding that Stanley did not try to confine his activities to his home but deliberately reached outside of his home by transmitting child pornography through his neighbor's wireless router).

observation outside of the home.[84] Because the Supreme Court in *Kyllo* held this type of search to be unconstitutional, use of the Moocherhunter to detect Stanley's activity within his home was also unconstitutional.[85]

Furthermore, the Third Circuit misapplied *Kyllo* by not addressing a significant aspect of that decision: the distinction between lawful and unlawful activity.[86] Like the thermal sensor in *Kyllo*, Moocherhunter software is able to detect both lawful and unlawful activity.[87] Law enforcement in *Kyllo* were only interested in using a thermal sensor to detect illegal activity, yet the fact that the device was capable of detecting legal activity rendered use of the device without a warrant a Fourth Amendment violation.[88] By ignoring the Supreme Court's reasoning in *Kyllo*, the Third Circuit omitted essential precedent.[89]

After refusing to recognize Moocherhunter as a sense-enhancing device that requires a warrant, the Third Circuit applied the expectation of privacy test to hold that Stanley lacked a legitimate expectation of privacy.[90] In *Kyllo*, the Supreme Court refused to consider whether or not the defendant's expectation of privacy in growing marijuana in his home was reasonable.[91] There, the Court held that an expectation of privacy for activities taking place within the home is inherently reasonable because protection of the home is the "very core" of the Fourth Amendment.[92] The Third Circuit once again failed to ap-

---

[84] *See* 533 U.S. at 34 (holding that use of a device to obtain information about the interior of a home that, absent the device, could not be obtained without entering the home is a Fourth Amendment violation). In *Kyllo*, the majority rejected the dissent's argument that details about the home that are transmitted outside of the home, or "off the wall," should not be protected. *See id.* at 35; *id.* at 42 (Stevens, J., dissenting) (arguing that by emitting heat waves outside of the home, defendant had exposed information to the public that was not protected by the Fourth Amendment).

[85] *See Kyllo*, 533 U.S. at 34; *Stanley II*, 753 F.3d at 119–20.

[86] *See Caballes*, 543 U.S. at 409–10 (stating that the *Kyllo* decision protects against devices that detect lawful and unlawful activity); *Stanley II*, 753 F.3d at 119–20.

[87] *See* United States v. Stanley (*Stanley I*), No. 11–272, 2012 WL 5512987, at *6 (W.D. Pa. Nov. 14, 2012), *aff'd*, 753 F.3d 114 (3d Cir. 2014). In *Stanley*, law enforcement used Moocherhunter in "passive mode" to track Stanley to his home. *See id.* But Moocherhunter can also be used in "active mode" to track any wireless signal being transmitted to any router, not just the signals being sent to a specific router. *Id.* The Third Circuit compared the use of Moocherhunter to the use of a drug-sniffing dog, stating that a warrant is not required to use a drug-sniffing dog because the dog is trained to detect only unlawful activity. *See Stanley II*, 753 F.3d at 121–22 (citing *Caballes*, 543 U.S. at 410). Yet this comparison is incorrect because Moocherhunter is capable of detecting both lawful and unlawful activity, making it the type of device the *Kyllo* court sought to provide protection against. *See Caballes*, 543 U.S. at 409–10.

[88] *See* 533 U.S. at 37–38, 40.

[89] *See id.*; *Stanley II*, 753 F.3d at 120–22.

[90] *See Stanley II*, 753 F.3d at 120–22.

[91] *See* 533 U.S. at 34 (noting that for questions regarding searches within the home, there is a minimum expectation of privacy that exists and is per se reasonable).

[92] *See id.* at 31, 34 (citing Silverman v. United States, 365 U.S. 505, 511 (1961)). In *Kyllo*, the Supreme Court held that "to withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." *See id.* at 34; *Sil-*

ply precedent from *Kyllo* when the court applied the expectation of privacy test to the facts in *Stanley*.[93]

As a broader issue, the Third Circuit's application of the expectation of privacy test to wireless Internet traffic illustrates the need to abandon the use of the expectation of privacy test in the Internet context.[94] In practice, the test reflects the reasonable expectations of judges, rather than the practices of the average Internet user.[95] Internet use has become so routinized that most users do not consider the privacy implications of their online activity.[96] The Third Circuit's holding showcases the disconnect between judge-made standards and the expectations of the average Internet user.[97] This application of the reasonable expectation of privacy test threatens the practices of law-abiding Internet users in order to avoid green-lighting a practice that may enable criminals to escape detection.[98]

---

verman, 365 U.S. at 511 ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

[93] *See Stanley II*, 753 F.3d at 120–22.

[94] *See id.*; Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 8–9 (2002) (arguing that the expectation of privacy test has diminished, rather than protected, individual privacy); Brandon T. Crowther, *(Un)reasonable Expectation of Digital Privacy*, 2012 BYU L. REV. 343, 344 (arguing that the test cannot protect privacy interests when applied to the digital realm).

[95] *See* United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("[J]udges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."); Cloud, *supra* note 94, at 28 (noting that reasonable expectations reflect the subjective views of judges); Crowther, *supra* note 94, at 356 (arguing that younger generations master technology before more senior judges are able to understand that same technology); Shindelman, *supra* note 3, at 1934–35 (stating that society's expectations of privacy change as technology changes).

[96] *See* Tokson, *supra* note 65, at 628 (arguing that Internet users consider their online activity to be private despite the reality that ISPs and others can track and divulge their online activities). The recent NSA leaks, as well as recent revelations regarding commercial uses of individual online activity, have made U.S. citizens more aware of personal privacy risks. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THEGUARDIAN.COM, Jun. 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, *archived at* http://perma.cc/2YRF-WVGU; Jack Schofield, *Can I Get Sites Like Facebook and Google to Remove All My Personal Data?*, THEGUARDIAN.COM, Aug. 14, 2014, http://www.theguardian.com/technology/askjack/2014/aug/14/can-i-get-sites-like-facebook-and-google-to-remove-all-my-personal-data, *archived at* http://perma.cc/AB57-V56N (discussing the difficulty in deleting personal tracking data that is collected and stored by websites). As Justice Marshall suggested of the telephone, the Internet has become a necessity that individuals cannot avoid using even if they suspect that others may be able to track their activity and location. *See* Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting).

[97] *See Jones*, 132 S. Ct. at 962 (Alito, J., concurring); Cloud, *supra* note 94, at 28; Crowther, *supra* note 94, at 356; Shindelman, *supra* note 3, at 1934–35.

[98] *See* 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, 115 (2004) (arguing that the criminal acts of some should not result in legal restrictions on open wireless networks); Wells, *supra* note 1, at 126 ("While fighting crime is important, it is not so important that the law should cease to develop concomitant to society.").

Finally, given the uncertainty regarding the legality of the use of unprotected wireless routers, Congress should step in and provide legislative clarity.[99] The Third Circuit's analysis requires an assumption that Stanley's use of an unprotected wireless router was, in fact, illegal.[100] The court described Stanley's unauthorized use of a neighbor's wireless router as an activity that is of "dubious legality" without identifying a statute that clearly prohibited such conduct.[101] Like many users, Stanley chose an open wireless network from a menu of available networks, some of which were likely password-protected, while others, like his neighbor's, were left open.[102] Wireless networks are often made available for others to use freely.[103] In fact, the growing Open Wireless Movement encourages wireless router owners to keep their Internet connection open to others.[104] What the Third Circuit views as "likely illegal" is viewed by many as an everyday activity that provides the ability to

---

[99] *See generally Jones*, 132 S. Ct. at 964 (Alito, J., dissenting) (stating that legislative action is needed when new technology threatens privacy interests).

[100] *See Stanley II*, 753 F.3d at 121; Bierlein, *supra* note 1, at 1125–26 (noting ambiguity as to whether or not state and federal laws apply to the use of open wireless networks); Kern, *supra* note 98, at 119–56 (2004) (providing a full discussion of the ambiguity of federal and state statutes as applied to accessing open wireless networks).

[101] *See Stanley II*, 753 F.3d at 120–21 nn.10–11. Pennsylvania statutes do not define "unauthorized access," and therefore, accessing an open wireless router is not clearly covered by the statutes. *See* 18 PA. CONS. STAT. §§ 3926, 7611 (2014); Bierlein, *supra* note 1, at 1125–26; Kern, *supra* note 98, at 161.

[102] *See* Bierlein, *supra* note 1, at 1131 (noting that wireless router owners often do not password-protect their routers, sometimes with the express intent of sharing their Internet access freely with others); Kern, *supra* note 98, at 161 (noting that it is easier for the owner of a wireless router to password-protect their router than for a user to intuit whether or not the owner wants to share their access or has merely been remiss in setting a password); Ned Snow, *Accessing the Internet Through the Neighbor's Wireless Internet Connection: Physical Trespass in Virtual Reality*, 84 NEB. L. REV. 1226, 1229 (2006) (arguing that when an individual does not set a password on their router they are implying consent for others to use their router).

[103] *See* Response Brief for the United States, *supra* note 8, at 19 (noting that Stanley used his neighbor's router because it was free); Bierlein, *supra* note 1, at 1131; Snow, *supra* note 102, at 1229; Dennis O'Reilly, *How to Find Truly Free Wireless Access*, CNET (Mar. 27, 2013, 10:39 AM), http://www.cnet.com/how-to/how-to-find-truly-free-wireless-access/, *archived at* http://perma.cc/46FS-HHHU (identifying different ways to locate and use free wireless Internet access).

[104] *See* OPEN WIRELESS MOVEMENT, https://openwireless.org/, *archived at* https://perma.cc/JBJ4-BFWS (last visited May 1, 2015) ("The Open Wireless Movement is a coalition of Internet freedom advocates, companies, organizations, and technologists working to develop new wireless technologies and to inspire a movement of Internet openness."); *see also* LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 14 (2001) (arguing that, as a free resource, the Internet promotes innovation); Bierlein, *supra* note 1, at 1126 (asserting that the law should allow individuals to share their Internet access in order to support the network effects of Internet use); Kern, *supra* note 98, at 108 (maintaining that shared wireless access promotes collaboration and the sharing of ideas).

communicate and conduct business and personal transactions from any location.[105]

The needs of law enforcement and the interests of Internet Service Providers ("ISPs") add another level of complexity to the mix.[106] Law enforcement must be able to apprehend criminals, like Stanley, who use the Internet to commit crimes.[107] When criminals use open wireless networks to conduct criminal activity, however, law enforcement faces a potentially impenetrable barrier to apprehension.[108] ISPs also have an interest in protecting their commodity, Internet access.[109] This interest is under attack by those who, like the Open Wireless Movement, believe that Internet access should be freely accessible to everyone.[110] Given the number of stakeholders and the diversity of opinions regarding open wireless Internet access, this is an area that is best regulated by the legislature rather than courts.[111]

---

[105] *See* Bierlein, *supra* note 1, at 1185 (stating that the Internet has transformed the way people engage in daily life). Similarly, the U.S. Supreme Court in 1967 in *Katz v. United States* recognized the "vital role" the telephone had come to play in people's lives and chose to provide protection for that essential technology. *See* 389 U.S. 347, 352 (1967). It is estimated that by 2012 there were 160 million wireless Internet users in the United States, accounting for roughly half of the population. *See* COMPUTER INDUSTRY ALMANAC INC. & FORECASTS, INTERNET USER FORECAST BY COUNTRY 9 (Apr. 2012); U.S. CENSUS BUREAU, U.S. DEP'T OF COMMERCE, *State & County QuickFacts*, http://quickfacts.census.gov/qfd/states/00000.html, *archived at* http://perma.cc/W8NB-F4NT (last visited May 1, 2015).

[106] *See* Bierlein, *supra* note 1, at 1176 (listing various stakeholders in the wireless networking space); David Gray et. al., *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 800 (2013) (arguing that privacy interests must be balanced with the needs of law enforcement); Kerr, *supra* note 1, at 543 (recognizing the need to balance the protection of an individual's civil liberties with the needs of law enforcement).

[107] *See* United States v. Broadhurst, No. 3:11–cr–00121–MO–1, 2012 WL 5985615, at *5 (D. Or. Nov. 28, 2012) (noting the potential inconsistency of refusing to allow tracking of open wireless network users while allowing tracking of individuals who use their own personal wireless network); Kerr, *supra* note 1, at 526 (noting the need to empower law enforcement to apprehend criminals).

[108] *See Stanley II*, 753 F.3d at 121 (stating that had Stanley accessed the Internet using his own wireless network law enforcement could have apprehended him); *Broadhurst,* 2012 WL 5985615, at *5; Wells*, supra* note 1, at 107 (noting that law enforcement must have the technological tools to keep up with cybercrime).

[109] *See* Kern, *supra* note 98, at 110 (noting that some ISPs try to protect their commodity by adding usage restrictions in Terms of Use policies).

[110] *See id.* at 111 (arguing that, despite the prohibitions of some ISPs, lost revenue from shared wireless Internet access is not sufficient to prohibit the activity); OPEN WIRELESS MOVEMENT, *supra* note 104. *See generally* LESSIG, *supra* note 104, at 14 (arguing that all aspects of the Internet, from architecture to access, must remain freely accessible to all).

[111] *See* Bierlein, *supra* note 1, at 1177 (noting that wireless networking policies must balance the needs of stakeholders); Solove, *supra* note 77, at 1515 (arguing that courts should review technology regulations set by the legislature instead of creating their own).

CONCLUSION

In *United States v. Stanley*, the U.S. Court of Appeals for the Third Circuit misapplied U.S. Supreme Court precedent to reach its holding. The Third Circuit applied the expectation of privacy test from *Katz v. United States* to hold that police did not need a warrant to use Internet tracking software to locate Stanley within his home. Yet under *Kyllo v. United States*, the expectation of privacy test is not applicable when devices are used to identify activity within the home if that activity could not otherwise be observed without entering the home. Although the U.S. Supreme Court denied Stanley's petition for writ of certiorari, the widespread use of open wireless networks will continue to implicate these privacy concerns. In the future, the U.S. Supreme Court should ensure that a warrant is required to use devices capable of detecting wireless Internet activity within the home.

EMILY W. ANDERSEN

Preferred Citation: Emily W. Andersen Comment, *Everybody's Going Surfing: The Third Circuit Approves the Warrantless Use of Internet Tracking Devices in* United States v. Stanley, 56 B.C. L. REV. E. SUPP. 1 (2015), http://lawdigitalcommons.bc.edu/bclr/vol56/iss6/1.