


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](mailto:emily.andersen@bc.edu)

Follow this and additional works at: <http://lawdigitalcommons.bc.edu/bclr>

 Part of the [Constitutional Law Commons](#), [Criminal Law Commons](#), [Fourth Amendment Commons](#), [Internet Law Commons](#), and the [Privacy Law Commons](#)

---

### Recommended Citation

Emily W. Andersen, *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/iss6/2>

This Comments is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact [nick.szydowski@bc.edu](mailto:nick.szydowski@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.<sup>1</sup> 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.<sup>2</sup> Legislators and courts are left to face these innovations as they arise, often without fully understanding the consequences to the general public.<sup>3</sup>

---

<sup>1</sup> 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).

<sup>2</sup> 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).

<sup>3</sup> See Anne Meredith Fulton, *Cyberspace and the Internet: Who Will Be the Privacy Police?*, 3 COMMLAW CONSPICUOUS 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.<sup>4</sup> 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.<sup>5</sup> The technology traced the source of the defendant’s wireless signal using an antenna and software called “Moocherhunter™.”<sup>6</sup> 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.<sup>7</sup> The Third Circuit, therefore, affirmed the lower court’s ruling that a warrant was not required to use the technology.<sup>8</sup>

---

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).

<sup>4</sup> 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).

<sup>5</sup> See *id.* at 116–17.

<sup>6</sup> *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.

<sup>7</sup> See *id.* at 115.

<sup>8</sup> 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.

*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.<sup>40</sup> 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.<sup>41</sup> Law enforcement found two computers in the neighbor's home, though neither contained the files in question.<sup>42</sup> Law enforcement also found a wireless router in the home.<sup>43</sup> 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.<sup>44</sup> Law enforcement located the third computer and the like-

---

*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.*

<sup>41</sup> *See id.* at \*3.

<sup>42</sup> *Id.*

<sup>43</sup> *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.*

<sup>44</sup> *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.<sup>45</sup>

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.<sup>46</sup> Using Moocherhunter, law enforcement tracked the unauthorized user by following the signal the third computer was transmitting to and from the router.<sup>47</sup> The signal was strongest when law enforcement stood on the sidewalk outside of Stanley’s apartment door.<sup>48</sup>

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

---

<sup>45</sup> 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.

<sup>46</sup> *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.*

<sup>47</sup> 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.

<sup>48</sup> See *id.* at \*8.

<sup>49</sup> See *id.*

<sup>50</sup> *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.*

<sup>51</sup> 18 U.S.C. § 2252(a)(4)(B) (2012); *Stanley I*, 2012 WL 5512987, at \*1.

<sup>52</sup> *Stanley I*, 2012 WL 5512987, at \*1.

<sup>53</sup> See *Stanley II*, 753 F.3d at 119.

<sup>54</sup> *Stanley I*, 2012 WL 5512987, at \*22.

<sup>55</sup> *Stanley II*, 753 F.3d at 114–15.

<sup>56</sup> See *id.* at 124.

<sup>57</sup> 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.<sup>58</sup> 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.<sup>59</sup> This Part reviews the Third Circuit's holding, beginning with its rejection of the third party doctrine.<sup>60</sup> This Part then reviews the Third Circuit's application of the expectation of privacy test.<sup>61</sup> Lastly, this Part discusses why the Third Circuit rejected the test developed in *Kyllo v. United States*.<sup>62</sup>

The Third Circuit rejected the lower court's application of the third party doctrine.<sup>63</sup> 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.<sup>64</sup> 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.<sup>65</sup> 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

---

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

<sup>59</sup> See *id.* at 122.

<sup>60</sup> See *infra* notes 63–66 and accompanying text.

<sup>61</sup> See *infra* notes 67–70 and accompanying text.

<sup>62</sup> See *infra* notes 71–74 and accompanying text.

<sup>63</sup> 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).

<sup>64</sup> 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.*

<sup>65</sup> 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.<sup>66</sup>

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.<sup>67</sup> 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.<sup>68</sup> 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.<sup>69</sup> 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.<sup>70</sup>

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.<sup>71</sup> The Third Circuit addressed the similarities between law enforcement’s use of Moocherhunter and law enforcement’s use of a thermal

---

<sup>66</sup> 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).

<sup>67</sup> 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.

<sup>68</sup> 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).

<sup>69</sup> 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.

<sup>70</sup> See *Stanley II*, 753 F.3d at 121, 124.

<sup>71</sup> 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*.<sup>72</sup> 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.<sup>73</sup> 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.<sup>74</sup>

---

<sup>72</sup> See *Kyllo*, 533 U.S. at 40; *Stanley II*, 753 F.3d at 119.

<sup>73</sup> 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.

<sup>74</sup> 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.*