Wireless Internet Searches: How the Fourth Amendment Applies to Police Searches of Information Accessed Over a Wireless Internet Connection

by TAYLOR HOBIN*

Introduction

In January 2010, the United States District Court for the District of Oregon ruled that there is no reasonable expectation of privacy in iTunes files that are accessed over an unsecured wireless Internet connection because the broadcasted information was openly accessible to the public (*Ahrndt I*).[1] In doing so, it became the first United States court to rule that the government can seize information broadcast over an unencrypted wireless Internet connection without a warrant.[2] However, this was merely where the confusion began relative to analyzing wireless Internet searches. In April 2012, the Ninth Circuit Court of Appeals reversed and remanded the decision for further consideration (*Ahrndt II*).[3] In response to the Ninth Circuit, the district court reversed its opinion and, in a decision published in January 2013, concluded that the Fourth Amendment had been violated (*Ahrndt III*).[4] Taken together, these rulings suggest that a person may not have an expectation of privacy in some computer files that are accessible through a secured, or even an unsecured, wireless network. This Note will use the reasoning in the

* J.D. Candidate 2014, University of California, Hastings College of the Law. I would like to extend a special thank you to UC Hastings Professor Aaron Rappaport for his guidance on this Note.

1. United States v. Ahrndt (*Ahrndt I*), No. 08–468–KI, 2010 WL 373994, at *5 (D. Or. Jan. 28, 2010).

2. *Id.*

3. United States v. Ahrndt (*Ahrndt II*), 475 F. App'x 656 (9th Cir. 2012).

4. United States v. Ahrndt (*Ahrndt III*), No. 3:08–CR–00468–KI, 2013 WL 179326, at *11 (D. Or. Jan. 17, 2013).

three *Ahrndt* decisions[5] to create a framework for analyzing the Fourth Amendment's application to secured and unsecured wireless Internet networks.

A secured wireless network and an unsecured wireless network may or may not be treated differently under the law.[6] Initially, one might assume that a person has a greater expectation of privacy in information that is accessed over a secured wireless network than over an unsecured network.[7] However, this issue may depend on how a court interprets the way secured wireless networks operate.[8] If a court follows an interpretation that securing wireless networks is similar to locking a message in a briefcase or a sealed envelope, then the court will likely find that there is a reasonable expectation of privacy to the information.[9] This is because the United States Supreme Court has a long history of finding a reasonable expectation of privacy in items locked in containers.[10] However, if a court follows an interpretation that securing wireless communications with an encryption is similar to encoding a message before broadcasting it, then the court will likely find that there is no reasonable expectation of privacy to the information.[11] This is because the Supreme Court has long held that messages encoded and broadcast in the public do not have a reasonable expectation of privacy and do not require a warrant to capture and decode.[12] This Note argues that the court's attempts to distinguish a secured network from an unsecured network highlight the inconsistencies in analyzing wireless networks under a traditional *Katz* analysis.[13] This note suggests that a *Jones* trespass analysis would establish a more predictable and functional standard.[14]

5. *Ahrndt I*; *Ahrndt II*; *Ahrndt III*.

6. *See* Orin Kerr, *Do Users of Wi–Fi Networks Have Fourth Amendment Rights Against Government Interception?*, VOLOKH CONSPIRACY (Sept. 24, 2012, 6:17 PM), http://www.volokh.com/2012/09/24/fourth-amendment-rights-for-users-of-wi-fi-networks-both-encrypted-and-unencrypted/.

7. *Id.*

8. *Id.*

9. *Id.*

10. *See* Georgetown Law Journal Annual Review of Criminal Procedure, Warrantless Searches and Seizures, 35 GEO. L.J. ANN. REV. CRIM. PROC. 37 (2006).

11. *Id.*

12. *Id.*

13. Katz v. United States, 389 U.S. 347, 361 (1967).

14. United States v. Jones, 132 S. Ct. 945, 949 (2012).

I. Background Information

A. The Wireless Internet Network

In recent years wireless Internet, or "Wi-Fi," has become the standard mode of Internet connection.[15] A wireless connection operates by broadcasting radio waves from an Internet router, replacing the need for computers to have a physical wired connection in order to access the Internet.[16] The government made specified radio frequencies available to private companies for the purpose of developing wireless Internet technology for the public, and these specified bands are still the frequencies used today.[17] The waves use "spread spectrum" technology, originally developed for military use, which spreads a radio signal over a wide range of frequencies, in contrast to the usual approach of transmitting on a single, well-defined frequency.[18] This makes the signal less susceptible to interference and creates a zone around the router that gives the user wireless access to the Internet.[19] A typical router will create a circular zone of approximately one hundred feet around the router in which wireless connection to the Internet is made possible.[20]

A user's wireless Internet network can be left unsecured.[21] An unsecured network is not password protected, so a person within range of the router can access the Internet wirelessly through that router by selecting the network on their computer.[22] Furthermore, an unsecured network broadcasts unencrypted information and, if the signal is intercepted, it is possible to view certain files on other's computers if the person who intercepts the signal has proper software.[23] As is the case in the *Ahrndt* decisions discussed *infra*, it is possible for two strangers connected to the same network to view

15. *See A brief history of Wi-Fi*, THE ECONOMIST (June 10, 2004), http://www.economist.com/node/2724397.

16. *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. Mitchell, Bradley, *What is the Typical Range of Wi–Fi LAN?*, ABOUT.COM, http://compnetworking.about.com/cs/wirelessproducts/f/wifirange.htm (last visited Mar. 3, 2014).

21. *See, e.g.*, Microsoft Safety and Security Center, http://www.microsoft.com/security/online–privacy/home–wireless.aspx (last visited Mar. 3, 2014).

22. *Id.*

23. *Id.*

some of one another's computer files when both people are using the same unsecured wireless network.[24]

In the alternative, a wireless Internet network can be secured with a password and encryption.[25] In this case, people who attempt to log onto a network must supply a password when they select the network on their computer.[26] When encrypted, even if someone intercepts the radio transmissions from the network, the information is not decipherable unless the password is provided or the encryption used is decoded.[27] Encryption methods vary in difficulty to decode.[28] There are currently three main types of encryption: WEP, WAP, and pre-shared key or WAP2/PSK.[29] WEP was the original code and it can now be readily decoded with software; WAP was the next development in encryption technology and it is of intermediate strength; and WAP2/PSK is the strongest and most difficult to decode.[30] Wireless routers usually have encryption turned off by default, thus the user must take affirmative steps to activate the encryption and secure the network.[31]

The use of wireless Internet in the Fourth Amendment context is new ground for the courts in the United States. A brief review of applicable standards is useful in starting to determine how a court will analyze the Fourth Amendment protection of information accessed over secured and unsecured wireless Internet networks.

B. The Fourth Amendment Principles

Government searches of any private property are subject to various constraints, both constitutional and statutory. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon

24. *Ahrndt I*, 2010 WL 373994, at *2 (D. Or. Jan. 28, 2010).

25. Aseem Kishore, *Which WiFi Encryption is Best?*, HELP DESK GEEK (July 7, 2009), http://helpdeskgeek.com/networking/comparison–of–wifi–encryption–types/.

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

> probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[32]

Thus, the Fourth Amendment prohibits the government from conducting unreasonable searches and seizures of persons, houses, papers, and effects.[33] The Fourth Amendment only protects against searches conducted by the government, not searches by private citizens.[34]

In *Katz v. United States*, the government, without a warrant, recorded conversations of a private citizen in a telephone booth with a wiretap and sought to introduce the recordings against him at trial.[35] The Supreme Court found the wiretapping was unconstitutional and established a two-pronged test to determine whether a government search had occurred.[36] The test asks (1) if the government has violated a person's actual expectation of privacy, and (2) if society recognizes an expectation of privacy in the area searched as reasonable.[37] The answer to both questions of the test must be in the affirmative for a court to find the government has violated a reasonable expectation of privacy and conducted a search that required a warrant.[38] Recently, in *United States v. Jones*, the Court articulated an alternative Fourth Amendment test and ruled that a search occurs when the government physically intrudes upon property for the purpose of obtaining information.[39]

There are also statutory federal guidelines indicating that stored communications have a reasonable expectation of privacy under a Fourth Amendment analysis.[40] The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511, is meant to prevent the unauthorized access of Internet information.[41] ECPA suggests a

32. U.S. CONST. amend. IV.

33. *Id*.

34. United States v. Jacobson, 466 U.S. 109, 113 (1984).

35. Katz v. United States, 389 U.S. 347, 353 (1967) (finding that police violated a reasonable expectation of privacy when they used a wiretap to eavesdrop on conversations that took place in a telephone booth).

36. *Id*.

37. *Id*. at 361 (Harlan, J., concurring).

38. *Id*.

39. United States v. Jones, 132 S. Ct. 945, 949 (2012).

40. 18 U.S.C. § 2511(g)(i). *See also Ahrndt I*, 2010 WL 373994, at *7 (D. Or. Jan. 28, 2010).

41. *Ahrndt I*, 2010 WL 373994, at *8.

reasonable expectation of privacy exists only when the information is not readily discoverable by the public.[42] The three *Ahrndt* decisions, however, demonstrate that these standards lead to confusion and inconsistency when applied to searches of secured and unsecured wireless Internet networks.

C. An Application of The Fourth Amendment to Wireless–Internet Searches: *Ahrndt*

On January 28, 2010, the United States District Court for the District of Oregon decided *United States v. John Henry Ahrndt* ("*Ahrndt I*").[43] The court used the *Katz* test to rule that there was no reasonable expectation of privacy in computer files viewed by police via a wireless Internet connection to an unsecured router in a private residence.[44] This was the first decision to directly deal with the privacy rights of information broadcast over an unsecured wireless Internet connection.[45] In April 2012, the Ninth Circuit Court of Appeals reversed and remanded the decision for further consideration ("*Ahrndt II*").[46] In 2013, the district court issued a new ruling ("*Ahrndt III*").[47] These cases illustrate which factors and tests are important in determining whether a search of a wireless Internet network has occurred and in identifying difficulties with Fourth Amendment analysis of this issue.[48]

In the *Ahrndt* cases, a private citizen—a woman referred to as JH—used her neighbor's unsecured wireless Internet network, and because no password was required, she used the wireless network by simply selecting it on her home computer.[49] When JH accessed her iTunes software, she saw images and names of files stored on her neighbor's computer because it was connected to the same unsecured wireless network.[50] Inadvertently, she viewed the names of files that her neighbor had downloaded and stored on his computer.[51] She

42. *Id.*

43. *Id*. at *1.

44. *Id*. at *3.

45. Duncan Stark, *Broadcasting Expectations: An Unprotected Wireless Network takes on Constitutional Dimensions*, 7 WASH. J.L. TECH. & ARTS 1, 1 (2011).

46. *Ahrndt II*, 475 F. App'x 656, 658 (9th Cir. 2012).

47. *Ahrndt III*, 2013 WL 179326, at *1 (D. Or. Jan. 17, 2013).

48. *See Ahrndt I*, 2010 WL 373994, at *7; *Ahrndt II*, 475 F. App'x at 656; *Ahrndt III*, 2013 WL 179326, at *9.

49. *Ahrndt I*, 2010 WL 373994, at *1.

50. *Id*. at *2.

51. *Id.*

believed that the titles of the videos indicated that they were child pornography.[52] JH contacted the police; a police officer came to her home and used her computer to access the videos in the same way.[53] The police initially viewed the videos from JH's computer without a warrant and subsequently used them at trial.[54]

In *Ahrndt I*, the District Court of Oregon applied *Katz*. It held that there was no expectation of privacy in the images and, thus, no search had occurred when the officer viewed the images because they were broadcasted from an unsecured wireless network.[55] The district court held that the use of wireless Internet is analogous to the use of wireless home phones for purposes of Fourth Amendment protection.[56] Citing the Eighth Circuit's decision in *Tyler v. Berodt*, the *Ahrndt I* court ruled that wireless home phone communications and wireless Internet communications are similar because they both operate by broadcasting information through radio waves that are easily intercepted.[57] In *Tyler*, the court ruled that wireless phone communications do not carry a reasonable expectation of privacy because they are often intercepted when a neighbor on another wireless home phone inadvertently intercepts a conversation.[58] The facts in *Tyler* illustrate this situation, and in the case, an individual's wireless home phone picked up a neighbor's conversation that revealed criminal conduct, which the police sought to use at trial.[59]

In *Ahrndt I*, the court ruled that a wireless home phone communication and an unsecured wireless Internet communication should be viewed similarly under the law because both operate by sending information through radio waves that can be intercepted by common devices.[60] The *Ahrndt I* court also affirmed that wired Internet connections, like landline phones, should be entitled to protection under the Fourth Amendment due to the "hard-wired" nature of the network that makes interception of the communication impossible without an affirmative act.[61] Thus, relying on the *Katz*

52. *Id*.
53. *Id*.
54. *Id*.
55. *Id*. at *9.
56. *Id*. at *3–4.
57. *Id*.
58. Tyler v. Berodt, 877 F.2d 705, 706 (8th Cir. 1989).
59. *Id.* at 705.
60. *Ahrndt I*, 2010 WL 373994, at *4.
61. *Id*. at *5.

analysis, the court reasoned that wired Internet communications carry a reasonable expectation of privacy, but that unsecured wireless Internet communications often do not carry a reasonable expectation of privacy.[62]

The *Ahrndt I* court further held that there was no reasonable expectation of privacy in unprotected wireless communications that were shared over iTunes because a person would have to take affirmative steps to allow for the sharing of his files over a wireless network.[63] The court noted that in order to share iTunes files over a wireless connection, a user must complete a several-step process on his computer. Thus, the user waives his expectation of privacy by taking those steps and affirmatively allowing others on the same wireless network to view the information in his iTunes account.[64] The district court relied on the Ninth Circuit decision *United States v. Ganoe*.[65] In *Ganoe*, a defendant used LimeWire, a free peer-to-peer file sharing client program that shared files with other computers by default.[66] The program allowed a user to stop sharing files by taking affirmative steps, but the defendant failed to take those steps and shared the files.[67] The Ninth Circuit ruled that the files on LimeWire were in plain view of the Internet-using public and not knowing how to disable the sharing option was not an excuse.[68] In *Ahrndt I*, the court used this reasoning in a *Katz* analysis to conclude that, because the defendant used iTunes and enabled the sharing feature, he exposed the files to the plain view of Internet users; consequently, he had no expectation of privacy in the information.[69]

The *Ahrndt I* court then looked at the application of the Electronic Communications Protection Act ("ECPA"), 18 U.S.C. § 2511. It held that the Act did not suggest that a reasonable expectation of privacy existed under a *Katz* analysis in this electronic communication.[70] The court ruled that the ECPA is "intended to protect against the unauthorized interception of electronic communications, and to protect stored electronic communications

62. *Id.*
63. *Id.* at *6.
64. *Id.* at *7.
65. United States v. Ganoe, 538 F.3d 1117, 1119 (9th Cir. 2008).
66. *Id.*
67. *Id.*
68. *Id.* at 1127.
69. *Ahrndt I*, 2010 WL 373994, at *6.
70. *Id.* at *7.

and transactional records from unauthorized access . . . ."[71] Noting that the FWA applies only when the information that is accessed is not readily available to the general public, the court in *Ahrndt I* ruled that the information was not protected under the FWA because the defendant took affirmative steps to allow the general public to be able to view his information through file sharing.[72]

In *Ahrndt II*, the Ninth Circuit reversed and remanded the *Ahrndt I* decision for further consideration.[73] The Ninth Circuit posed three questions to the district court, and asked the court to analyze the case under the newly decided *United States v. Jones*.[74] First, the court of appeals asked whether sharing files over a wireless connection would be accurately depicted as a "broadcast" of information, or whether the act of accessing files on the defendant's computer involved sending wireless signals into his home to communicate with his router and his computer.[75] Second, the court inquired into whether defendant intentionally enabled sharing of the files on his computer—or, in the event that he did not—whether he knew or should have known that others could access his files by logging onto his wireless network.[76] Third, the court asked whether the image that JH and the police officer accessed was openly available to Internet users at the time the police accessed it or at anytime before the police accessed it.[77]

On remand, in *Ahrndt III*, the district court reversed the *Ahrndt I* ruling and held that a Fourth Amendment search had occurred and that it was unconstitutional.[78] The court noted that it had misunderstood the computer software used by the defendant and had concluded, without evidence, that he had affirmatively allowed sharing of files over his unsecured wireless network.[79] Combined with the fact that JH had never viewed the videos she came across, the videos were excluded from trial and the charges against Ahrndt were dismissed.[80]

71. *Id.* at *6.
72. *Id.*
73. *Ahrdnt II*, 475 F. App'x 656, 658 (9th Cir. 2012).
74. *Id.*; United States v. Jones, 132 S. Ct. 945, 945 (2012).
75. *Ahrndt II*, 475 F. App'x at 658.
76. *Id.*
77. *Id.*
78. *Ahrndt III*, 2013 WL 179326, at *7.
79. *Id.* at *6.
80. *Id.* at *10.

By analyzing the three *Ahrndt* decisions, an observer can begin to identify how a court would approach a Fourth Amendment question involving the search of a wireless network. Applying *Katz*, the three *Ahrndt* courts had to determine how a wireless Internet connection works, how the software that allowed access to the file actually operated, and what steps (if any) a software user must take to allow third parties access to his files. The *Katz* analysis led to confusion in the district court when it misunderstood how iTunes operated, and that misunderstanding was later the basis of the Ninth Circuit reversing the decision. However, the Ninth Circuit also suggested that a *Jones* analysis should have been considered by the district court. Would a *Jones* analysis be a more appropriate standard in wireless Internet cases?

II. Analysis

A. The *Jones* Rule Applied to a Wireless Internet Search

The first question the Ninth Circuit asked was whether wireless Internet is accurately depicted as a "broadcast" of information, or whether the act of accessing files on the defendant's computer involved sending wireless signals into his home to communicate with his router and his computer.[81] As noted, wireless Internet operates by sending radio signals from a router to a computer, thereby replacing the need for wired Internet.[82] In that way, a wireless router sends information similarly to how a radio or wireless home phone "broadcasts" information to the public. However, some courts have also recognized that others may access a wireless Internet user's computer when they send a signal to the computer, and a physical invasion can occur based on that access.[83] This view undermines the idea that the wireless Internet is "broadcast" because it must be "reached out and taken" from the wireless router.[84] Furthermore, the Supreme Court recently ruled in *Jones* that when the government physically invades property for the purpose of obtaining information,

81. *Ahrndt II*, 475 F. App'x 656, 658 (9th Cir. 2012).

82. *See generally*, *A Brief History of Wi-Fi*, *supra* note 15.

83. *See* Am. Online, Inc. v. Nat'l Health Care Disc., 121 F. Supp. 2d 1255, 1259, 1277 (N.D. Iowa 2000); Am. Online, Inc. v. LCGM, 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021–22 (S.D. Ohio 1997); Hotmail Corp. v. Van$ Money Pie, Inc., No. C 98–20064 JW, 1998 WL 388389, at *7 (N.D. Cal. Apr. 16, 1998).

84. *Id.*

a search has occurred.[85] Thus, a wireless Internet router could be viewed as an object, rather than a broadcasting device, which must be "reached out to" and intentionally contacted in order to gather information.

1. The Problem with "Physical Invasion" in Wireless Internet Searches

A number of district courts have ruled that communicating with a computer through the Internet can constitute a physical contact.[86] The Supreme Court held in *Jones* that a search occurs when the government physically makes contact with "private property for the purpose of obtaining information."[87] When using the wireless Internet, physical contact may seem intuitively impossible since the connection is not physically wired.[88] However, the assertion that physical contact occurs when a computer sends electronic signals to a wireless router is supported by recent decisions, including numerous federal court decisions regarding unsolicited mass emails.[89]

The first decision to hold that physical contact occurs when a computer sends electronic information to a wireless router was *CompuServe, Inc. v. Cyber Promotions, Inc.*[90] In *CompuServe*, the United States District Court for the Southern District of Ohio held that the electronic signals that the defendant's computer had generated in order to send an email over the Internet resulted in a physical contact.[91] After the *CompuServe* decision, the ruling was regularly cited in cases involving mass emails, and the proposition that a physical contact is possible over the Internet is now an oft cited

85. United States v. Jones, 132 S. Ct. 945, 949 (2012).

86. *See Nat'l Health Care Disc.,* 121 F. Supp. 2d at 1259, 1277; *LCGM*, 46 F. Supp. 2d at 451–52; *IMS*, 24 F. Supp. 2d at 550–51; *CompuServe*, 962 F. Supp. at 1021–22; *Hotmail*, 1998 WL 388389, at *7.

87. *Jones*, 132 S. Ct. at 949.

88. *See* RESTATEMENT (SECOND) OF TORTS § 217 cmt. e (1965) (requiring physical contact for trespassory intermeddling); Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 830 (2003) (stating that a trespass argument requires that the electronic signal be viewed as physical contact).

89. *See Nat'l Health Care Disc.,* 121 F. Supp. 2d at 1259, 1277; *LCGM*, 46 F. Supp. 2d at 451–52; *IMS*, 24 F. Supp. 2d at 550–51; *CompuServe*, 962 F. Supp. at 1021–22; *Hotmail*, 1998 WL 388389, at *7.

89. *Jones*, 132 S. Ct. at 949.

90. *CompuServe*, 962 F. Supp. at 1015.

91. *Id.* at 1021.

principle.[92] Indeed, the proposition was affirmed by the United States District Court for the Eastern District of Virginia in *America Online, Inc. v. LCGM*, in which the court held that "the transmission of electronic signals through a computer network is sufficient to constitute a physical contact."[93]

Furthermore, the line of cases establishing that a physical contact occurs in mass-email cases was extended to cases where someone used software to collect data from other websites.[94] In *eBay, Inc. v. Bidder's Edge, Inc.*, the United States District Court for the Northern District of California extended the principle of physical contact through the Internet to the situation where individuals use software to extract information from another's website.[95] The court ruled that electronic signals sent by Bidder's Edge to retrieve information from eBay's server were sufficient to constitute a physical contact for trespass.[96]

These cases adopt the idea that electronic signals sent to a computer constitute a legal physical contact.[97] Applying this principle to the *Jones* analysis for a search, it is possible for a search to occur when the government accesses an individual's information over a wireless Internet connection.[98] Electronic signals are sent to a router when someone accesses the Internet through that router.[99] This means that a physical contact occurs when the police access and use a defendant's router under a *Jones* analysis.[100] Furthermore, if police access the wireless connection "for the purpose of obtaining information" from the defendant, then a search occurs under *Jones*.[101] The Ninth Circuit suggested that it was open to entertaining a similar

92. *See* eBay Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058, 1069–72 (N.D. Cal. 2000); *IMS*, 24 F. Supp. 2d at 55051; *CompuServe*, 962 F. Supp. at 1021–22; *Hotmail*, 1998 WL 388389, at *7.

93. *LCGM*, 46 F. Supp. 2d at 452 (citing *CompuServe, Inc.*, 962 F. Supp. at 1021).

94. *Bidder's Edge*, 100 F. Supp. 2d at 1058.

95. *Id.*

96. *Id.* at 1069.

97. *See Bidder's Edge*, 100 F. Supp. 2d at 1069–72; *Nat'l Health Care Disc.,* 121 F. Supp. 2d at 1259, 1277; *LCGM*, 46 F. Supp. 2d at 451–52; *IMS*, 24 F. Supp. 2d at 550–51; *CompuServe*, 962 F. Supp. at 1021–22; *Hotmail*, 1998 WL 388389, at *7.

97. United States v. Jones, 132 S. Ct. 945, 949 (2012).

98. *Id.*

99. *See* Bradley Mitchell, *Wireless Product Equipments—Network Routers, Access Points, Adapters and More*, ABOUT.COM, http://compnetworking.about.com/od/wireless/ss/wirelessgear.htm (last visited Mar. 3, 2014).

100. *Jones*, 132 S. Ct. at 949.

101. *Id.*

argument in *Ahrndt*, and it tasked the lower court with further fact-finding to determine whether the police had sent any signals to the defendant's router, and whether a search occurred under *Jones*.[102] There are also criticisms, however, of the "physical-contact-through-the-Internet" theory that should be acknowledged—and it should be noted that this theory has not yet been applied in criminal cases.[103]

2. *The Rebuttal to the "Physical-Contact-through-the-Internet" Argument*

The view that a physical contact occurs when electronic signals are sent through the Internet has been rebutted.[104] Traditional conceptions of physical contact are at odds with the idea that a physical contact occurs when electronic signals are sent through the Internet.[105] Furthermore, courts have ruled that cordless telephone broadcasts of radio signals that may be intercepted by police for information are not subject to Fourth Amendment protection.[106] This suggests that other forms of intercepted radio communication have not historically had a reasonable expectation of privacy.

It has also been argued that if physical contact can be established through electronic signal transmission over the Internet, this theory opens the door for preposterous causes of action.[107] For example, the inadvertent dialing of a wrong number on a phone may support a trespass claim because a physical contact has technically occurred.[108] However, this logic is inapplicable to the *Jones* analysis because for a search to occur, the physical contact must be accompanied by police action performed "for the purpose of obtaining information."[109]

Moreover, the physical-contact-through-the-Internet principle has not yet been applied to a physical trespass argument under a

102. *Ahrndt II*, 475 F. App'x 656, 658 (9th Cir. 2012) (asking whether connecting to the defendant's network and accessing his files "involve[d] sending wireless signals into the defendant's home to communicate with his router and computer").

103. Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 32 (2000) (expressing concerns over applications of this cyberspace theory to common law trespass claims).

104. *See generally id.*

105. *Id*. at 32–33.

106. In Re Askin, 47 F.3d 100, 104 (4th Cir. 1995); United States v. Smith, 978 F.2d 171, 178–81 (5th Cir. 1992).

107. Burk, *supra* note 102, at 34.

108. *Id.*

109. United States v. Jones, 132 S. Ct. 945, 949 (2012).

Jones analysis.[110] Indeed, there is disagreement over whether a physical contact is even possible through the Internet.[111] However, the Ninth Circuit's question on remand to the district court in *Ahrndt I*, asking whether the police sent a signal to the defendant's router, suggests that the court may be open to an argument of physical trespass in similar wireless Internet cases under *Jones*.[112] The *Jones* test would provide consistency and credibility to decisions regarding wireless Internet searches if the physical trespass through the Internet argument is adopted in criminal cases. If accessing a wireless router were to be accepted as a physical contact, then the only remaining questions are: (1) whether it occurred in a constitutionally protected area; and (2) whether the police were attempting to obtain information. This would bypass the court's current need to accurately analyze the specific computer software and security of the wireless router in every case, as required under *Katz*.

B. The *Katz* Analysis in Wireless Internet Networks

The Ninth Circuit also asked whether the manner in which the information was stored on the computer would give rise to a reasonable expectation of privacy in that information under a *Katz* analysis.[113] To determine this, the district court asked whether Ahrndt had intentionally enabled sharing of files on his computer or whether he knew or should have known that the files on his computer could be viewed by others using his wireless Internet.[114] Under *Katz*, a search occurs when a person has a subjective expectation of privacy in an area searched and society is prepared to recognize that expectation as objectively reasonable.[115] In a *Katz* analysis, a finding that a person knew or should have known his files were public would suggest he had no reasonable expectation of privacy in the files.

To determine whether an individual knew or should have known his computer files were public under a *Katz* analysis of a wireless Internet search, the court must take a case-by-case approach and examine the specific computer software used in each case. The *Ahrndt I* court found that iTunes software would only share information if a user affirmatively chose to allow sharing through a

110. *Id*.

111. *See generally* Burk, *supra* note 102.

112. *Ahrndt II*, 475 F. App'x 656, 658 (9th Cir. 2012); *Jones,* 132 S. Ct. at 949.

113. *Ahrndt II*, 475 F. App'x at 658.

114. *Id.*

115. Katz v. United States, 389 U.S. 347, 361 (1967).

multi-step process.[116] Based on this, the court reasoned that Ahrndt had no expectation of privacy because he had selected to share his computer files.[117]

While the logic sounded convincing, the Ninth Circuit noted that the analysis was factually flawed because it misunderstood the iTunes software that was used in the case.[118] The record only supported that JH had viewed the files on her personal iTunes software that was installed on her computer.[119] Just because a user can view files on their own iTunes does not mean that the files they are viewing originated from another iTunes program.[120] This is because iTunes allows a user to view music that is downloaded by other software like LimeWire.[121] Thus, the assumption that Ahrndt had iTunes on his computer and had to affirmatively allow sharing of his files was unsubstantiated by any evidence and was based on the lower court's misconception of how iTunes worked.

The treachery of a *Katz* inquiry into a wireless Internet search is demonstrated by the *Ahrndt* court's misunderstanding of the computer software.[122] This misunderstanding illustrates the difficulties and inconsistencies that the courts will encounter in a *Katz* analysis of wireless Internet searches.[123] For an example of a court's software-specific analysis under the *Katz* test, this Note will examine the effect of peer-to-peer software on reasonable expectations to privacy.

C. A *Katz* Analysis Applied to Peer-to-Peer Software Searches

The Ninth Circuit asked whether the defendant's computer files were accessible to others over the Internet, since he was using a peer-to-peer file sharing program.[124] This suggests that, under a *Katz* analysis, the court may be willing to accept the proposition that people who share files stored on peer-to-peer software have no

116. *Ahrndt I*, 2010 WL 373994, at *6 (D. Or. Jan. 28, 2010).

117. *Id.*

118. *Ahrndt II*, 475 F. App'x at 658.

119. *Id.*

120. *iTunes: How to Share Music and Video*, http://support.apple.com/kb/HT2688 (last visited Mar. 24, 2013).

121. *Id.*

122. *Ahrndt II*, 475 F. App'x at 658.

123. *See generally Ahrndt I*, 2010 WL 373994 (D. Or. Jan. 28, 2010); *Ahrndt II*, 475 F. App'x 656 (9th Cir. 2012).

124. *Ahrndt II*, 475 F. App'x at 658.

reasonable expectation of privacy. Peer-to-peer networks are special networks that link computers through the Internet and allow people who download software to access files on all computers that have also downloaded the necessary software.[125] In *United States v. Stanley*, the District Court for the Western District of Pennsylvania took the view that people have no reasonable expectation of privacy in information stored on peer-to-peer software.[126] In *Stanley*, the defendant had no reasonable expectation of privacy in files that are stored on peer-to-peer software because the files are readily available to the public.[127] Similarly, the court in *Ahrndt* noted that where a file is saved on a peer-to-peer network, it will likely extinguish any reasonable expectation of privacy in the files since they are readily available to other computer users.[128]

As an aside, it should be noted that the *Stanley* court also dealt with the police tracking a wireless Internet signal in order to find the location of a home.[129] The court ruled that no search had occurred when the police utilized a device to learn the origin of a wireless Internet signal.[130] The court relied on *Smith v. Maryland* and ruled that any information voluntarily turned over to a third party—here, the broadcasting of information about a router to the Internet service provider—meant that the information was not protected by the Fourth Amendment.[131] This doctrine, known as the third-party doctrine, likely applies when the police intercept a wireless Internet signal only to obtain the origin of the signal.[132]

Furthermore, the court in *Stanley* applied *Kyllo v. United States*, which is a case that introduced a *Katz*-like test that may be valuable when used in a wireless Internet search analysis.[133] The *Kyllo* test states that a search occurs when the police use a sense-enhancing technology not in common use to learn the inner details of the home,

125. United States v. Stanley, No. 11–272, 2012 WL 5512987, at *9 (W.D. Pa. Nov. 14, 2012).

126. *Id.* at *14.

127. *Id.* at *11.

128. *Ahrndt I*, 2010 WL 373994, at *5.

129. *Stanley*, 2012 WL 5512987, at *14.

130. *Id.*

131. Smith v. Maryland, 442 U.S. 735, 743 (1979); *Stanley*, 2012 WL 5512987, at *14.

132. *See Smith*, 442 U.S. at 743; United States v. Miller, 425 U.S. 435, 442–44 (1976); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966).

133. *Stanley*, 2012 WL 5512987, at *14.

which would not otherwise be knowable without physical trespass.[134] In a case where police use a device to obtain computer files from inside of a home—in *Stanley* the police used a tracking device called Moocherhunter to determine an IP address—the *Kyllo* test may be applicable.[135] However, when the police use a home computer—as was the case in *Ahrndt*—the *Kyllo* test will not be useful because the computer will likely be viewed as a device that is in common use.[136]

Thus, under a *Katz* analysis, it is important to identify if the information that is obtained through a wireless Internet connection is stored on peer-to-peer software because this information likely does not carry a reasonable expectation of privacy under a *Katz* analysis.[137] It may also be harder to prove that a reasonable expectation of privacy existed when the police only obtain information about the location of a router's signal through the third party doctrine.[138] Furthermore, the *Kyllo* test should be applied if the police use a device that is not in common use to obtain computer files from a network that is inside of a home.[139] In the *Katz* analysis, all of these inquiries will be necessary and relevant in determining whether a reasonable expectation of privacy exists in a wireless Internet search. However, the issue will become even more complicated for a court when it has to confront the issue of whether securing a wireless Internet network creates a reasonable expectation of privacy under *Katz*.

D. *Katz* Analysis and the Effect of a Secured Wireless Internet Network

Thus far, this Note has focused on whether a search occurs when the police access an unencrypted wireless network. How might these principles apply to an encrypted wireless network? It should not be assumed that encrypting a wireless Internet connection will grant Fourth Amendment protection to files accessed through the network.

Wireless Internet encryption is an affirmative step that the owner of a router may undergo if they want (and know how) to do so.[140]

134. Kyllo v. United States, 533 U.S. 27, 40 (2001).

135. *Stanley*, 2012 WL 5512987, at *14.

136. *Kyllo*, 533 U.S. at 40.

137. *See generally Ahrndt I*, 2010 WL 373994 (D. Or. Jan. 28, 2010); *Ahrndt II*, 475 F. App'x 656 (9th Cir. 2012); *Stanley*, 2012 WL 5512987.

138. *See generally Stanley*, 2012 WL 5512987.

139. *Kyllo,* 533 U.S. at 40.

140. HELP DESK GEEK, *supra* note 25.

Once a user has encrypted a wireless network, the information is then sent out on radio waves in a coded format that cannot be deciphered unless someone can decode the information.[141] However, as decoding the information has become easier with advancing technology, encryption methods have become more sophisticated as old code systems have been cracked.[142] At first glance, activating encryption may seem to be an affirmative step that the user takes to retain a reasonable expectation of privacy under a *Katz* analysis.[143] If the court views encryption as "sealing the information in a locked case," encryption may strengthen the argument for a reasonable expectation of privacy on the information broadcasted on a wireless Internet network.[144] In the alternative, the court may view the encryption as "en0coding a message" and sending it with the hope that someone will not capture and decode the message.[145] If this was the case, encryption would not strengthen the argument for a reasonable expectation of privacy. This Note will now explore these two possible, and conflicting, interpretations.

1. Characterizing a Secure Network as an Encoded Message

Generally, courts have ruled that a message is not protected by the Fourth Amendment simply because it is encoded.[146] Although no court has addressed whether wireless Internet encryption should receive Fourth Amendment protection, a number of courts have addressed the effect of concealing a message by making it indecipherable to police.[147] In *United States v. Scott*,[148] *United States v. Longoria*,[149] and *Commonwealth v. Copenhefer*,[150] the court has consistently held that the Fourth Amendment does not protect messages with a hidden meaning.

141. *Id.*

142. *Id.*

143. *See Ahrndt I*, 2010 WL 373994, at *4 (D. Or. Jan. 28, 2010).

144. United States v. Ross, 456 U.S. 798, 821 (1982); Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 356 (8th Cir. 2004).

145. *See generally* United States v. Scott, 975 F.2d 927 (1st Cir. 1992); United States v. Longoria, 177 F.3d 1179 (10th Cir. 1999); Pennsylvania v. Copenhefer, 587 A.2d 1353 (Pa. 1991), *abrogated on different grounds by* Pennsylvania v. Rizzuto, 777 A.2d 1069 (Pa. 2001).

146. *Id.*

147. *Id.*

148. *Id.*

149. *Longoria*, 177 F.3d at 1179.

150. *Copenhefer*, 587 A.2d at 1533.

In *Scott*, the court retrieved shredded documents that contained evidence of tax evasion from the defendant's trash.[151] Over a number of days, the police reassembled the documents and were able to obtain information from the papers.[152] The court held that no warrant was required to seize the shredded documents because the documents were available to the public and "the Fourth Amendment does not protect a defendant when a third party expends money and effort to solve a jigsaw puzzle."[153]

In *Longoria*, defendants "encoded" their conversation by speaking in a foreign language in front of English-speaking police.[154] However, the police secretly recorded the conversation and had it translated.[155] The defendants argued that the police needed a warrant since the conversations were purposefully encoded, and thus carried a reasonable expectation of privacy.[156] The court disagreed, and ruled that a defendant's hope that society would not understand his communication was not reasonable under *Katz*.[157]

In *Copenhefer*, the police searched the home computer of a suspected kidnapping and murder suspect.[158] With a warrant to search the home computer, the police recovered a number of ransom notes.[159] The defendant had attempted to delete the messages from the computer prior to the police search, so no one could read them.[160] The police were able to "undelete" the files using special software.[161] The court ruled that no warrant was needed to "undelete" the files because "a mere hope of secrecy is not a legally protected expectation [of privacy]."[162]

Furthermore, the encryption of messages is not a new concept.[163] During the American Revolutionary War there were many examples

151. *Scott*, 975 F.2d at 928.

152. *Id.*

153. *Id.* at 930.

154. *Longoria*, 177 F.3d at 1181.

155. *Id.*

156. *Id.* at 1182.

157. *Id.* at 1183.

158. Pennsylvania v. Copenhefer, 587 A.2d 1353, 1355 (Pa. 1991).

159. *Id.*

160. *Id.*

161. *Id*. at 1356.

162. *Id.*

163. *See generally* Jennifer Wilcox, *Revolutionary Secrets: Secret Communications of the American Revolution* (2005), http://www.nsa.gov/about/_files/cryptologic_heritage/

of the use of encryption for secret messages.[164] In fact, the decryption of British messages gave George Washington the confidence he needed to storm and capture Yorktown in 1781.[165] George Washington also exiled the Chief Physician of the Constitutional Army based on a decoded message suggesting the physician was a spy.[166] Furthermore, the trial of Aaron Burr in 1807 revolved around an encoded letter that the Supreme Court ordered Burr's assistant to decipher.[167] Thus, the Framers likely understood and contemplated examples of the encoded message when they drafted the Fourth Amendment.[168]

These examples suggest that "encoding" a message was familiar to the founders of our country and of some relevance at the time.[169] Thus, the Framers likely considered encoded messages as unprotected by the Fourth Amendment as evidenced by the prevalence of the messages in history and in early court cases in the United States. Furthermore, common law supports the proposition that encoded messages are not protected by the Fourth Amendment if they are available to the public and are decoded by police.[170] Therefore, if the courts view wireless Internet encryption as a system that encodes a message broadcasted to the public by a router, it is likely that even encrypted wireless Internet communications will not be protected by the Fourth Amendment.

2. Characterizing a Secured Network as a Message Sealed in a Container

Federal courts have also generally ruled that the Fourth Amendment protects messages that are in a locked container.[171] Most recently in *United States v. Jacobsen* and in *United States v. Ross*, the Supreme Court held that this protection extends specifically to

publications/prewii/revolutionary_secrets.pdf (noting many examples of the use of coded messages during the American Revolutionary War).

164. *Id.*

165. *Id.* at 1.

166. *Id.* at 4.

167. United States v. Burr, 25 F. Cas. 38, 40 (C.C.D. Va. 1807).

168. *See generally* Wilcox, *supra* note 162.

169. *Id.*

170. United States v. Longoria, 177 F.3d 1179, 1183 (10th Cir. 1999); United States v. Scott, 975 F.2d 927, 930 (1st Cir. 1992); Pennsylvania v. Copenhefer, 587 A.2d 1353, 1356 (Pa. 1991), *abrogated on different grounds by* Pennsylvania v. Rizzuto, 777 A.2d 1069 (Pa. 2001).

171. United States v. Jacobsen, 466 U.S. 109, 114 (1984); United States v. Ross, 456 U.S. 798, 800 (1982); Doe *ex rel.* Doe v. Little Rock Sch. Dist., 380 F.3d 349, 354 (8th Cir. 2004).

envelopes and sealed packages.[172] In *Jacobsen* and *Ross*, the Court held that searches of envelopes and sealed containers are presumptively unreasonable, and that society has a reasonable expectation of privacy in effects contained therein.[173]

In *Jacobsen* and *Ross*, the Court reaffirmed the notion that a sealed envelope or package is protected under the Fourth Amendment.[174] However, in both of these cases, the Court found there were exceptions to that rule.[175] In *Jacobsen*, the Court ruled that the contents of a sealed container, that had broken open, had no reasonable expectation of privacy because the contents were exposed to the outside world.[176] In *Ross*, the Court ruled that the police legally opened a sealed package inside of a vehicle because the vehicle was lawfully stopped and they had probable cause to believe that contraband was inside the package.[177] In the absence of narrow exceptions like these, the protection of the contents of sealed letters and packages render any warrantless search of their contents unreasonable.[178]

Internet communication may be seen as the modern replacement for the postal service in many ways and commentators have speculated that it will someday replace the post office.[179] If courts view wireless Internet encryption as a package that encapsulates a message, then they are likely to extend Fourth Amendment protection to wireless Internet communications. In this way, society would expect the same privacy in wireless Internet communications that they would expect in physical mail sent through the postal service. However, there are many differences between mail and wireless Internet communications These differences may be roughly illustrated by a "lock-and-key" analogy.

Wireless Internet encryption can be viewed as a lock with the password to decode the network.[180] The Fourth Amendment has long

172. *Jacobsen*, 466 U.S. at 114.

173. *Id*.

174. *Id.*; *Ross*, 456 U.S. at 800.

175. *See Jacobsen*, 466 U.S. at 109; *Ross*, 456 U.S. at 798.

176. *Jacobsen*, 466 U.S. at 120–24.

177. *Ross*, 456 U.S. at 800.

178. *See generally Jacobsen*, 466 U.S. at 109; *Ross*, 456 U.S. at 798.

179. Susanna Kim, *Do We Need the Postal Service?*, ABC NEWS CONSUMER REPORT (Sept. 6, 2011, 1:07pm), http://abcnews.go.com/blogs/business/2011/09/do-we-need-the-postal-service/.

180. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create A "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 504 (2001).

protected locked packages—and mail has been viewed as belonging to this category.[181] However, it is inconsistent to extend the lock-and-key analogy to Internet encryption because it relies on the justification that a locked message is protected since an outsider cannot see the message.[182] An encrypted wireless Internet transmission can be viewed, although the information is in an unreadable form known as "ciphertext," and can only be read if it is decoded.[183] Thus, practically, the question is whether a person can decipher the message—not whether he can see that the information is hidden from sight by a barrier.[184] This distinction makes it possible to argue that the lock-and-key analogy should not be extended to wireless encryption because the wireless encryption functions more like a code than a sealed envelope or a lock and key.[185] The effect that securing a wireless Internet network will have on a reasonable expectation of privacy under a *Katz* test is unclear. The coded message and the sealed envelope characterizations demonstrate the difficulty a court may have in analyzing the effects of securing a wireless network. Thus, even the assumption that securing a wireless network will give a person's computer files a reasonable expectation of privacy under a *Katz* analysis may not prove to be true.

III. Proposal: Selecting the Sensible Test for Wireless Internet Searches

It is inevitable that courts will face the issues outlined in this Note because wireless Internet has become ubiquitous in modern society.[186] If the courts apply a *Katz* test to wireless Internet searches, the analysis will be painstaking and the inconsistency in decisions will be great. First, under *Katz*, a court must determine how the particular computer software in the case functions.[187] This would require a court to understand every new program in the ever-developing world of computer software. The reversal of the district court's decision in *Ahrndt I* demonstrates how ineffective this

181. *Id.*

182. *Id.* at 522.

183. *Id.*

184. *Id.* at 523.

185. *Id.* at 522.

186. *See A Brief History of Wi–Fi*, *supra* note 15.

187. *See generally Ahrndt I*, 2010 WL 373994 (D. Or. Jan. 28, 2010); *Ahrndt II*, 475 F. App'x 656 (9th Cir. 2012); *Ahrndt III*, 2013 WL 179326 (D. Or. Jan. 17, 2013).

approach could be.[188] Second, under *Katz*, if the wireless network were secured, a court would face the challenge of how to characterize the encryption. Information on a secure wireless Internet network may either be viewed as being a coded message or as being a locked container under common law.[189] As one commentator has noted, selecting the appropriate characterization will largely depend on a court's views of how encryption functions.[190] If a court looks at how encryption technically functions, then securing a network may be viewed as a way to encrypt a message and may be no reasonable expectation of privacy even in secured wireless Internet networks.[191] If a court views securing a network through the lens of societal expectations, then it will likely view securing a network as analogous to a sealing an envelope for a letter; accordingly, a reasonable expectation of privacy in a secured wireless Internet network will be found.[192] Thus, every court would be left to delve into the technical function of computer software and make determinations on how encryption affects a reasonable expectation of privacy.

On the other hand, *Jones* presents an alternative to the *Katz* analysis. A *Jones* analysis would ask whether the police physically invaded a protected area for the purpose of obtaining information.[193] In the wireless Internet context, the police would have sent a signal that contacted the router. Note that the premise of a contact occurring through the Internet will have to be adopted in criminal courts for the *Jones* test to be relevant.[194] Once a physical contact is established, a court must ask: (1) whether the router and the network were in a constitutionally protected area; and (2) whether a reasonable person would think that the police were attempting to obtain information by the contact. In *Ahrndt*, the court ruled that a Fourth Amendment search occurred because the police contacted the router when accessing the network through JH's computer. The

188. *Ahrndt I*, 2010 WL 373994, at *6.

189. Kerr, *supra* note 179, at 522.

190. *Id.* at 523.

191. *Id.* at 532.

192. *Id.*

193. United States v. Jones, 132 S. Ct. 945, 949 (2012).

194. *See* Am. Online, Inc. v. Nat'l Health Care Disc., 121 F. Supp. 2d 1255, 1259, 1277 (N.D. Iowa 2000); Am. Online, Inc. v. LCGM, 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021–22 (S.D. Ohio 1997); Hotmail Corp. v. Van$ Money Pie, Inc., No. C–98 JW PVT ENE, C 98–20064 JW, 1998 WL 388389, at *7 (N.D. Cal. Apr. 16, 1998).

router was in the home—the most constitutionally protected area.[195] A reasonable person would think that the police intended to obtain information, evidenced by the police coming to JH's home in order to use her computer to access files for an investigation.[196] Thus, in *Ahrndt*, the police should have known that they needed a warrant. In addition, all citizens would retain an expectation of privacy in computer files within their homes unless the police could point to articulable facts that suggested that unlawful activity is occurring on the network.[197]

Unlike a *Katz* analysis that requires a court to intricately understand society's privacy expectation based on how every piece of computer software is designed, a *Jones* analysis would focus on the protections of the location of the router and wireless network. This would allow the court to enforce Fourth Amendment protection in areas where people expect to be free from government intrusion, like the home.[198] For wireless Internet searches, the *Jones* test would result in a "brighter line" and more consistent results than a *Katz* analysis. One must consider the disparity in rulings if courts were to apply to the *Katz* test to all future cases involving wireless Internet searches based on the issues brought up in this Note alone. A bright line *Jones* analysis in this area will allow the police to conduct investigations while complying with the Fourth Amendment. It will allow the police to have confidence that their investigations and convictions will be upheld. Furthermore, it will allow citizens to be free from governmental intrusion in the locations where privacy is commonly expected. For these reasons, the application of the *Jones* test to wireless Internet searches will lead to the most consistent and just future jurisprudence in this area.

Conclusion

The courts have begun to create precedent for cases where the police intercept information over a wireless Internet connection. A search can occur in two ways. First, under *Katz,* a search occurs when a defendant has a subjective expectation of privacy in an area

195. Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

196. *Ahrndt III*, 2013 WL 179326, at *10 (D. Or. Jan. 17, 2013).

197. Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 63 (2005).

198. *Silverman*, 365 U.S. at 511.

searched and society recognizes that expectation as reasonable.[199] For a wireless Internet search under the *Katz* analysis, courts must understand how the software technically stores the file that the police accessed. Furthermore, courts must determine how much weight is given to the fact that the network was secure or unsecure. Alternatively, a search occurs under *Jones* when the police physically invade a protected area for the purpose of obtaining information.[200] The *Jones* test should be the test courts utilize when analyzing a search of a wireless Internet network. This is because the court can focus on what matters: the constitutional protection of the area that contains the wireless network. This analysis more accurately reflects society's expectation of privacy, compared to the *Katz* analysis, which examines society's expectations of privacy based on its understanding of computer software. The understanding of software varies from person to person, while privacy in the home is generally understood by all. Thus, the *Jones* analysis will offer a more precise and predictable test when applied to wireless Internet searches. For this reason, the *Jones* test should be considered the first choice of courts in wireless Internet search cases. For this reason, the *Jones* test should be the test utilized by courts in wireless Internet search cases.

199. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

200. United States v. Jones, 132 S. Ct. 945, 949 (2012).

* * *