Berkeley Technology Law Journal

Volume 28
Issue 4 *Annual Review 2013*

Article 20

9-1-2013

The Fourth Amendment and Government Interception of Unsecured Wireless Communications

Shaina Hyder

Follow this and additional works at: https://scholarship.law.berkeley.edu/btlj

Recommended Citation

Shaina Hyder, *The Fourth Amendment and Government Interception of Unsecured Wireless Communications* , 28 Berkeley Tech. L.J. (2013).

Link to publisher version (DOI)
https://doi.org/10.15779/Z38W68K

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Technology Law Journal by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.

THE FOURTH AMENDMENT AND GOVERNMENT INTERCEPTION OF UNSECURED WIRELESS COMMUNICATIONS

Shaina Hyder[†]

From its inception, Google Street View fascinated users with detailed, "360-degree street-level imagery"[1] of locations ranging from famous landmarks to small town neighborhoods.[2] To capture these images, Google sent a fleet of cars equipped with cameras and GPS receivers around the world.[3] In addition to taking photographs, Google utilized car-mounted antennas to take snapshots of the surrounding Wireless Fidelity ("Wi-Fi") landscape, scanning the airwaves for traces of Wi-Fi beacons to identify Wi-Fi networks by their name, numeric hardware ID, and other details.[4] Google then uploaded lists of Wi-Fi network identities and signal strengths in order to create a Wi-Fi network location database to broaden Google's geolocation-based services.[5] This database allowed Google to track a mobile

© 2013 Shaina Hyder.

† J.D. Candidate, 2014, University of California, Berkeley School of Law.

1. *Street View*, GOOGLE MAPS, http://maps.google.com/intl/en/help/maps/streetview/#utm_campaign=en&utm_medium=van&utm_source=en-van-na-us-gns-svn (last visited Nov. 21, 2012).

2. *See* Mani Potnuru, Note, *Limits of the Federal Wiretap Acts Ability to Protect Against Wi-Fi Sniffing*, 111 MICH. L. REV. 89 (2012).

3. Glenn Fleishman, *Sniffing Problems*, THE ECONOMIST'S BABBAGE SCI. AND TECH. BLOG (May 3, 2012, 3:37 PM), http://www.economist.com/blogs/babbage/2012/05/googles-wi-fi-scanning-travails.

4. In re Google Inc. St. View Elec. Comms. Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011); *see* Fleishman, *supra* note 3; *see also WiFi data collection: an update*, OFFICIAL GOOGLE BLOG, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (last visited Feb. 19, 2013). On the Official Google Blog, Google stated:

> When we announced three weeks ago that we had mistakenly included code in our software that collected samples of payload data from WiFi networks, we said we would ask a third party to review the software at issue, how it worked, and what data it gathered. That report, by the security consulting firm Stroz Friedberg, is now complete and was sent to the interested data protection authorities today. In short, it confirms that Google did indeed collect and store payload data from unencrypted WiFi networks, but not from networks that were encrypted.

5. Ian Paul, *Google Street View's Wi-Fi Snooping Engineer is Outed*, PC WORLD (May 1, 2012, 08:24 AM), http://www.pcworld.com/article/254774/google_street_views_wi_fi_

device's—and thus a user's—approximate position based on Wi-Fi network signals and the degree to which those signals overlap with the signal of the mobile device.[6]

Today, most homeowners encrypt their home Wi-Fi networks. However, when Google first began deploying its Street View vehicles, far fewer households encrypted their Wi-Fi networks.[7] Google's Street View cars intercepted the data packets coming from and leaving homes with unencrypted Wi-Fi networks by employing a device called a packet sniffer.[8] Though Google claimed it was interested only in the public names of the wireless networks, Google used the packet sniffer to collect and analyze all types of data broadcasted through unprotected Wi-Fi connections,[9] including sensitive private information such as e-mails and passwords.[10]

The ease with which Google conducted large-scale interception of wireless communication for a period spanning multiple years gives rise to the possibility that governments might use similar technology to conduct large-scale surveillance of the wireless communications of individual citizens, without any perceptible legal checks in place. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,"[11] but the extent to which the Fourth Amendment will provide individuals a right to privacy for the contents of their wireless communications remains an open question. This question falls at the intersection of the Federal Wiretap Act and the Fourth Amendment. The Federal Wiretap Act prohibits the intentional interception of "any wire, oral, or electronic communication" unless one or more statutory exceptions applies.[12] Importantly, § 2511(2) of the Wiretap Act provides a statutory exception where the "electronic communications system [is] configured so that such electronic communication is readily accessible to the general

snooping_engineer_is_outed.html; In re Google Inc. St. View Elec. Comms. Litig., 794 F. Supp. 2d at 1071.

6. *See* Fleishman, *supra* note 3.

7. *Id.*

8. *See* Adrian Hannah, *Packet Sniffing Basics*, LINUX JOURNAL (Nov. 14, 2011), http://www.linuxjournal.com/content/packet-sniffing-basics. Packet sniffing, or packet analysis, is the process of intercepting and logging data passing over a digital network or part of a network. It is amongst the most common tools used for intercepting wireless communications.

9. *Id.*

10. *See* Fleishman, *supra* note 3.

11. U.S. CONST. amend. IV.

12. 18 U.S.C. § 2511 (2006).

public."[13] Under this exception, companies like Google have virtually free rein to intercept Wi-Fi communications if the Fourth Amendment does not protect those communications. If Congress or Courts do not limit this exception, the exception could set a dangerous precedent permitting law enforcement officials to freely intercept information exchanged through unsecured wireless networks.[14]

This Note examines the budding tension between the Fourth Amendment and the Federal Wiretap Act, concluding that although current cases read the Wiretap Act as permitting certain private instances of Wi-Fi sniffing, the Fourth Amendment should prohibit the government from intercepting unsecured Wi-Fi signals.

Part I of this Note provides an overview of Wi-Fi technology. It explains the distinction between encrypted ("secured") and unencrypted ("unsecured") communications and explains how readily available technology allows third parties to intercept both. Part II provides an overview of the Fourth Amendment with a discussion of four Supreme Court cases assessing the constitutionality of law enforcement searches that utilized information-gathering technology. Part III discusses *In re Innovatio IP Ventures, LLC Patent Litigation* and a related case addressing the legality of such interceptions by private actors under the Wiretap Act.[15] Finally, Part IV applies the rationale of these cases concerning private actors to government interception of information exchanged through unsecured wireless networks, concluding that such interception—absent the grant of a wiretap order—is an unlawful search and is thus prohibited by the Fourth Amendment.

I. WI-FI TECHNOLOGY

A. BASICS

A basic Wi-Fi network consists of a Wireless Access Point ("WAP"), commonly known as a "wireless router," which connects to an Internet Service Provider's ("ISP") Network through a wired connection that communicates over radio frequencies with any device that is equipped with a Wi-Fi adapter. The Federal Communications Commission ("FCC") regulates

13. 18 U.S.C. § 2511(2)(g)(i).

14. United States v. Young, 153 F.3d 1079, 1080 (9th Cir. 1998) ("The Fourth Amendment limits searches conducted by the government, not by a private party, unless the private party acts as an "instrument or agent" of the government.").

15. In re Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888 (N.D. Ill. Aug. 22, 2012).

most radio communications in the United States,[16] though most Wi-Fi networks operate in unregulated frequency ranges known as Industrial, Scientific, and Medical ("ISM") radio bands.[17] These bands can be used by anyone, even those that do not have a license from the FCC.[18] Other devices such as cordless telephones, wireless microphones, and amateur radios also operate on ISM radio bands.[19] Radio frequency ranges of the ISM bands are further divided into channels, and each individual wireless network operates on one of these channels.[20]

B. NETWORK ENCRYPTION

Wi-Fi technology allows users to restrict access to networks through the use of a password. The information transmitted over the network is encrypted when a wireless network is password protected.[21] Wired Equivalent Privacy ("WEP") is a security protocol for wireless networks that encrypts transmitted data.[22] Wi-Fi Protected Access ("WPA") and Wi-Fi Protected Access II ("WPA2") are two additional forms of Wi-Fi encryption developed by the Wi-Fi Alliance to secure wireless computer networks. WPA and WPA2 have largely replaced WEP encryption.[23] When the password

16. *Case History: A Brief History of Wi-Fi*, THE ECONOMIST, http://www.economist.com/node/2724397 (Jun. 10, 2004). ("Wi-Fi would certainly not exist without a decision taken in 1985 by the Federal Communications Commission (FCC), America's telecoms regulator, to open several bands of wireless spectrum, allowing them to be used without the need for a government licence.").

17. John Herman, *Giz Explains: Why Everything Wireless is 2.4GHz*, GIZMODO (Sept. 7, 2010, 1:00 PM), http://gizmodo.com/5629814/giz-explains-why-everything-wireless0is-24ghz.

18. *See* Definition of: ISM Band, PCMag.com Encyclopedia, http://pcmag.com/encyclopedia_term/0,2542, t=unlicensed+band&i=45467,00.asp (last visited Jan. 31, 2013). The FCC regulates and allocates use of radio frequency ranges:

> In 1985, the FCC Rules (Part 15.247) opened up the ISM bands for wireless LANs and mobile communications. In 1997, it added additional bands in the 5 GHz range under Part 15.407, known as the Unlicensed National Information Infrastructure (U-NII). Europe's HIPERLAN wireless LANs use the same 5 GHz bands, which are titled the "Broadband Radio Access Network." Numerous applications use the ISM/U-NII bands, including cordless phones, wireless garage door openers, wireless microphones, vehicle tracking and amateur radio.

Id.

19. *Id.*

20. *See* 802.11B WiFi Frequency Channels, MOONBLINK, http://www.moonblinkwifi.com/2point4freq.cfm, (last visited Jan. 31, 2013).

21. *See* Potnuru, *supra* note 2.

22. Becky Waring, *How to Secure Your Wireless Network*, PC WORLD (Apr. 9, 2012, 1:00 AM), http://www.pcworld.com/article/130330/article.html.

23. *Id.*

protection to a wireless network is set to "off," the information transmits unencrypted and unprotected through the Wi-Fi network.[24] The information exchanged under a secured setting is encrypted, and must be decoded if intercepted.[25] There are other security technologies such as the data encryption standard and virtual private networks that can provide additional security for wireless network users.[26]

Encryption predates the Internet and Wi-Fi communications, stretching all the way back to the founding fathers of the United States.[27] Encryption of wireless communications uses "complex algorithms to mix characters of a message with other characters or values in a seemingly nonsensical way."[28] The end product is an electronic file with code that is undecipherable to anyone who does not have the encryption key or password. The document only becomes readable when the document's encryption key is applied to the plaintext.[29] Similar to the way physical property may be protected by a lock and key, the use of encryption on electronic files similarly protects the contents of the file by creating a lock and key system through which only the encryption key can open the document at hand.[30] Without the encryption key, "it would be impossible to decode a document without having a supercomputer work on it for hundreds, or sometimes thousands, of years."[31]

C. PACKET SNIFFING

The packet analyzer ("sniffer") is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital

24. *See Wi-Fi (802.11) Security*, GETNETWISE, http://security.getnetwise.org/tips/wifi (last visited June 22, 2011).

25. *Id.*

26. Margaret Rouse, *Data Encryption Standard*, SEARCH SECURITY (July 2006), http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard ("Data Encryption Standard (DES) is a widely used method of data encryption . . . . There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used."). *See also* Jack Schofield, *Using a VPN to Protect Your Web Use*, THE GUARDIAN'S ASK JACK BLOG (May 17, 2012, 8:56 AM), http://www.guardian.co.uk/technology/askjack/2012/may/17/vpn-internet-privacy-security ("A VPN, or virtual private network, creates a virtual "tunnel" of encrypted data running over the public Internet.").

27. *Id.*

28. Sean J. Edgett, *Double-Clicking on Fourth Amendment Protection: Encryption Creates A Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 342–43 (2003); *see* Alex Salkever, *Uncle Sam Should Learn to Hack*, BUS. WK. ONLINE (Oct. 15, 2001), http://www.businessweek.com/stories/2001-10-01/uncle-sam-should-learn-to-hack.

29. Edgett, *supra* note 28.

30. *Id.*

31. *Id.*

network or part of a network.[32] It is among the most common tools used for intercepting wireless communications.[33] As data streams flow across a given network, the sniffer captures each data packet.[34] A data packet is made up of a small amount of computer data sent over a network.[35] Each data packet contains both "payload" information, consisting of the personal information sent over the wireless connection, and also data that identifies the source and destination of the payload data.[36] This Note focuses primarily on wireless users' privacy interests in payload data. Whether or not Wi-Fi networks are encrypted, wireless communications are susceptible to interception by packet sniffers.[37] However, encrypted interceptions require decoding whereas unencrypted interceptions do not.[38]

II. THE FOURTH AMENDMENT: THEN AND NOW

The Fourth Amendment guarantees that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[39] The Fourth Amendment was drafted almost directly in response to the British government's issuance of writs of assistance.[40] Writs of assistance were invasive, unpopular[41] general warrants granting law enforcement officials broad authority to search for evidence to be used in subsequent trials;[42] in terms of breadth, they permitted

32. *See* Hannah, *supra* note 8.

33. *Id.*

34. Jared Howe, *A Hacker's Toolkit*, PRIVATE WIFI (Apr. 14, 2011), https://www.privatewifi.com/a-hacker's-toolkit/.

35. *Packet*, TECHTERMS.COM, http://www.techterms.com/definition/packet (last visited Feb. 21, 2013).

36. *Payload*, TECHTERMS.COM, http://www.techterms.com/definition/payload (last visited Feb. 21, 2013). Construed in terms of postal mail, payload data can be analogized to the letter contained in the envelope to be mailed. The additional data identifying the source and destination of the payload data can be analogized to the to and from addresses written on the outside of an envelope sent through postal mail.

37. *Id.*

38. *Id.*

39. U.S. CONST. amend. IV.

40. *See* Olmstead v. United States, 277 U.S. 438, 463 (1928) (noting that the "well known historical purpose of the Fourth Amendment" was "directed against general warrants and writs of assistance").

41. Brower v. County of Inyo, 489 U.S. 593 (1989); *see also* THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH ROSE UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 301–02 (1868).

42. *Brower*, 489 U.S. 593; *see also* THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH ROSE UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 301–02 (1868).

officials to search virtually any home, at any time, and for any reason.[43] In one notable case, *The Case of John Wilkes*, Lord Halifax, the British Secretary of State, sought to find the author of a libelous pamphlet and issued a search warrant that did not name any individual by name. Lord Halifax instead directed officials "to make strict and diligent search for the authors, printers and publishers of a seditious and treasonable paper" and "to apprehend and seize [them], together with their papers." The officials carrying out the warrant arrested a total of fifty men, including Wilkes, by forcibly entering and searching their homes.[44] As a result, Entick, an associate of Wilkes, brought a civil action against Nathan Carrington and three other messengers to the King in *Entick v. Carrington*.[45] The messengers forcibly entered Entick's home and spent four hours searching the premises; they broke open locked boxes, chests, and drawers; they read Entick's private papers and carried away printed charts and pamphlets.[46] Lord Camden held the aggressive search to be destructive "of all the comforts of society" and the warrant that was issued to be insufficient to merit a search.[47] The Court's holding helped establish civil liberties and limit governmental power.

In the Colonies, English authorities continued to use writs of assistance.[48] Such oppressive and frequent invasions of privacy prompted the proposal and ratification of the Fourth Amendment.[49] Subsequent case law also strongly suggests that the framers intended for the Fourth Amendment to protect privacy interests against abuses of governmental power; stemming from an interest in privacy, the exclusionary rule fashioned in *Weeks v. United States*[50] and *Mapp v. Ohio*[51] excludes evidence seized in violation of a

43. John Burkoff, *"A Flame of File": The Fourth Amendment in Perilous Times*, 74 MISS. L.J. 631 (2004); *see* William Cuddihy, The Fourth Amendment: Origins and Original Meaning, 602-1791, 763 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (on file with UMI Dissertation Services).

44. The Case of John Wilkes, 19 Howell's State Trials 1029, 95 Eng. 807 (1765). *See* Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1333 (2002).

45. 19 Howell's State Trials 1029, 95 Eng. 807 (1765).

46. *Id.*

47. *Id.* at 817–18.

48. *See* Burkoff, *supra* note 42.

49. *Id.*; *see also* United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990). Chief Justice Rehnquist stated, "The driving force behind the adoption of the [Fourth] Amendment . . . was widespread hostility among the former colonists to the issuance of writs of assistance empowering revenue officers to search suspected places for smuggled goods, and general search warrants permitting the search of private houses, often to uncover papers that might be used to convict persons of libel."

50. Weeks v. United States, 232 U.S. 383, 393 (1914) ("The efforts of the courts and their officials to bring the guilty to punishment, praiseworthy as they are, are not to be aided

defendant's Fourth Amendment rights from use in trial.[52] Like that of the Amendment itself, the primary rationale for the exclusionary rule was, and still remains, to protect the privacy interests of citizens.[53]

As early as 1961, the U.S. Supreme Court held that Fourth Amendment protections are not "measurable in terms of ancient niceties of tort or real property law."[54] In *Silverman v. United States*, the government investigated an illegal gambling ring with headquarters in a row house.[55] The government obtained permission from the owner of the neighboring row house to use the neighboring house as an observation post.[56] Government agents found a crack in the wall between the two houses, and used a simple device called a "spike mike," consisting of a foot-long spike attached to a microphone, together with an amplifier, a power pack, and earphones—positioned against the heating duct of the adjoining house—to listen in to conversations.[57] The *Silverman* Court ruled that this constituted a search because it was "accomplished by means of an unauthorized physical penetration into the premises occupied by the petitioners."[58] Contrasting the Court's own prior opinions,[59] the *Silverman* Court noted that "officers overheard the [defendant's] conversations only by usurping the heating system," an "integral" part of the defendant's row house.[60] Law enforcement effected the usurpation of the defendant's heating system without the defendant's knowledge or consent.[61] The Court reasoned that in such circumstances, a court need not consider whether or not there was a technical trespass under the local property law related to the party walls, because even resting the spike mike against the defendant's heating vent constituted an unauthorized physical penetration that violated the defendant's Fourth Amendment

by the sacrifice of those great principles established be years of endeavor and suffering which have resulted in their embodiment in the fundamental law of the land.").

51. Mapp v. Ohio, 367 U.S. 643, 655 (1961).

52. *Id.*; *see also Weeks*, 232 U.S. 383.

53. Ryan A. Ray, *The Warrantless Interception of E-Mail: Fourth Amendment Search or Free Rein for the Police?*, 36 RUTGERS COMPUTER & TECH. L.J. 178, 184–87 (2010).

54. Silverman v. United States, 365 U.S. 505, 511 (1961).

55. *Id.* at 506.

56. *Id.* at 506.

57. *Id.* at 506–07.

58. *Id.* at 509. *Silverman* distinguished decisions in *Goldman v. United States*, 316 U.S. 129 (1942), and *Lee v. United States*, 343 U.S. 747 (1952), in which the Court ruled that the eavesdropping had not been accomplished by means of an unauthorized physical encroachment within a constitutionally protected area, and was therefore a permissible invasion of privacy. *Id.* at 507.

59. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961).

60. Silverman v. United States, 365 U.S. 505, 511 (1961).

61. *Id.* at 511.

rights.[62] That singular, small trespass violated the defendant's privacy not necessarily because of the private nature of the heating vent, but because the heating vent was part of the home as a whole and through it, the officers were able to access the defendant's intimate conversations.

In *United States v. Katz*—one of the most famous Fourth Amendment cases—the Supreme Court held that the Fourth Amendment is intended to protect people, not places.[63] Under the *Katz* rule, an expectation of privacy may exist even in public places and is protected by the Fourth Amendment.[64] In *Katz*, the Court held that the government's use of an electronic surveillance device placed outside of a public telephone booth to listen to and record the defendant as he conducted illegal gambling violated the privacy upon which he relied while using the telephone booth.[65] The majority, led by Justice Stewart, focused on the idea of Katz's intention in using the phone booth, and noted that "what [Katz] sought to exclude when he entered the [phone] booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen."[66]

In a separate concurrence, Justice Harlan parsed out a two-part reasonable-expectation-of-privacy test for determining whether government activity constitutes a search.[67] The test requires (1) that a person exhibit an actual, subjective expectation of privacy and (2) that the expectation be one that society is prepared to recognize as "reasonable."[68] Under this test, whether the incident occurred in a public or a private space may be one factor courts consider in evaluating the reasonable expectation of privacy. But location does not necessarily make an expectation of privacy unreasonable or unworthy of protection under the Fourth Amendment. The *Katz* test—even now—is used to delimit the scope of the Fourth Amendment in the context of law enforcement investigations and has become the nearly exclusive test for the Fourth Amendment.[69]

Almost half a century after *Katz*, the Supreme Court applied Justice Harlan's test to the Department of the Interior's use of more sophisticated

62. *Id.* at 512.
63. Katz v. United States, 389 U.S. 347, 353 (1967).
64. *Id.*
65. *Id.*
66. *Id.* at 352.
67. *Id.* at 360.
68. *Id.* at 361.
69. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a Reasonable Expectation of Privacy?*, 33 CONN. L. REV. 503 (2001) (emphasis added); *see also* Rakas v. Illinois, 439 US 128, 143 (1978); Smith v. Maryland, 442 US 735, 739 (1979).

government surveillance technology.[70] In *United States v. Kyllo*, the Court held that the use of a thermal imaging device to monitor the radiation of heat from a person's home constituted a search within the meaning of the Fourth Amendment and thus required a warrant.[71] The court held this to be a search, despite the fact that the government remained outside of the house and monitored the heat emanating through the walls of the home from a public vantage point.[72] The Court found the government's search presumptively unreasonable because the surveillance technology was not commonly available to the public. In his opinion, Justice Scalia—writing for the majority—sought to protect privacy interests against evolving surveillance equipment.[73] Justice Scalia held that both off-the-wall surveillance and through-the-wall surveillance intrude upon the privacy of the home and refused to draw a distinction between the two methods of surveillance. The Court held that in the home, "*all* details are intimate details because the entire area is held safe from prying government eyes."[74]

In dissent, Justice Stevens adhered to the distinction between off-the-wall and through-the-wall surveillance. Justice Stevens wrote that excessive heat emanating from Kyllo's walls could have been perceived by the passerby as just as it could have been perceived by the thermal imaging device.[75] Justice Stevens further elaborated that "[h]eat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building."[76] The dissent argued that the officer's conduct did not amount to a search because the officers were doing no more than drawing off-the-wall inferences that a passerby could have drawn by walking past the home, rather than conducting any through-the-wall surveillance that would constitute a more invasive search and reveal more intimate details.[77]

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

71. *Id.* at 40.

72. *Id.*

73. *Id.* at 35–36. ("[A mechanical interpretation of the Fourth Amendment] would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

74. *Kyllo*, 533 U.S. at 37 (emphasis added).

75. *Id.* at 43.

76. *Id.* at 43–44.

77. *Id.* at 41.

III. SNIFFING UNDER THE WIRETAP ACT

The Federal Wiretap Act is broadly written and provides that, with certain exceptions, "any person who . . . intentionally intercepts . . . any wire, oral, or electronic communication" shall be subject to liability.[78] Under the Wiretap Act, an "electronic communication" includes "any transfer of signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[79]

A. CORDLESS PHONES AND RADIO BASED COMMUNICATIONS: THE WIRETAP ACT BEFORE WI-FI

McKamey v. Roach is an early case involving cordless telephones, where the Sixth Circuit held that the Wiretap Act did not protect cordless telephone communications from third-party interception.[80] Plaintiffs McKamey and Jett alleged that Jett's neighbors, the Roachs, intercepted and recorded twelve to thirty telephone conversations between McKamey and Jett in violation of the Wiretap Act.[81] Neither plaintiff knew that the Roachs were intercepting and recording their private conversations. One of the plaintiffs, Jett, used a cordless telephone.[82] The cordless portions of the conversations travelled between the cordless telephone base unit and the handset through AM or FM radio signals, and the Roachs intercepted the conversations with a radio scanner.[83] At the time the McKamey-Jett conversations took place, the Wiretap Act permitted the interception of cordless telephone communications without exception.[84] Because the Roachs' scanner only intercepted the radio portion of the conversation between the plaintiffs, the court held that the Wiretap Act did not protect the plaintiffs' cordless telephone communications from the defendants' interception.[85] The court also noted that the owner's manual to Jett's cordless telephone stated that it used "radio transmission[s]" and cautioned owners that "[i]t is not possible to ensure privacy of communication when using this telephone."[86] Finally, the court noted that there might be interference problems between cordless

78. 18 U.S.C. § 2511(1)(a) (2006); *see also* 18 U.S.C. § 2520(a).
79. 18 U.S.C. § 2510 (12).
80. McKamey v. Roach, 55 F.3d 1236 (6th Cir. 1995).
81. *Id.* at 1237.
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.* at 1240.

telephones if a neighbor also has a cordless telephone that operates on the same channel.[87]

B. UNAUTHORIZED WI-FI INTERCEPTIONS: *UNITED STATES V. AHRNDT*

A district court considered the issue of Wi-Fi interception in a 2010 case, *United States v. Ahrndt*.[88] The court analogized the expectation of privacy in wireless networks to the expectation of privacy in cordless telephones because both devices transmit data over radio waves and both are easily intercepted.[89] Ahrndt was charged with the transportation and possession of child pornography.[90] He argued that his neighbor violated the Electronic Communications Privacy Act ("ECPA") when she accessed his iTunes library—a system for playing, storing, and sharing audio, video, and image files[91]—through his unsecured Wi-Fi network while a police officer observed.[92] The court noted that under ECPA, it is not unlawful for any person "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic

87. *Id.* at 1237.

88. United States v. Ahrndt, CRIM. 08-468-KI, 2010 WL 373994 (D. Or. Jan. 28, 2010), *rev'd and remanded*, 475 F. App'x 656 (9th Cir. 2012) (reversing the district court's denial of Ahrndt's motion to suppress, because a computer expert found that Ahrndt's iTunes was capable of detecting other files shared by other programs on his computer, making it unclear whether he affirmatively shared those files, and remanding for further proceedings and fact finding). The court also posed the following questions for further fact finding:

> 1. As a technical matter, is sharing files over a wireless network accurately characterized as a "broadcast" of the contents of those files, such that JH's computer simply intercepted Ahrndt's images outside Ahrndt's home? Or, alternatively, did the act of connecting to Ahrndt's network, accessing his library and opening the image involve sending wireless signals into Ahrndt's home to communicate with his router and computer?
>
> 2. Did Ahrndt intentionally enable sharing of his files over his wireless network? If not, did he know or should he have known that others could access his files by connecting to his wireless network?
>
> Was the image in "Dad's LimeWire Tunes" library that JH and McCullough opened accessible over the Internet by Limewire users at the time JH and McCullough accessed the files, or at any time prior?

Id. at 658.

89. *Id.* at *3 ("The expectation of privacy in cordless phones is analogous to the expectation of privacy in wireless networks, because wireless networks are so easily intercepted.").

90. *Id.* at *1.

91. *Id.*

92. *Id.* at *1–2.

communication is readily accessible to the general public."[93] Because Ahrndt's router broadcast his wireless network in a 400-foot radius around his house, and because Ahrndt had configured his iTunes program to automatically share files with any computer that joined that network, the court held that the wireless network was "readily accessible to the general public."[94] The court also denied Ahrndt's claim that officers who viewed his iTunes library violated his Fourth Amendment right against unreasonable search.[95] The court held that Ahrndt "failed to demonstrate either a reasonable objective or subjective expectation of privacy" in his use of the shared iTunes library on an unsecured wireless network and therefore could not invoke the protections of the Fourth Amendment.[96]

The court held that Ahrndt had no reasonable expectation of privacy in his iTunes files.[97] Importantly, the court concluded that society recognizes a lower expectation of privacy in information broadcast through an unsecured wireless network as opposed to information transmitted through a hardwired network or password-protected network.[98] According to the court, Ahrndt had no socially recognizable right to privacy because the default setting of iTunes is *not* to share music or images with others, and his iTunes library was set to share.[99] To enable sharing—as Ahrndt did—a user must take six affirmative steps, thus knowingly and purposefully sharing their iTunes.[100]

Upon an appeal and a subsequent motion to suppress evidence, the same district court *granted* Ahrndt's motion to suppress evidence.[101] In his opinion and order on motion to suppress, Judge King concluded, "Ahrndt's reasonable expectation of privacy in the contents of his computer was *not* eliminated when he attached it to his unsecured wireless network router . . . . Accordingly, although Ahrndt's failure to secure his network suggests a lesser subjective expectation of privacy, I could not say he lost all expectation of privacy in the contents of files on his personal computer."[102] Further, the court found that since the evidence suggested that the default setting of LimeWire, a peer-to-peer file sharing software, was set to share content,

93. *Id.* at *6–8. *See* 18 U.S.C. § 2511(2)(g)(i) (2006).
94. *Id.* at *18–19.
95. *Id.* at *9.
96. *Id.*
97. *Id.* at *5.
98. *Id.*
99. *Id.* at *7.
100. *Id.*
101. United States v. Ahrndt, 3:08-CR-00468-KI, 2013 WL 179326 (D. Or. Jan. 17, 2013).
102. *Id.* at *6 (emphasis added).

there was "no evidence Ahrndt intentionally enabled the sharing of his files over his wireless network."[103]

C. A SPLIT IN INTERPRETATION?

Against the backdrop of an ongoing debate, the district court for the Northern District of Illinois, in *In re Innovatio IP Ventures*, ruled that the Wiretap Act does not cover interception of unencrypted Wi-Fi communications.[104] The court reasoned that Wi-Fi sniffing falls under the statutory exception to the Wiretap Act that permits a person "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[105] The court distinguished contrary precedent by highlighting the public availability of packet analyzers.[106]

As discussed in *Innovatio*, while public availability of a given technology may be relevant to a court's determination as to whether § 2511(g)(i) of the Wiretap Act applies to a given interception of electronic communication, the consideration is not determinative for the constitutionality of law enforcement searches under the Fourth Amendment.[107]

---

103. *Id.* at *7.

104. In re Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012), (citing 18 U.S.C. §2511(g)(i)).

105. *Id.* (citing 18 U.S.C. § 2511(g)(i)).

106. *Id.* at 893 (distinguishing In re Google Inc. St. View Elec. Communications Litig. 794 F. Supp. 2d 1067, 1070 (N.D. Cal. 2011)). The court also stated that, "upon examination, the proposition that Wi–Fi communications are accessible only with sophisticated technology breaks down. As mentioned . . . Innovatio is intercepting Wi–Fi communications with a Riverbed AirPcap Nx packet capture adapter, which is available to the public for purchase for $698.00." *Id.*

107. Orin Kerr, *District Court Rules that the Wiretap Act Does Not Prohibit Interception Unencrypted Wireless Communications*, THE VOLOKH CONSPIRACY (Sept. 6, 2012, 7:08 PM), http://www.volokh.com/2012/09/06/district-court-rules-that-the-wiretap-act-does-not-prohibit-intercepting-unencrypted-wireless-communications/. In a recent article on wireless networks and the Fourth Amendment, Orin Kerr suggested that the court's analysis of § 2511(g)(i) in *Innovatio* is flawed. Kerr advances the argument that the term "configured" in § 2511(g)(1) refers to the intent of the designer. He states that the exemption "focuses on the person who does the *configuring* of the network *so* that it works a particular way—to design the network so that the general public was *supposed* to be able to access them," rather than on whether the end user sets up the Wi-Fi network as an encrypted or unencrypted network. To Kerr, it seems obvious that while one might not know the actual intent of the packet sniffer's designer with 100% certainty, here, as with many technologies, the standards for an "expected use" and an "unexpected use" should be clear to users. Kerr writes that "[n]o one suggests that unsecured wireless networks are set up with the goal that everyone on the network would be free to read the private communications of others." Just because

In *In Re Google Streetview*, currently on appeal before the Ninth Circuit, the district court held that § 2511(g)(i) of the Wiretap Act does not apply to private sniffing because information exchanged through unsecured wireless networks is not readily accessible to the public and the technology used to access such information ("packet sniffers") is "sophisticated."[108] While collecting data, Google—like Innovatio—sniffed private information exchanged through unsecured wireless networks, collected payload data, and in some instances also captured emails, URLs, and passwords.[109] On motion for summary judgment, Google argued that it could not be held liable under the Wiretap Act because (1) the collected data was "readily accessible to the general public," and (2) the Wiretap Act's statutory definition of "readily accessible" applies solely to "radio communications" and is inapplicable to "electronic communications."[110]

The court rejected the latter argument by narrowly construing "radio communications" in light of the Wiretap Act's legislative history.[111] The court likened Wi-Fi communications to cellular communications, which the Ninth Circuit had previously deemed to be "wire communications."[112] For the Act to make sense, these "wire communications" could not also have been "radio communications," and thus the "radio communications" exception did not apply.[113] The court also rejected Google's argument that the collected data was "readily accessible to the general public"—an argument that prevailed in *Innovatio*—on procedural grounds.[114] In rejecting this argument, the court accepted at face value the plaintiff's pleadings that although the sniffed

unsecured Wi-Fi may be easily intercepted, does not mean that users of unsecured Wi-Fi networks intend for everyone else with access to the network to read their communications.

108. In re Google Inc. St. View Elec. Communications Litig., 794 F. Supp. 2d 1067, 1082 (N.D. Cal. 2011).

109. Alan Eustace, *Creating Stronger Privacy Controls Inside Google*, OFFICIAL GOOGLE BLOG (OCT. 22, 2010), http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html.

110. In re Google Inc. St. View Elec. Communications Litig., 794 F. Supp. 2d at 1073.

111. *Id.* at 1081.

112. *Id.* at 1078. The court noted:

> An interpretation of "radio communication" that presumptively included all technologies that transmit over radio waves, such as cellular phones, under the purview of electronic communications and held that technology bound by Section 2510(16)'s definition of "readily accessible to the general public," would contravene Ninth Circuit precedent holding that cellular phone communications are wire communications for purposes of the Wiretap Act.

Id. See also In the Matter of the Application of the United States for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d 1132 (9th Cir. 2003).

113. *Id.*

114. *Id.* at 1081.

networks were unsecure, the networks were configured to prevent the general public from gaining access, and interception required "sophisticated packet sniffer technology" to which the general public did not have access when the Street View project began.[115] The court reasoned that

> Wi–Fi technology shares a common design with cellular phone technology, in that they both use radio waves to transmit communications, however they are both designed to send communications privately, as in solely to select recipients, and both types of technology are architected in order to make intentional monitoring by third parties difficult.[116]

Depending on the outcome of the *Google* appeal, *Google* and *Innovatio* may be at odds with one another. For now, their tension as to the permissibility of private sniffing raises two issues. First, it suggests that the Wiretap Act's current categorization of communication mediums may be too outdated and simplistic to account for new media that—like unencrypted Wi-Fi—are private by convention but public by design. Second, if a federal enforcement agency such as the Federal Bureau of Investigation ("FBI") put together a street team of like Google's, drove across the country sniffing private information from unencrypted networks, and cited *Innovatio* as authority, the government could argue that it is entitled to intercept unsecured, and possibly even secured, Wi-Fi communications.

IV. THE FOURTH AMENDMENT SHOULD BE CONSTRUED AS PROTECTING THE USERS OF UNSECURED WIRELESS NETWORKS FROM GOVERNMENT WI-FI INTERCEPTION.

Because courts have traditionally used the Wiretap Act to protect wireless networks, there have been relatively few references to the Fourth Amendment in the case law surrounding wireless networks."[117] That said, the Wiretap Act is a poor substitute for the Fourth Amendment with respect to protecting the privacy of Wi-Fi signals. The Wiretap Act, with the exception of a few statutory exemptions, fails to account for the public's reasonable expectation of privacy in a rapidly changing technological climate.

115. *Id.* at 1082.

116. *Id.* at 1082–83.

117. *See* Orin Kerr, *Do Users of Wi-Fi Networks Have Fourth Amendment Rights Against Government Interception*, THE 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/.

A. UNDER FOURTH AMENDMENT CASE LAW, WI-FI NETWORKS SHOULD BE ENTITLED TO PROTECTION

The extent to which the Fourth Amendment will provide individuals a right to privacy for the contents of their electronic communications remains an open question in light of new and emerging technologies and methods of communication.[118] *Innovatio* held that the general availability of a device used to intercept Wi-Fi network information might be determinative as to whether one's expectation of privacy is reasonable under § 2511(g)(i) of the Wiretap Act.[119] Regardless of whether this is true as a matter of statutory interpretation, it is inconsistent with Fourth Amendment jurisprudence. Public access to the tools that colonial British law enforcement officials used to execute writs of assistance was not the mischief that the Fourth Amendment was drafted to cure. The mischief the Fourth Amendment was drafted to cure was an unwarranted invasion of privacy, exemplifying this nation's "express and profound constitutional commitment to individual freedom from unjustified and unreasonable government searches and seizures."[120]

In *Silverman*, the Supreme Court did not hold the search unconstitutional because the police used cutting-edge technology to gain access to information in a way that ordinary individuals would not have expected. The microphone was in use for nearly a century prior to the Supreme Court's decision in *Silverman*: it was invented by Thomas Edison in 1877 and was surely available to the general public in 1961.[121] Nor did the Court hold the search unconstitutional because the government had unlawfully trespassed (in the traditional sense) on *Silverman's* home. Instead, the *Silverman* opinion may be read as suggesting that citizens have a protected privacy interest in the sound waves that they create in confined spaces. In *Silverman*, the Justices noted that the Court:

> has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard. . . . It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in

118. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904 (9th Cir. 2008).

119. In re Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 893 (N.D. Ill. 2012).

120. *See* Burkoff, *supra* note 42.

121. IEEE Computer Society, *Microphone*, GLOBAL HISTORY NETWORK, http://www.ieeeghn.org/wiki/index.php/Microphone, (last visited Jan. 21, 2012).

> that way, namely, by silent approaches and slight deviations from legal modes of procedure.[122]

The Court did not find a physical trespass to be the offensive factor,[123] nor did it find the government's use of sophisticated tools to be the egregious conduct.[124] The government's unwarranted invasion of privacy—by listening to the conversations that the citizen wished to keep private—was the mischief that the *Silverman* Court would not tolerate.[125]

Katz may be read as extending the logic of *Silverman*.[126] As with *Silverman*, the surveillance tool used in *Katz* was not treated or referred to as particularly sophisticated.[127] In defining the standard that still governs the reasonable expectation of privacy, the *Katz* Court focused on Katz's intention in using the phone booth and noted that he used the booth in order to exclude the "*uninvited ear*."[128] The Court explained:

> One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[129]

122. Silverman v. United States, 365 U.S. 505, 511–12 (1961).

123. Departing from earlier, tangible property based notions of trespass, the Court has since held that the "Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any 'technical trespass under local property law.' " Katz v. United States, 389 U.S. 347, 353 (1967) (citing *Silverman*, 365 U.S. at 511–12).

124. In *Silverman*, the surveillance device used was a "spike mike," a simply constructed, and comparatively inexpensive, instrument consisting of a foot-long spike attached to a microphone. *Silverman*, 365 U.S. at 506.

125. *Id.*

126. *Katz*, 389 U.S. at 353 ("Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people-and not simply 'areas'-against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

127. In *Katz*, the surveillance tool used as electronic listening and recording device. *Id.* at 347. In *Silverman*, the surveillance device used was a "spike mike." *Silverman*, 365 U.S. at 506. Neither Court regarded the surveillance devices used in *Katz* or *Silverman* to be sophisticated, or outside of use by ordinary individuals.

128. *Katz*, 389 U.S. at 352 (emphasis added).

129. *Id.*

The *Katz* Court noted the vital role that public telephones played in society at the time.[130] As was true then, when one thinks of speech in common parlance, one does not think of mechanical oscillations of pressure that travel from one's vocal chords and mouth to another's eardrum, and one does not think of speech in terms of travelling waves.

The Supreme Court's holding in *Kyllo* aligns with the interpretation of the Fourth Amendment put forth in *Katz*. In *Kyllo*, the Court reasoned that because the device was not commonly available to the public, the government's search was presumptively unreasonable. The Court based its decision on the sophistication of the heat detecting technology that the government used to gather its information but cited the *Katz* Court's rationale, which rejected a purely mechanical interpretation of the Fourth Amendment.[131] The Court stated, "[r]eversing [*Katz*] would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home."[132]

Supreme Court jurisprudence makes clear that heat waves coming from the home, sound waves coming from the home, and sound waves coming from confined spaces—such as public telephone booths—all warrant Fourth Amendment protection.[133] Expecting such waves to be kept private is reasonable, especially since many modern communications require the use of radio waves. Analogizing Wi-Fi waves to sound waves and heat waves establishes a sound basis for the assertion that a reasonable expectation of privacy applies to radio waves and thus Wi-Fi networks transmitted via radio waves.[134] In addition, a person should have a reasonable expectation of privacy in their Wi-Fi communications. Wireless communications, by

130. Justice Stewart's opinion for the Court stated that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Id.* at 352.

131. Kyllo v. United States, 533 U.S. 27, 34 (2001). The court stated:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," Silverman, 365 U.S. at 512, 81 S. Ct. 679, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.

Id.

132. *Id.* at 28.

133. Referencing *Silverman*, *Katz*, and *Kyllo*.

134. *See Kyllo*, 533 U.S. at 36.

definition, are transmitted through radio frequencies. The medium through which information is transmitted is not, by itself, determinative of whether such expectation exists under the Fourth Amendment; wireless communications, even on unsecured networks, should not be exempt from protection simply because the medium that they travel in is susceptible to interception.

B. WHAT DETERMINES A REASONABLE EXPECTATION OF PRIVACY IN WI-FI COMMUNICATIONS?

The Wiretap cases take an approach to delimiting the reasonable expectation of privacy in the Wi-Fi context that often overemphasizes the technological nuances and user understanding of Wi-Fi technology. Courts, such as the one in *Innovatio*, use reasoning that is based primarily on the statutory interpretation of the Wiretap Act.[135] The reasoning of the court in *Innovatio* largely echoes the reasoning in another Fourth Amendment case, *United States v. Granderson*, in which Court held that the defendant did not have a reasonable expectation of privacy in his dwelling because of the sizeable slot in a boarded window through which the defendant conducted his illicit drug business.[136] The *Granderson* Court stated that "[a]lthough society generally respects a person's expectations of privacy in a dwelling, what a person chooses voluntarily to expose to public view thereby loses its Fourth Amendment protection."[137]

In *Granderson*, the Court noted that the defendant could have shielded his activities with "simple and obvious" steps, and was not entitled to a reasonable expectation of privacy.[138] The court in *Innovatio* seems to have applied a similar standard for an individual's expectation of privacy—finding

135. In re Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012) (citing 18 U.S.C. §2511(g)(i) (2006)). The court stated:

> The public's lack of awareness of the ease with which unencrypted Wi–Fi communications can be intercepted by a third party is, however, irrelevant to a determination of whether those communications are "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). The language of the exception does not, after all, refer to "communications that the general public knows are readily accessible to the general public." Therefore, the public's expectation of privacy in a particular communication is irrelevant to the application of the Wiretap Act as currently written. Because data packets sent over unencrypted Wi–Fi networks are readily accessible using the basic equipment described above, the Wiretap Act does not apply here.

Id.

136. United States v. Granderson, 182 F. Supp. 2d 315, 321–22 (W.D.N.Y. 2001).

137. *Id.* at 321.

138. *Id.*

that the Wiretap Act does not apply to Wi-Fi interceptions of unencrypted Wi-Fi networks because data packets sent over unencrypted Wi–Fi networks are readily accessible.[139]

However, the "simple and obvious" stream of reasoning is far too simplistic in the context of wireless technologies, especially considering that wireless users are of various technical backgrounds, ranging from the extremely inexperienced to the highly sophisticated. What may be simple and obvious for one Wi-Fi user may be not be simple and obvious for another Wi-Fi user.

Even reasoning distinguishing between encrypted and unencrypted Wi-Fi networks may not be appropriate. Under the *Innovatio* and *Google* approaches, the expectation of privacy may depend on the level of encryption. For many scholars however, the distinction between encrypted communications and unencrypted communications is a distinction without a difference with regard to delimiting the reasonable expectation of privacy. Consider the following:

> When the government obtains encoded text that can only be decrypted with an individual's private key, that individual enjoys an excellent chance that the government will be unable to discover the key and decrypt the communication. However, the Fourth Amendment does not protect the individual if the government decides to devote its resources to decrypting the communication and manages to succeed. From a rights-based perspective, the individual has no enforceable legal means of blocking the government from attempting to *translate* the encoded text into plaintext. She has no right to stop government agents from examining the encoded text and trying to *think of patterns* that might provide the key to translating the encoded text into plaintext . . . . Thus, the government is free to try to crack the code if it wishes: the fact that it will probably fail does not create Fourth Amendment protection.[140]

Treating encryption as a distinction without a difference corresponds with Fourth Amendment jurisprudence. Heat waves cannot be encoded, but sound waves can. Through language or speaking in code, *Katz* and *Silverman* may have encoded the messages that law enforcement officials intercepted. Such measures would have made it more difficult for law enforcement to use the information intercepted, but the interception—and not the decoding—was deemed to be the unconstitutional intrusion.

139. *In re Innovatio IP Ventures*, 886 F. Supp. 2d at 894.
140. Kerr, *supra* note 113 (emphasis added).

A misplaced focus on the nuance of Wi-Fi technology, rather than on the fact that Wi-Fi communications often emanate from spaces where one may have a reasonable expectation of privacy—could lead to the formation of confusing or conflicting theories in case law. By 1994, Congress specifically expanded privacy and security protection for cordless telephone communications by striking out the express exclusion of cordless telephone conversations from the definition of wire communication.[141] Congress reasoned that the widespread, private use of cordless telephones justified the exclusion.[142]

As with sound waves in *Katz* and *Silverman* and heat waves in *Kyllo*, Congress understood that radio waves emanating from cordless telephones were entitled to protection from warrantless surveillance. Courts have had little trouble finding that heat waves, sound waves, and radio waves (in the context of cordless phones) emanating from the home are broadcast widely, but are not broadcast for all to detect and perceive.[143] The same logic should apply to Wi-Fi communications that emanate from private spaces, whether or not the Wi-Fi communications are secured or unsecured. Utilizing an unencrypted Wi-Fi network does not amount to a user openly broadcasting the network to the public. Failure to acknowledge this distinction would be out of line with the Fourth Amendment's purpose[144] and would undermine the vital role that the Internet has—in the Supreme Court's words—"come to play" in private communication.[145]

In *Johnson v. United States*, Justice Jackson summarized the downfalls of the allowing liberal police surveillance in regards to Fourth Amendment privacy rights and the importance of courts to regulate such government surveillance:

> The point of the Fourth Amendment that often is not grasped by zealous officers is not that it denies law enforcement the support of

141. Adam P. Mastroleo, *Does the Fourth Amendment Protect Cordless Telephone Communications, and If So, When?*, 56 SYRACUSE L. REV. 459, 466–67 (2006).

142. *Id.*

143. *See* United States v. Kyllo, 533 U.S. 27, 36 (2001); *see also* Dow Chemical Co. v. United States, 476 U.S. 227, 247 (1986) (Powell, J., concurring in part and dissenting in part) ("The reasonable expectation of privacy standard was designed to ensure that the Fourth Amendment continues to protect privacy in an era when official surveillance can be accomplished without any physical penetration of or proximity to the area under inspection.").

144. *Id.*; *see* Katz v. United States, 389 U.S. 347, 352 (1967) ("[W]hat [Katz] sought to exclude when he entered the [phone] booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen.").

145. *Id.* (emphasis added).

> the usual inferences that reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate, instead of being judged by the officers working on the ground, enterprise of ferreting out crime . . . . The right of officers to thrust themselves into a home is also a grave concern, not only to the individual, but also to a society that chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent.[146]

Given the prevalence of Wi-Fi technology and the judicial precedent concerning analogous technologies, courts should understand that not all broadcasted communication is intended to be public. Under the protection of the Fourth Amendment, communications intended to be private should not be subject to government surveillance without a warrant.

Wireless signals emanating from places other than a person's home are likely not subject to a reasonable expectation of privacy. The majority of Fourth Amendment cases have revolved around the home and public spaces that are understood to be private—such as Katz's phone booth.[147] A public Wi-Fi network is very different because a public Wi-Fi network would be subject to both physical and non-physical monitoring. For example, an individual using a public Wi-Fi network in a coffee shop could reasonably expect other patrons to peek over at the computer screen. In the instance of a workplace, an individual might even be subject to non-physical monitoring or restrictions of use. As such, Fourth Amendment protections would be weaker in the instance of a public Wi-Fi network, given the public nature of the use.

However, in the gray area between public and private Wi-Fi networks, there are a number of scenarios where individuals not using their own, private wireless home connection might have Fourth Amendment protections similar to that of the home. Individuals sharing a large wireless network for personal dwelling or private space, such as students living in a campus dormitory, might hold a reasonable expectation of privacy in their Wi-Fi communications. Even though the network is not private, the origin of

146. Johnson v. United States, 333 U.S. 10, 13 (1948).

147. *Id.* at 351 ("But what [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."). Though Katz's phone booth was in a public location, it is reasonably understood to be private. One would not enter a phone booth if one saw the booth to be already occupied. The sheer size of the phone booth implies that it should only be used to accommodate one, and the closed off nature of the phone booth lends credence to the idea that the booth is a private place, which serves to confine the contents of the phone conversation even if the individual is in view.

the individual's use and the origin of the waves lie in the individual's private space.

V. GOVERNMENTAL PROTECTIONS AGAINST FOURTH AMENDMENT PRIVACY RIGHTS

Although Fourth Amendment precedent suggests that sniffing of private Wi-Fi networks should be protected against unreasonable search and seizure, counterarguments exist. The government might rely upon individual, non-governmental actors to take the initial step towards wireless network surveillance to use as a shield against the Fourth Amendment.[148] In cases such as *Ahrndt*, in which the initial interception was by a third party, the defendant's neighbor, who accessed the defendant's iTunes library through his unsecured Wi-Fi network while a police officer observed the shield becomes especially compelling.[149] Cases such as *United States v. Jacobsen*[150] show that private action does not necessarily render the government's action unreasonable. In *Jacobsen*, the Supreme Court held that police seizure of cocaine found by FedEx employees was not unreasonable because a non-governmental actor conducted the initial search.[151] Although the government agent went beyond the initial private search, the Court held that the Fourth Amendment did not apply.[152]

The government could also easily make an open fields argument—that privacy is not afforded to the open fields and spaces surrounding one's home—against a Fourth Amendment right to privacy,[153] arguing that since the wireless signal went beyond the boundaries and curtilage of the home, an interception was proper. In *United States v. Dunn*,[154] the Court posed a

148. Walter v. United States, 447 U.S. 649, 662 (1980). ("[T]he Fourth Amendment proscribes only governmental action, and does not apply to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.").

149. United States v. Ahrndt, CRIM. 08-468-KI, 2010 WL 373994, at *1–2. (D. Or. Jan. 28, 2010).

150. United States v. Jacobsen, 466 U.S. 109 (1984).

151. *Id.* at 118.

152. *Id.*

153. *See* Dow Chemical Co. v. United States, 476 U.S. 227, 238 (1986) (holding that the government's enhanced aerial photography of the Dow Chemical factory's industrial complex was not protected by the Fourth Amendment, because the Fourth Amendment did not protect "open fields" that surrounded the complex).

154. United States v. Dunn, 480 U.S. 294, 294–95 (1987) (holding that extent-of-curtilage questions should be resolved with particular reference to four factors, which are used to gauge whether the area claimed to be curtilage is so intimately tied to the home itself that it should be placed under the home's "umbrella" of protection).

significant question in terms of Fourth Amendment protection surrounding the home itself: is the area to be searched so intimately tied to the home itself that it should be placed under the home's "umbrella" of Fourth Amendment protection?[155] The government might argue that communications that are broadcast via radio waves outside of the home—even if intercepted within the radius of the Wi-Fi signal—are not under Fourth Amendment protection because they extend outside of the home's curtilage. Especially in cases of students living on a college campus or a professional staying in a hotel overnight, the government might argue that there is so much sharing and cross-using of wireless networks that it extends beyond the curtilage of the home, and that no reasonable expectation of privacy should apply, even in a private place.

Lastly, the government might also argue that Wi-Fi sniffers actually are in common use, and therefore users of unencrypted Wi-Fi networks should reasonably be aware that their wireless communications hold a likelihood of interception. The government might cite the relatively inexpensive nature of the packet sniffer, and the use of the packet sniffer by corporations such as Google and Innovatio, to make the claim that packet sniffers should not be considered sophisticated technology in the current technological climate. The government might reason that unsecured wireless communications falls under the statutory exception to the Wiretap Act that permits a person "to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[156] The implication is that users should not have a reasonable expectation of privacy in the use of unsecured networks and should readily expect that their wireless communications are not private.

VI. CONCLUSION

Recently decided and pending cases such as *Innovatio* and *Google* may establish that the Wiretap Act does not protect the users of unencrypted Wi-Fi networks from interception. Precedent from cases litigated under the Wiretap Act suggests that this determination may depend on technological nuances such as (1) the presence or absence of data encryption and (2) the mechanics of Wi-Fi communication.

155. *Id.*

156. In re Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 892 (N.D. Ill. 2012) (citing 18 U.S.C. §2511(g)(i) (2006)).

If the Wiretap Act does not prevent the government from intercepting unencrypted Wi-Fi networks, it will be imperative for the Supreme Court or Congress to determine whether the Fourth Amendment provides protection. Supreme Court jurisprudence makes clear that other forms of waves—heat waves coming from the home, sound waves coming from the home, and sound waves coming from private spaces—all warrant Fourth Amendment protection.[157] Fourth Amendment jurisprudence, unlike cases interpreting the Wiretap Act, favors individuals' privacy rights in their wireless communications. This right should not rest on technological details and usage but rather on an individual's reasonable expectation of privacy in their wireless communications.

157. Referencing *Silverman*, *Katz*, and *Kyllo*.