THE NEED FOR THE FEDERAL WIRETAP ACT TO EXPAND PROTECTION OF OUR WIRELESS COMMUNICATIONS

Christina Wong*

The uses of Wi-Fi technology are progressing to the point where users may not fully understand the risks of operating on an unsecured Wi-Fi network. Data and communications transmitted on such networks are prone to interception, and it is unclear whether the Federal Wiretap Act offers protection to users. Conflicting provisions in the Federal Wiretap Act do not offer a clear answer as to whether protection is afforded to users.[1]

This paper examines the current Federal Wiretap Act and if it protects unsecured Wi-Fi communications. An analysis of conflicting case law demonstrates that our courts are ill-equipped to take into account policy considerations; I will argue that Congress should step in. A reading of the Communications Act and the Federal Wiretap Act together demonstrates a current lack of understanding of how to protect unsecured Wi-Fi communications. This paper looks at users' mistaken expectations of privacy in their internet communications that stem from a lack of understanding about the technology and a false sense of security. I will also assess these laws under the Fourth Amendment's reasonable expectation of privacy analysis. Finally, this paper advocates for the amendment of the Federal Wiretap Act so that it clearly protects unsecured Wi-Fi communications, meaning that such communications would not be interpreted to be "readily accessible to the general public."[2] Clear protections against the interception of unsecured Wi-Fi communications avoid possible private and social costs of data theft and compensate for users' lack of technical knowledge and ability to protect themselves.

*J.D., May 2014, University of Pennsylvania Law School. Thank you to Professor Christopher Yoo of the University of Pennsylvania Law School, and to student editors Anne Aufhauser and Andrew Morris for their helpful guidance.

[1] 28 U.S.C. § 2511 (2006).

[2] *Id.*

INTRODUCTION

In 2007, Google began its Street View program to collect street-level images of various locations.[3] The service initially allowed users to access panoramic views of only five major U.S. cities, but since the platform's launch, "almost a dozen countries around the world in North America, Europe and the Asia-Pacific region" are now accessible via Street View.[4] People are now able to see real pictures of a possible destination from the comfort of their homes. After several years and iterations, Google now uses a fleet of cars, each of which uses fifteen lenses to take a three hundred and sixty degree photo.[5] Each car also has motion sensors to track its position, a hard drive to store data, a small computer running the system, and lasers to capture three dimensional data to determine distances within

3. *Street View Car*, GOOGLE STREET VIEW, http://www.google.com/intl/en_us/help/maps/streetview/technology/cars-trikes.html (last visited Sept. 29, 2013).

4. Matt Williams, *Behind the Scenes*, GOOGLE MAPS UK, http://www.google.co.uk/maps/about/behind-the-scenes/streetview/ (last visited Jan. 5, 2013).

5. *See Street View Car*, *supra* note 3 (describing the camera technology used on Street View cars).

the Street View imagery.[6]

In May 2010, Google admitted to having collected data from Wi-Fi[7] networks as part of the Street View project. Google claimed the purpose of this collection was to help Google establish users' locations and provide location-based services. However, Google also collected "payload" data—the content of Internet communications—which included email and text messages, passwords, Internet usage history, and other highly sensitive personal information.[8] Google maintained that it had only collected fragmented data from non-password-protected and unsecured Wi-Fi networks.[9] However, in October 2010, Google admitted that "in some instances, entire emails and URLs were captured, as well as passwords."[10] None of this collected information was publicly disseminated by Google.

This admission raised serious concerns about privacy and potential violations of the Federal Wiretap Act (FWA)[11] and Communications Act (CA).[12] Google argued that unsecured Wi-Fi communications are excluded from the Federal Wiretap Act's regulations because such communications are "readily accessible to the general public."[13] Both the Federal Trade Commission (FTC) and Federal Communications Commission (FCC) investigated the scandal.[14] The FTC closed its investigation, concluding that Google's deletion of the material and revised privacy procedures sufficiently remedied the situation.[15] The FCC took over the investigation

6. *See Street View Car*, *supra* note 3 (referencing the technology that the Street View car utilizes to gather and store data).

7. "Wi-Fi" is shorthand for "Wireless Fidelity" and is the current industry standard for most wireless data networks. There are other important standards such as WiMax and Bluetooth. *A guide to Wireless Network Standards*, PIXAVI http://www.pixavi.com/company-technology8-wireless-pixavi.html (last visited March 21, 2013).

8. Alan Eustace, *WiFi Data Collection: An Update*, GOOGLE OFFICIAL BLOG (June 9, 2010), http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

9. *See id.* (explaining that Google had "been mistakenly collecting samples of payload data from open (i.e. non-password-protected) WiFi networks").

10. Alan Eustace, Creating stronger privacy controls inside Google, Google Official Blog (October 22, 2010), http://googlepublicpolicy.blogspot.com/2010/10/creating-stronger-privacy-controls.html.

11. 18 U.S.C. § 2510-22 (2006).

12. 47 U.S.C. § 605 (2006).

13. *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1073 (N.D. Cal. 2011).

14. *See* Letter from Marc Rotenberg, Exec. Dir., Elec. Privacy Info. Ctr., to Julius Genachowski, Chairman, Fed. Commc'ns Comm'n (May 18, 2010), *available at* http://epic.org/privacy/cloudcomputing/google/EPIC_StreetView_FCC_Letter_05_21_10.pdf (noting that two senior members of the House Commerce Committee urged the FTC "to undertake an investigation and to reply to certain questions by June 2, 2010.").

15. *See* Letter from John Verdi, Dir., EPIC Open Gov't Project, to Office of Gen. Counsel, Fed. Trade Comm'n (Feb. 11, 2011), *available at*

and, in April 2012, fined Google $25,000 for obstructing its investigation.[16] The FCC chose, however not to take any enforcement action with respect to the FWA or the CA.[17] As of 2012, at least twelve countries have investigated Google's actions and at least nine have found that Google violated their laws.[18]

Google's accessing of data demonstrates the rising risks to private users' Wi-Fi communications. Many people who set up Wi-Fi routers choose to leave them open. Such open Wi-Fi networks have become more popular with an increasing number of access points, known as "hotspots,"[19] emerging in various public spaces such as airports, restaurants,[20] parks, buses, trains,[21] and airplanes. Many people operate on such networks, which usually need a user to agree to the respective Terms and Conditions,[22] without really realizing that these networks are "open."

This paper highlights the uncertainty of unsecured Wi-Fi communications protection when, at best, the FWA can only offer piecemeal protection. Part I lays out the current state of wireless technology and provides the foundation for subsequent statutory interpretation. Part II analyzes the FWA and CA separately and discusses current statutory interpretations of the provisions in tension. Part II also explores how different courts have come to opposite conclusions on whether the FWA protects unsecured Wi-Fi communications. Part III analyzes what it means to protect such communications when reading the FWA and CA together. Expectations of privacy stem from users' understanding of the technology, and a comparable Fourth Amendment analysis is offered as support that such expectations are reasonable. Finally, Part IV advocates ways to reform the FWA by clearly delineating

http://epic.org/privacy/ftc/google/FTC_Streetview_FOIA_Appeal2.pdf (appealing administratively the FTC's decision to close the investigation, believing that the FTC should have pursued the claim further).

16. Google Inc., 27 FCC Rcd 4012 (April 13, 2012) (Notice of Apparent Liability for Forfeiture) [hereinafter Notice of Apparent Liability for Forfeiture].

17. *Id.*

18. *Investigations of Google Street View*, ELECTRONIC PRIVACY INFORMATION CENTER, *available at* http://epic.org/privacy/streetview/ (last visited Jan. 5, 2012).

19. *See, e.g., XFINITY WiFi Hotspots*, COMCAST, http://customer.comcast.com/help-and-support/internet/about-xfinity-wifi-internet/ (last visited Dec. 26, 2013).

20. *See, e.g.*, *AT&T Wi-Fi (United States)*, STARBUCKS, http://www.starbucks.com/coffeehouse/wireless-internet (last visited Dec. 29, 2012) (discussing Wi-Fi access at Starbucks).

21. *See, e.g.*, *Journey with Wi-Fi*, AMTRAK, http://www.amtrak.com/journey-with-wi-fi-train-station (last visited Dec. 29, 2012) (offering Wi-Fi access to Amtrak train passengers).

22. *See, e.g., Accept & Connect*, STARBUCKS, http://www.starbucks.com/coffeehouse/wi-fi-auth (last visited Dec. 26, 2013) (requiring users to abide by the AT&T Terms and Conditions and Acceptable Use Policy).

how unsecured Wi-Fi communications should be protected by clarifying certain provisions of the existing statute.

I. THE CURRENT STATE OF WIRELESS TECHNOLOGY

Wi-Fi allows electronic devices to exchange data wirelessly. These devices operate using the common standards, collectively referred to as 802.11 protocols, which are set by the Institute of Electrical and Electronics Engineers ("IEEE").[23] The basic network setup consists of a Wireless Access Point ("WAP"), often referred to as a "wireless router," which is typically connected to the user's Internet Service Provider ("ISP") network through a wired connection. Communications travel from the WAP over radio frequencies to any device that is equipped with a Wi-Fi adapter, such as a laptop or smartphone.

Although the FCC regulates most radio communications in the United States, Wi-Fi networks operate in the unregulated frequency ranges known as Industrial, Scientific and Medical ("ISM") radio bands.[24] Anyone can use this part of the radio spectrum without a license from the FCC. Many devices such as microwaves, cordless phones, Bluetooth devices, and wireless garage door openers operate in one of the ISM bands.[25] Wi-Fi networks use different frequency[26] ranges of the ISM bands depending on the particular protocol being used. Wi-Fi products are identified as 802.11, and are then further delineated by a lower case letter that identifies which specific technology is in operation.[27] Each Wi-Fi network is configured to operate on a channel, which is a subdivision of one of the frequency ranges of the ISM bands.[28]

Wi-Fi technology is increasingly used in our lives, with more Wi-Fi enabled devices entering the market[29] and progressive Wi-Fi technology

23. IEEE Computer Society, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (2012), *available at* http://standards.ieee.org/getieee802/download/802.11-2012.pdf.

24. Patrick Butler and Austin Harney, *A Smart Modem for Robust Wireless Data Transmission Over ISM Bands (433 MHz, 868 MHz and 902 MHz)*, 39 ANALOG DIALOGUE 1, 1 (Mar. 2005), http://www.analog.com/library/analogDialogue/archives/39-03/smart_modem.pdf.

25. *See id.* at 1 (listing other devices that use ISM bands).

26. Wi-Fi products operate in the 2.4 GHz or 5 GHz bands. Discover and Learn, WI-FI ALLIANCE, http://www.wi-fi.org/discover-and-learn (last visited Jan. 2, 2013).

27. The subdivision of protocols are 802.11a, 802.11b, 802.11g, and 802.11n, all of which operate in the 2.4 GHz or 5 GHz bands with different bandwidth data rates. *Id.*

28. *802.11b WiFi Frequency Channels*, MOONBLINK, http://www.moonblinkwifi.com/2point4freq.cfm (last visited Dec. 29, 2012).

29. WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) are two

being developed.[30] When using Wi-Fi devices, users can protect their data through various encryption schemes.[31] However, the user must manually enable these security mechanisms, or the Wi-Fi networks will operate in an open and unsecured mode.[32] This tends to create a bias towards unsecured Wi-Fi networks, which may impede users' privacy protection. Users, however, are becoming more aware of the potential risks of an unsecured network thanks to numerous hacking incidents[33] and many articles describing and encouraging the use of network security systems.[34]

Interestingly, there are also many who advocate for more open wireless networks.[35] One of the largest coalitions in this movement is the Open Wireless Movement, which advocates for open wireless networks in order to make the Internet more open and available.[36] Offered benefits include increasing efficiency, boosting innovation and the economy, and bringing the Internet to those who cannot afford it.[37] The group's website

different schemes, with the latter providing much stronger protection. *Wi-Fi Enabled Devices*, OPTIMUM, http://optimum.custhelp.com/app/answers/detail/a_id/2421/~/wi-fi-enabled-devices (last visited Dec. 29, 2012).

30. *See, e.g.*, Long Term Evolution (LTE): A Technical Overview, MOTOROLA, (2007), *available at* http://www.motorola.com/web/Business/Solutions/Industry%20Solutions/Service%20Providers/Wireless%20Operators/LTE/_Document/Static%20Files/6834_MotDoc_New.pdf (discussing one such technology, Long-Term Evolution (LTE)).

31. Ashley Poland, *What is the Strongest WiFi Encryption?*, HOUS. CHRON. http://smallbusiness.chron.com/strongest-wifi-encryption-66876.html (last visited Dec. 26, 2013).

32. *Security*, WI-FI ALLIANCE, http://www.wi-fi.org/discover-and-learn/security (last visited Jan. 2, 2013).

33. Though unrelated to unsecured networks specifically, recent revelations that the National Security Agency collects meta-data may have also increased interest in secured networks and what information can be obtained from individuals. Charlie Savage, *N.S.A. Often Broke Rules on Privacy, Audit Shows*, N.Y. TIMES, Aug. 16, 2013, at A0, *available at* http://www.nytimes.com/2013/08/16/us/nsa-often-broke-rules-on-privacy-audit-shows.html; *see also, e.g.*, Tim Bradshaw, *Hackers embarrass Apple with data leak*, FINANCIAL TIMES, http://www.ft.com/cms/s/0/effd1712-f6af-11e1-827f-00144feabdc0.html#axzz2H7aG42k8 (noting that a hacker group allegedly obtained data about Apple product users by hacking into an FBI laptop).

34. *See, e.g.*, MOONBLINK, *supra* note 28 (illustrating how certain Wi-Fi channels can enhance a wireless security system).

35. For example, numerous cities and municipalities are offering free wireless access. *See, e.g.*, Phillip Dampier, *Binghamton To Expand Free Wi-Fi in Downtown Region – Encourages Residents to Share Their Connection*, STOP THE CAP! (July 22, 2009), http://stopthecap.com/2009/07/22/binghamton-to-expand-free-wi-fi-in-downtown-region-encourages-residents-to-share-their-connection/ (documenting the expansion of free Wi-Fi in the town of Binghamton); *Wi-Fi (Wireless Internet)*, CITY OF PONCA CITY, OKLAHOMA, http://www.poncacityok.gov/index.aspx?NID=417 (describing the free Wi-Fi service offered in Ponca City, Oklahoma) (last visited Jan. 2, 2013).

36. OPEN WIRELESS MOVEMENT, https://openwireless.org/ (last visited Jan. 2, 2013).

37. *Id.*

seeks to dispel myths that an open wireless network is a security risk by encouraging users to educate themselves about further security measures they can take.[38] Such tools include personal firewalls, Virtual Private Networks[39] (VPN), Secure Socket Layer[40] (SSL), and Hypertext Transfer Protocol Secure (HTTPS) to reduce the risk of compromised privacy.[41]

II. PRIVACY FOR ELECTRONIC COMMUNICATIONS

The United States Constitution does not explicitly provide for the right to privacy, though the Supreme Court has recognized it in many amendments, guaranteeing that the government will refrain from intruding in private speech, religion, homes, and thoughts.[42] The Fourth Amendment is analyzed in Part III.B in more detail, though it is important to note that this doctrine only applies to government searches and that courts have found that it provides little privacy protection to technological information exposed to the public.[43] The Supreme Court typically addresses issues of privacy on a case-by-case basis where new technologies create new privacy problems.[44] Historically, the Court has been slow to respond to such problems. With respect to technology, privacy law has evolved to define a

38. *Id.*

39. VPN technology uses public unsecured network infrastructure to provide secure access to private networks. Usually, VPN technology is used to provide remote offices or individual users with access to their organization's work. Roger Cheng, *Lost Connections*, WALL ST. J., Dec. 11, 2007, http://online.wsj.com/article/SB119717610996418467.html.

40. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. *FAQ: What is SSL?*, SSL.COM, *available at* http://info.ssl.com/article.aspx?id=10241 (last visited Jan. 4, 2013).

41. *See*, WI-FI ALLIANCE , *supra* note 32 (listing the different security measures that can be used to maintain privacy on the Internet).

42. U.S. CONST. amend. I–V.

43. See *infra* Part III.B for an analysis under the Fourth Amendment.

44. *See, e.g.*, Hank Greely, *The Supreme Court, New Technologies, and Privacy—Another Case of Approach/Avoidance*, SLS BLOG (Jan. 23, 2012), http://blogs.law.stanford.edu/lawandbiosciences/2012/01/23/the-supreme-court-new-technologies-and-privacy-%E2%80%93-another-case-of-approachavoidance/ (noting the Court's tendency to "approach answering questions . . . but then back off them" in *United States v. Jones*, 132 S.Ct. 945 (2012)); Nicole Greenstein, *Privacy and the Law: How the Supreme Court Defines a Controversial Right*, TIME.COM (July 31, 2013) http://nation.time.com/2013/08/01/privacy-and-the-law-how-the-supreme-court-defines-a-controversial-right/ (discussing the Supreme Court's approach to five previous privacy cases); Kashmir Hill, *Supreme Court Justices Concerned Abourt Pervasive, Technology-Enabled Government Surveillance*, FORBES.COM (Nov. 8, 2011, 1:30 PM), http://www.forbes.com/sites/kashmirhill/2011/11/08/supreme-court-justices-concerned-about-pervasive-technology-enabled-government-surveillance/ (discussing the arguments in *United States v. Jones*, 132 S.Ct. 945 (2012)).

reasonable expectation of privacy under *Katz v. United States*.[45] No expectation of privacy exists, however, where a communication is disclosed to a third party.[46] Finally, the Electronic Communications Privacy Act[47] of 1986 (ECPA) which was enacted a year after *Katz,* requires a balancing of the individual's privacy needs with the needs of law enforcement. Congress enacted the ECPA to "meet the constitutional requirements for electronic surveillance" enunciated in *Katz*.[48]

In addressing privacy concerns for electronic communications, the FWA and CA should be read together.[49] The FWA was enacted in 1968 and was amended by the ECPA in 1986.[50] The CA was enacted in 1934 and amended in 1968 to cross-reference the FWA.[51]

A. The Federal Wiretap Act

The FWA has been famously resistant to interpretation.[52] The statute has an interlocking set of prohibitions, definitions, and exceptions that defies facile comprehension. Congress, in enacting the FWA in 1968, was primarily concerned with the live surveillance of telephone conversations and electronic eavesdropping. The statute focused on regulating law enforcement and investigation techniques to combat crime, though it also

45. 389 U.S. 347, 351 (1967).

46. United States v. Miller, 425 U.S. 435, 443 (1976).

47. 18 U.S.C. §§ 2510-2522 (2006).

48. Mitchell v. Forsyth, 472 U.S. 511, 532 (1985) (citing United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 300 (1972)).

49. The House Report stated that the "Committee has drafted the present Act [18 U.S.C. § 2510 et seq.] with an eye to its interplay with Section 705(a) of the Communications Act of 1934." H.R. REP. NO. 99-647, at 41 (1986).

50. U.S. Dep't of Justice, *Federal Statutes*, JUSTICE INFORMATION SHARING, https://it.ojp.gov/default.aspx?area=privacy&page=1284.

51. Google Inc., 27 F.C.C.R. 4012, 4014 (2012).

52. *See, e.g.*, United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (stating that the FWA is "a complex, often convoluted, area of the law"); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (calling the ECPA "famous (if not infamous) for its lack of clarity"); Briggs v. Am. Air Filter Co., 630 F.2d 414, 415 (5th Cir. 1980) (commenting on the court's desire to have "planted a powerful electronic bug in a Congressional antechamber to garner every clue concerning Title III" to aid in "the troublesome task of an interstitial interpretation of an amorphous Congressional enactment"); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820 (2003) (stating that the "law of electronic surveillance is famously complex, if not entirely impenetrable"); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1292 (2004) ("[The ECPA contains] a myriad of different terms with complicated definitions. The statute zigzags with dozens of cross-references. . . . [I]t contains at least seven different legal threshold requirements for government surveillance . . .").

regulated private conduct in the same realm.[53] Much scholarship has also focused on the statute's role in regulating government surveillance.[54] Whether the FWA protects all unsecured Wi-Fi communications is unclear. While the statutory language is not specifically aimed at protecting unsecured Wi-Fi communications, the laws nevertheless could be applied to Wi-Fi communications.

The FWA defines liability based solely on whether the privacy of communications has been breached, and not, for the most part, on what information was obtained, who obtained it, or how it was used. Regulation under the FWA is binary: permitted actions are not subject to any regulation whatsoever[55] and prohibited actions are a potential felony and subject to statutory damages of $10,000 per violation.[56] The FWA prohibits intentionally intercepting[57] or disclosing wire, oral, or electrical communications, except under certain exceptions.[58] Courts have interpreted "intercept" to mean an acquisition of a communication contemporaneous with transmission.[59] The original version of the act before 1986 only protected wire and oral communications.[60] The addition of "electronic communications" as a form of protected communications in 1986 covers "any transfer of signs, signals, writing, images, sounds, data,

53. S. REP. NO. 90-1097, at 70 (1968) ("The major purpose of title III [of the Federal Wiretap Act] is to combat organized crime.").

54. *See, e.g.*, Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1287 n.11 (2005) (stating that modern surveillance statutes were primarily passed to address the legality of government surveillance activities under the Fourth Amendment); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007), available at http:// stlr.stanford.edu/pdf/freiwald-first-principles.pdf (contending that a four factor test should be used to assess whether statutes "implicate Fourth Amendment concerns about intrusive government investigatory methods"); Kerr, *supra* note 51, at 807 (stating that unless Congress clarifies statutes "[t]he government's compliance with the Internet surveillance laws will remain unexamined.").

55. This is in contrast to many other privacy regulations that govern based on social context, the judgments of reasonable people, detailed administrative regulations subject to discretion in enforcement, or more finely graded scales of potential damages.

56. 18 U.S.C. §§ 2511(4)(a), 2520(c)(2) (2006).

57. The structure and legislative history of the FWA suggest that interceptions must, at some level, be accomplished by a person. 18 U.S.C. § 2510(4) (2006) ("'[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.").

58. 18 U.S.C. §§ 2510-2522 (2006).

59. United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (holding that accessing or retrieving stored communications, not in transit, falls under the regulation of the Storage Communications Act, 18 U.S.C. §§ 2701-2712 (2006)). Interception of such communications is not within the scope of this paper.

60. 18 U.S.C. §§ 2510-2522 (2006) ("Title III originally covered only 'wire' and 'oral' communications but was significantly revised by Title I of the ECPA in 1986 to include electronic communications.").

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 . . . ."[61] Data that is transmitted over a Wi-Fi network uses radio signals, placing such electronic communications within the provenance of the FWA.[62]

The FWA provides a set of exceptions to the broad prohibitions placed on the interception of electronic communications.[63] The provision applicable to Wi-Fi communications is as follows:

> It shall not be unlawful under this chapter or chapter 121 of this title for any 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.[64]

In applying the law to its collection of personal data over unsecured Wi-Fi networks, Google claimed that its actions fell under this exception because unsecured Wi-Fi communications are "readily accessible to the general public."[65] The terms "readily accessible to the general public" and "configured" are key to understanding this exception. The definition of "readily accessible" is provided in subsection 2510(16) of the FWA:

> (16) "[R]eadily accessible to the general public" means, with respect to a radio communication, that such communication is not—
> (A) scrambled or encrypted;
> (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention

61. 18 U.S.C. § 2510(12) (2006).

62. *See generally In re* Pharmatrack, Inc., 329 F.3d 9, 18 (1st Cir. 2003) (holding that transmissions of completed online forms to a website constitute "electronic communications" under the FWA); Steiger, 318 F.3d at 1047 (holding that information transmitted by a computer virus falls within the meaning of "electronic communications" under the FWA); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002) (holding that website content is included in the definition of "electronic communications" under the FWA because the information is transmitted from the website to the user via a server, which is one of the specified mediums within the FWA) .

63. Most of these exceptions do not apply in the case of obtaining payload data from an open and unsecured Wi-Fi network. For example, one exception is when there is permission for an electronic communications provider's agent to intercept communication "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service." 18 U.S.C. § 2511(2)(a)(i) (2006). Another exception is if one of the parties to the communication gives consent to the interception or if the person intercepting the communication is acting under the "color of the law." 18 U.S.C. § 2511(2)(c) (2006).

64. 18 U.S.C. § 2511(2)(g)(i) (2006).

65. Notice of Apparent Liability for Forfeiture, *supra* note 16.

> of preserving the privacy of such communication;
> (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
> (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
> (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94, of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.[66]

The legislative history clarifies that:

> [radio] communications are considered readily accessible to the general public unless they fit into one of the five specified categories . . . . Thus, the radio communications specified in [the then-]proposed subsection 2510(16) are afforded privacy protections under [the FWA] unless another exception applies.[67]

The question here is whether this definition of "readily accessible to the general public" applies to electronic communications.

1. "Readily Accessible"

Subsection 2510(16)'s definition of "readily accessible" with respect to "radio communication," does not clarify whether Wi-Fi communications, as electronic communications, can benefit from the exception in subsection 2510(16). However, subsection 2510's opening language, "As used in this chapter," implies that 2150(16)'s definition of "readily accessible" should apply wherever the term appears, unless the definition was explicitly confined to specific subsections.[68] If the 2510(16) definition does not apply, the term "readily accessible" will be left without any statutory definition with respect to electronic communications unrelated to "traditional radio services," including Wi-Fi communications.[69]

If subsection 2510(16)'s definition of "readily accessible to the general public" applies to Wi-Fi communications, then whether such communications were secured would determine whether Wi-Fi

66. 18 U.S.C. § 2510(16) (2006).
67. S. REP. NO. 99-541, at 14-15 (1986).
68. 18 U.S.C. § 2510 (2006).
69. *Id.*

communications would receive protection. Therefore, secured Wi-Fi communications would fall under 2510(16)(A)'s "scrambled or encrypted" provision, and thus the "readily accessible to the general public" exception would not apply and such communications would be protected. Whether unsecured Wi-Fi communications would receive protection is unclear.

Protection for unsecured Wi-Fi communications could fall under subsection 2510(16)(E). A plain reading of subsection 2510(16)(E) indicates that at least some communications over certain Wi-Fi radio frequencies—allocated under parts 25 and 94 and subparts D, E, and F of part 74 of the FCC rules—do not fall under the "readily accessible to the general public" exception. The Senate Report states that the scope of this provision includes "satellite communications, auxiliary broadcast services and private microwave services, each of which routinely carries private business or personal communications."[70]

The frequencies allocated under parts of the FCC rules in subsection 2510(16)(E) partly overlap with the Wi-Fi operating frequencies. As discussed in Part I, Wi-Fi networks divide their operating frequency bands into channels. Only certain parts of the 802.11 protocol's frequency range are allocated under the FCC rules, which means that communications over channel 11 and parts of channels 7, 8, 9, and 10 of the 802.11b protocol are covered under the protections of subsection 2510(16)(E).[71] Channel 11 is the only commonly used 802.11b protocol channel that may be fully protected under subsection 2510(16)(E).[72] Any electronic communications transmitted over channel 11 of the 802.11b, 802.11g, or 802.11n Wi-Fi networks might not be considered "readily accessible to the general public," meaning such communications could still violate the FWA. Similarly, only certain channels of the 802.11a networks are covered by subsection 2510(16)(E) and could still be protected from interception under the FWA.[73] However, practically, the privacy protections found in subsection 2510(16)(E) are limited because the interception must be found on the exact channels discussed above.

Admittedly, while these frequencies are used by Wi-Fi communications, they were mostly discussed in the context of radio

70. S. REP. NO. 99-541, at 15 (1986).

71. The operating frequency range 2400—2495 MHz of the 802.11b, g, n protocols overlaps with the frequency bands 2450—2467, 2467—2483.5 allocated under the FCC rules.

72. Channels 1, 6, and 11 are the most commonly used channels in operating 802.11b Wi-Fi networks, but channels 1 and 6 are outside the frequency ranges of § 2510(16)(E).

73. 802.11a, which operates in the 5170-5815 MHz frequency range, uses twelve official channels. Only the 5091—5250 MHz frequency range is allocated by the FCC under part 25 of its rules, which means that only communications over the channels 36, 40, 44, and 48 of the 802.11a networks are covered by § 2510(16)(E).

broadcasting technology.[74] Yet the legislative history does not indicate that Congress intended to exclude unsecured Wi-Fi communications from the FWA's protection. The Senate Report accompanying subsection 2510(16)(E) indicates that the Senate's main concern was protecting "private business or personal communications," without mention of whether these communications are encrypted or not.[75] Without further clarification, it is unclear whether unsecured Wi-Fi communications are afforded protection. However, as is, users will not be able to benefit from subsection 2510(16)(E)'s protections for two reasons: the unclear meaning of "with respect to a radio communication"[76] and the uncertainty about whether 2510(16)(E)'s protections apply to Wi-Fi communications. Furthermore, users may not benefit because of the need for a communication to be on a certain frequency or channel.

2. Configuration

The FWA's "configuration" requirement must be satisfied for the exemption from the FWA's protection to apply, assuming that unsecured Wi-Fi communications are determined to be "readily accessible to the general public." Subsection 2511(2)(g)(i) states that it is legal to intercept "electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[77] In making a configuration requirement, a user knowingly allows or disallows access to his communications.

Neither the FWA nor the Senate Report elaborates on whether a system needs to be configured by the user himself to fall under the "readily accessible to the general public" exception or whether a default open network configuration deprives the user of privacy protection. If the exception requires an affirmative choice in configuration by the user, then a user who has simply acquiesced in the default setting might be protected under the act. If the exception does not require a choice in configuration, then a user who has acquiesced in the default setting might not be protected.

Even if a user is operating on an open network, the user's private

74. *See* 47 C.F.R. 94 (2010) (discussing 47 C.F.R. 94 (2010)'s point 24 regarding personal communication services and point 74 regarding experimental radio, auxiliary, special broadcast and other program distributional services); 47 C.F.R. 94 (1995) (detailing point 94 and its treatment of private-operational–fixed microwave service).

75. *See* S. REP. NO. 99-541, at 15 (1986) ("These communications include satellite communications, auxiliary broadcast services and private microwave services, each of which routinely carries private business or personal communications.").

76. 18 U.S.C. § 2510(16) (2006)

77. 18 U.S.C. § 2511(2)(g)(i) (2006).

communications are probably not intended to be public communications. The Senate Report noted that "[t]he term 'configure' is intended to establish an objective standard of design configuration for determining whether a system receives privacy protection."[78] This language suggests that if the electronic communications system enables what users consider private communications, then such communications may protected under the FWA. For example, a home Wi-Fi network is not necessarily designed to provide public communications. Some users may choose to enable their system for public access. In that instance, the focus is on "access," not whether the communications themselves are public. Similarly, a public Wi-Fi hotspot at a local coffee shop is enabled to provide public access to a Wi-Fi network, but users still expect a degree of privacy while on the Internet.[79]

Although the case law dealing with the "configuration" issue is sparse, *United States v. Ahrdnt*[80] sheds some light on how courts are approaching the issue. In this case, the defendant had operated on an unsecured Wi-Fi network at his home and had his iTunes[81] program configured to publicly share his video library, including a collection of child pornography. A police officer accessed some of these files using the defendant's unsecured Wi-Fi network. The district court held that since the wireless network and iTunes software were configured to allow general public access, the police officer lawfully accessed the defendant's files under the FWA.[82] The court came to this conclusion even though operating the Wi-Fi network as "open" did not require any positive action by the defendant. However, since the default factory configuration of the wireless router was to operate in an unsecured mode, sharing an iTunes library did require positive action by the defendant. The Ninth Circuit reversed and remanded, setting out three areas for further fact finding:[83] (1) whether file sharing over a wireless network can be characterized as a "broadcast" of the contents of those files; (2) whether the defendant intentionally enabled sharing of his files over his wireless network; and (3) whether the accessed images were accessible via the Internet at that time or any time prior.[84] With regard to the first question, "broadcast" does not fall under the FWA, but rather the

78. S. REP. NO. 99–541, at 18 (1986).

79. *See, e.g.*, *Dangers of Free Public WiFi*, CBS News, July 8, 2010, *available at* http://www.cbsnews.com/news/dangers-of-free-public-wifi/.

80. 475 Fed. App. 656 (9th Cir. 2012).

81. iTunes is a software application that lets users purchase, play, and organize digital music and video on their computers and other mobile devices. *What is iTunes?*, ITUNES, http://www.apple.com/itunes/what-is/ (last visited Jan. 3, 2012).

82. *See* Ahrdnt, 475 Fed. App.,at 657.

83. *Id.* at 656.

84. *Id.* at 658.

CA. The second question focuses on whether the defendant himself took a positive action by sharing his files instead of just enabling access to them. Although this second question concerns access to files, an analogy can be made to whether a user actively allowed access to a personal Wi-Fi network. Perhaps "configuration" can be determined based on a user's actual actions, instead of the configuration of a manufacturer's actions in configuring a default setting. The third question is not directly applicable to this analysis.

3. Case Law

There have not been many cases that have dealt with the issue of whether unsecured Wi-Fi communications are protected under the FWA. The two cases existing to date have reached opposite conclusions.

a. Cases Involving Google

In the first of the cases to rule on intercepting unsecured Wi-Fi communications, *In re Google Inc. Street View Electronic Communications Litigation*, the United States District Court for the Northern District of California chose not to apply subsection 2510(16)'s definition of "readily accessible to the general public" to Wi-Fi communications.[85] The court construed the term "radio communication" narrowly to include only "traditional radio services," such as "public-directed radio broadcast communication."[86] Since the FWA defined "electronic communication," but not "radio communication," the court, relying on legislative history, found that Congress added the definition in subsection 2510(16) to alleviate radio hobbyists' concerns and to clarify that "intercepting traditional radio services is not unlawful."[87] The court further reasoned that the 2510(16) exceptions were "drafted for the particular technology of traditional radio broadcast mediums and do not address any broader radio-based communications technology."[88] Essentially, the court found that even though Wi-Fi networks do transmit data using radio waves, "Congress did not intend Section 2510(16)'s narrow definition of 'readily accessible to the general public' to apply for purposes" of subsection 2511(2)(g)(i)'s

85. In November 2013, Google settled these cases by agreeing to pay $17 million to 37 states and the District of Columbia. Claire Miller, *Google to Pay $17 Million to Settle Privacy Case*, N.Y. TIMES, (Nov. 18, 2013), http://www.nytimes.com/2013/11/19/technology/google-to-pay-17-million-to-settle-privacy-case.html?hpw&rref=technology.

86. *In re* Google Inc., 794 F. Supp. 2d 1080 (2011)

87. *Id.* at 1079 (quoting 132 Cong. Rec. 14,601 (1986)) (internal quotations omitted).

88. *Id.* at 1080.

exception to liability for intercepting all electronic communications.[89] The court also noted that the data transmitted and collected by Google "w[as] not readable by the general public without the use of sophisticated packet sniffer technology."[90] Thus, these communications were not designed or intended to be public.[91]

The Ninth Circuit affirmed the district court's decision in *Joffe v. Google, Inc.*, ruling that Google's data collection did not fall within the "readily accessible to the general public" exception within the FWA.[92] The court further held that data transmitted over a Wi-Fi network is not a "radio communication" as defined in the FWA, since the technical definition does not conform to the common understanding held by the enacting Congress.[93] The court found that "radio communication" usually does not encompass technologies like satellite television and thus should not encompass other types of technology like Wi-Fi communications that do not fit in the traditional radio technologies.[94] In its analysis, the court looks at the possible interpretations of the terms "radio communication" and "electronic communication," and whether one is a subset of the other.[95] Congress's enactment and repeal of § 2510(16)(F) offers little guidance.[96]

b. In re Innovatio IP Ventures, LLC Patent Litigation

In contrast to *In re Google*, the United States District Court for the Northern District of Illinois in *In re Innovatio IP Ventures, LLC Patent Litig.* ruled that the FWA did not prohibit the interception of communications sent over unsecured Wi-Fi networks provided by various commercial entities.[97] This case was an infringement suit in which Innovatio accused various commercial entities that provide Wi-Fi to their customers of violating its patents in Wi-Fi technology.[98] To gather evidence of the defendants' alleged infringement, Innovatio used "commercially available Wi-Fi network analyzers" to intercept data.[99] Concerned that its activities might violate the FWA, Innovatio sought a

89. *Id.* at 1081.
90. *Id.* at 1082.
91. *Id.*
92. Joffe v. Google, Inc., No. 11-17483, slip op. at 12 (9th Cir. Sept. 10, 2013).
93. *Id.* at 13.
94. *Id.* at 15.
95. *Id.* at 31.
96. *Id.*
97. 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012).
98. *Id.* at 889.
99. *Id.* at 890.

preliminary ruling on the admissibility of the evidence it obtained.[100]

The court distinguished *In re Google*, noting how that decision was based in part on the fact that the plaintiffs had alleged that their communications were not readable by the general public without the use of sophisticated packet sniffing technology, a proposition that the court accepted as true under the standards applicable to a motion to dismiss.[101] The court in *In re Innovatio* was not held to accept such an allegation and ruled that Innovatio's collection activities did not violate the FWA, per subsection 2511(2)(g)(i), because the Wi-Fi technology Innovatio used is readily accessible to the general public.[102] This technology "is available to the public for purchase for $698.00," and a more basic version can be purchased for $198.00.[103]

In re Innovatio seems to suggest that "readily accessible to the general public" can be fulfilled by the technology itself being accessible to the public at a local store.[104] This adds another dimension to the debate over public networks versus private communications.

B. The Communications Act

In 1934, Congress enacted the CA. The precise scope of subsection 605(a) of the CA was difficult to determine, since the language used to regulate a new technology, telephones, was more appropriate for an older and well-understood technology, telegraphs. The problems with subsection 605 were widely recognized at the time of its enactment and debates centered on amending the CA gradually shifted to calling for entirely new legislation. In 1968, Congress amended the CA to cross-reference the FWA, which had been enacted in 1968 as well. The first sentence of subsection 605(a) prohibits certain conduct "[e]xcept as authorized by [the FWA]." Subsection 605(a) governs unauthorized publication or use of communications,[105] the provisions of which are as follows:

100. *Id.*
101. *Id.* at 893.
102. *Id.* at 894.
103. *Id.* at 893.
104. Subsequent cases at the district level have not ruled directly on the issue of what is "readily accessible to the general public." *See In re* Innovatio IP Ventures, LLC Patent Litig., No. 11-C-9308, 2013 WL 3874042 (N.D. Ill. July 26, 2013) (holding that the patent claims were essential to the implementation of wireless standards proposed by professional organizations); *In re* Innovatio IP Ventures, LLC Patent Litig., 921 F.Supp.2d. at 922 (holding that the licensing campaign was protected as petitioning activity under the First Amendment and Noerr-Pennington Doctrine, and the manufacturers stated a breach of contract claim against the patent owner).
105. 47 U.S.C. § 605(a) (2006).

> [N]o person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto.[106]

The passage of the FWA transferred "regulation of the interception of wire or oral communications" from the CA to the new FWA.[107] The FWA outlined a comprehensive scheme of the conditions under which such communications could be intercepted, disclosed, or used without incurring criminal or civil penalties.[108]

The Senate Report stated that subsection 605(a) was "not intended to apply to radio broadcasts or transmission by amateurs or others for the use of the general public."[109] There currently is no FCC precedent in addressing the application of subsection 605(a) to Wi-Fi communications. Likewise, the courts have not explicitly ruled on such communications, though there is some case law on interception of oral communications. In *United States v. Rose*,[110] the First Circuit concluded that in amending subsection 605 to cross-reference the FWA, Congress incorporated an expectation of privacy in subsection 605.[111] The court recognized, however, that incorporating subjective and reasonable objectives would diminish subsection 605's protection.[112] This expectation of privacy will be addressed below.

III. EXPECTATIONS IN PROTECTING UNSECURED WI-FI COMMUNICATIONS

A fork in the analysis occurs in determining how to protect Wi-Fi communications based on the interaction between the FWA and CA. If unsecured Wi-Fi communications are determined to be readily accessible, meaning that they do not fall under the exceptions in subsection 2510(16), then these communications would not be protected. This exemption means that unsecured Wi-Fi communications can be intercepted lawfully per subsection 2511(2)(g)(i). Thus we move to subsection 605(a) of the CA to

106. *Id.*
107. S. REP. NO. 90-1097, at 107 (1968).
108. 18 U.S.C. § 2511 (2006).
109. S. REP. NO. 90-1097, at 108 (1968).
110. 660 F.2d 23 (1st Cir. 1982).
111. *Id.* at 27.
112. *Id.*

seek protection for such communications. However, as mentioned above, there have not been any applications of subsection 605(a) to Wi-Fi communications. Congress also seemed to have transferred regulation of interceptions to the FWA.[113]

If, however, unsecured Wi-Fi communications are not readily accessible, which means that they fall under an exception in subsection 2510(16), then such communications would be protected and subsection 605(a) of the CA need not apply.

While the FWA and CA, both individually and as read together, are unclear in how they protect Wi-Fi communications, it is worth looking to non-statutory expectations of privacy with regard to such communications.

A. User Expectations

Privacy is determined by the individual's intent to preserve his privacy, even in an area accessible by the public.[114] Users presumably have an expectation of privacy[115] with regard to their Internet communications regardless of whether they are operating on a secure[116] or unsecure network. This expectation stems from a lack of appreciation about the risks associated with operating on an unsecure network, which itself stems from not fully understanding the technology. The data transmitted over an unsecured Wi-Fi network can still be intercepted unless the data itself is encrypted.[117] Individuals are increasingly using Wi-Fi hotspots since many public spaces are being equipped with such systems. Users also "mooch" their neighbors' Wi-Fi when convenient.[118] Although an individual may

113. *See supra* Part II.B (discussing transferring regulation duties).

114. Katz v. United States, 389 U.S. 347, 351 (1967) (holding that even though a phone booth was normally a public place, the act of making a private call turned it into a private one).

115. To be clear, this paper is not suggesting a different interpretation of the FWA based on users' expectations because, after all, the statutory language is "readily accessible to the general public" and not "communications that the general public knows are readily available to the general public." *See In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888 (2012) (distinguishing accessibility of networks generally and the electronic communications sent over them).

116. Amongst expert radio scanners, encryption was a proxy for the transmitter's expectation of privacy. This expectation cannot necessarily be so clearly applied to other devices that have broadcast capability. *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary*, 99th Cong., 1st & 2d Sess. at 169-70.

117. *Configuring Network Data Encrypting*, CISCO, http://www.cisco.com/en/US/docs/ios/11_3/security/configuration/guide/scencryp.html#wp4667 (last visited Jan. 4, 2013).

118. A recent survey found that 32 percent of respondents admitted to using their neighbors' unsecured Wi-Fi networks. Byron Acohido, *Survey: 32% Admit Mooching*

consciously realize that he is operating on a *public* network, he still expects that there will be no interception of his *private* communications as discussed in Part II.A.2.

Users could theoretically choose to take extra security measures by only operating on secure Wi-Fi networks or using tools like those mentioned in Part I such as installing firewalls, using VPN, HTTPS, and SSL. Practically, however, implementation of such features may be too difficult for the average user to understand and effectively use. Since such settings are not generally the default enabled by the equipment manufacturers, users may have a false sense of security when operating on an open Wi-Fi network.[119]

The seemingly pervasive availability of public hotspots, whether free or commercial, adds to this false sense of security. Many free public hotspots leave their networks "open" and do not require users to authenticate before using their network.[120] Setting up a secure Wi-Fi network may be difficult and may hamper accessibility[121] by requiring credentials to log onto the network. Even if an authentication mechanism is enabled, the data transmitted between the wireless router and a users' device still might not be secure. Some Wi-Fi hotspots use software authentication applications that can implement the WEP (wired equivalent privacy) security scheme to encrypt individual users' data, but this has proven to be ineffective to protect against interception by users of the same Wi-Fi network.[122] Some commercial hotspot providers that require payment explicitly will advise their customers to use other encryption mechanisms.[123] Users tend to have a sense of security in using all these

Neighbor's Wi-Fi, USA TODAY,(Feb. 4, 2011,), http://usatoday30.usatoday.com/tech/news/2011-02-04-wifimoochers04_ST_N.htm (finding that 32 percent of survey respondents admitted to using their neighbors' unsecured Wi-Fi networks).

119. *See, e.g.*, Predreg Klasnja et al., *"When I Am on Wi-Fi, I am Fearless": Privacy Concerns & Practices in Everyday Wi-Fi Use*, in CHI '09 PROC. 27TH INT'L CONF. (2009), *available at* http://appanalysis.org/jjung/jaeyeon-pub/FormativeUserStudy4CHI.pdf (reporting the results of a study involving eleven participants and concluding that users from the general public "were largely unaware of . . . the visibility of unencrypted communications," which "led them to a false sense of security that reduced how much they thought about privacy and security while using Wi-Fi").

120. *See, e.g.*, Bradley, *supra* note 31 (discussing open networks).

121. Barnes & Noble, for example, seeks to make their stores feel like home by providing no-hassle Internet connection. *AT&T Wi-Fi in B&N Stores*, BARNES & NOBLE, http://www.barnesandnoble.com/u/Wi-fi-at-Barnes-and-Noble/379001240/ (last visited Jan. 4, 2013).

122. Adrian Hannah, *Packet Sniffing Basics*, LINUX JOURNAL (Nov. 14, 2011), http://www.linuxjournal.com/content/packet-sniffing-basics.

123. *See, e.g.*, *Frequently Asked Questions*, BOINGO WIRELESS, http://www.boingo.com/boingo-faq.php (last visited Jan. 4, 2012).

hotspot providers because so many other people continue to use (and sometimes pay) for this network access.

1. Looking at the History of Cordless Phone Conversations

Courts initially had refused to recognize an expectation of privacy in cordless phone conversations because there was no explicit reference to the monitoring of radio transmissions in the original enactment of the FWA.[124] In 1994, Congress amended the FWA to prohibit the interception of cordless phone communications.[125] How courts have treated expectations of privacy with respect to cordless phone conversations in the absence of explicit statutes could be helpful in determining what privacy users should expect with regard to unsecured Wi-Fi communications. Currently there is no explicit statute protecting such Wi-Fi communications, which leaves unclear the status of protecting such communications, much in the same way that cellphones were once treated.

Another reason why courts refused to recognize an expectation of privacy in cordless phone conversations as reasonable is because such conversations "could be intercepted easily with readily available technology, such as AM radio."[126] After cordless phone technology improved to make such interceptions more difficult, Congress amended the FWA to extend protection to cordless phone conversations that could no longer be analogized to AM/FM radio transmissions.[127] In the case of Wi-Fi communications, some intercepting mechanisms require a level of expertise, but others do not.[128] The movement to educate users about Wi-Fi communications could spur development on the other side of better interception technologies, which supports the case that such technology is not "in general public use" and that such users should receive protection.

B. Comparable Fourth Amendment Analysis

While the Fourth Amendment doctrine only applies to government

124. Price v. Turner, 260 F.3d 1144, 1148 (9th Cir. 2001) (quoting S. REP. NO. 99-541, at 12) (internal quotation marks omitted).

125. 18 U.S.C. § 2510(1), (12)(A) (2006).

126. *Price*, 260 F.3d at 1148 (quoting S. REP. NO. 99-541, at 12) (internal quotation marks omitted).

127. *Id.*

128. There are some tools that an average user could figure out, such as Firesheep, that allows anyone to effectively hack into various accounts. However, other "hacking" tools may require some expertise. *See, e.g.*, Jared Howe, *A Hacker's Toolkit*, PRIVATE WIFI, http://www.privatewifi.com/a-hacker%E2%80%99s-toolkit/ (last visited Jan. 4, 2013) (discussing complex hacking tools that require expertise).

searches and courts have found that it provides little privacy protection to technological information exposed to the public,[129] a brief analysis provides further context into what a reasonable expectation of privacy is. 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."[130] A two-prong test is used to determine if a piece of information merits Fourth Amendment protection.[131] The first prong requires that the individual have a subjective expectation of privacy, and the second prong requires that society is willing to recognize that expectation as reasonable, which is an objective criterion.[132]

Thus far, courts have only read a reasonable expectation of privacy that conforms to Fourth Amendment law for "oral communications" under the ECPA.[133] The statute defines "oral communication" as "any communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[134] The definition of "electronic communications" does not have any similar language suggesting an "expectation" of privacy, which seems to imply that Congress meant to afford less protection to electronic communications than oral communications.[135] However, the ECPA was enacted at a time when the Internet was in its infancy and not accessible to the general public.. A Fourth Amendment reasonable expectation of privacy analysis can still be conducted to provide a basis for users' expectations for their Wi-Fi communications.

The first prong for determining Fourth Amendment protection should be easily satisfied because users expect their Wi-Fi communications will be private, without even really considering if they are working on a secure or unsecure network. The second prong should be relatively easy to satisfy as

129. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (distinguishing between the content of electronic communications and non-content information); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005) (distinguishing public information from the content of electronic communications) .

130. U.S. CONST. amend. IV.

131. Katz v. United States, 389 U.S. 347, 361-62 (1967).

132. *Id.*

133. Kee v. City of Rowlett, 247 F.3d 206, 213–214 (5th Cir. 2001). The Supreme Court has declined to answer directly the question of if a reasonable expectation of privacy exists in electronic communications. Hector Gonzalez, James McGuire and Rebecca Kahan, *Do Privacy Rights in Electronic Communications Exist?* (N.Y. L.J.), Jan. 17, 2012, http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202538187981&Do_Privacy_Rights_in_Electronic_Communications_Exist&slreturn=20130305104853.

134. 18 U.S.C. § 2510(2) (2006).

135. 18 U.S.C. § 2510(12) (2006); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1582-84 (2004).

well, as society would expect that users would like to keep their email passwords, browsing history, etc. private. A "reasonable expectation of privacy" under the Fourth Amendment would prevent the police from intercepting such communications without a warrant. .

In *Kyllo v. United States*, the Supreme Court applied the "reasonable expectation of privacy" test to modern technology, ruling that the use of a thermal imaging device from a public vantage point to monitor the radiation of heat from a person's home was a "search" within the meaning of the Fourth Amendment.[136] Intercepting Wi-Fi communications from an unsecured network could be thought of as monitoring radio waves emanating from the home. In *Kyllo*, the Court held that to use "technology . . . not in general public use" to gain information that could not be obtained except by actually entering the home is a Fourth Amendment search.[137] In referring to technology that is not in "general public use," the Court was essentially applying the objective prong of the *Katz* test, where society recognizes this expectation of privacy as reasonable.[138] Whether this ruling is applicable to intercepting private Wi-Fi communications on an unsecured network depends in part on the state of the technology.

1. Password Protection

While courts have given less Fourth Amendment protection to wireless communications, they have determined that people have a reasonable expectation of privacy when they have enabled password protection. In *United States v. Heckenkemp*, the Ninth Circuit held that a student had a reasonable expectation of privacy in his computer's files despite having used the computer to hack into the university's email system because the files were password protected.[139] This expectation of privacy will not be upheld if a person shares the password with others. In *United States v. D'Andrea*, the defendant and her boyfriend allegedly sexually abused the defendant's eight-year-old daughter and posted pictures of the abuse on a password-protected site.[140] The United States District Court for the District of Massachusetts held that although password protection gives a reasonable expectation of privacy, sharing the password meant the defendant assumed the risk that the password would be shared.[141] In

136. 533 U.S. 26, 40 (2001).
137. *Id.* at 34.
138. *Id.* at 33.
139. 482 F.3d 1142, 1147 (9th Cir. 2007).
140. 497 F. Supp. 2d 117, 118 (D. Mass. 2007).
141. *Id.* at 123.

Casella v. Borders, the United States District Court for the Western District of Virginia found that the absence of a password was a reason to find that there was no expectation of privacy in the digital files on a phone.[142]

A distinguishing feature of unsecured Wi-Fi networks from the password protected files in the above-mentioned Fourth Amendment case law is that the system itself does not have a password, but the communications can still be subject to an expectation of privacy. Users do not necessarily have a reasonable expectation of privacy in their network in that people seemingly do not mind sharing a network with others, as demonstrated by the increased use of public hotspots. However, users seem to have an expectation that the communications on such a network would not be intercepted.[143]

IV. AMENDING THE FEDERAL WIRETAP ACT

The statutory interpretation of the FWA is too uncertain to determine reliably if unsecured Wi-Fi communications are protected.[144] Given that the FWA is the predominant law in protecting the privacy of electronic communications, the statute should be amended to expressly address concerns about Wi-Fi communications. The FWA was amended in 1986 to account for improved technology, at a time when wireless communications were far from the norm and individuals used dial-up modems to connect to the Internet. The FWA now is too unwieldy and unreliable as a law enforcement tool, and it is difficult for judges and investigators to apply.[145] While the Ninth Circuit took a step in its recent *Joffe* decision in ruling that "radio communication" should be given its ordinary meaning,[146] this still leaves the exact boundaries of protection for "electronic communications" unclear. Now is an appropriate time to revisit the FWA to account for the technological improvements of the last few decades. There have been hearings in both the House and the Senate,[147] and several new bills were

142. 649 F. Supp. 2d 435, 439 (W.D. Va. 2009).

143. *See supra* Part III.A (arguing that public network users expect privacy of private messages).

144. This paper will not analyze amending the CA, since the focus of conflicting statutory interpretation surrounds the FWA. Note that Congress transferred regulation of such communications to the FWA. *Supra* Part II.B.

145. Even in 1994, the Fifth Circuit was already calling the FWA "famous (if not infamous) for its lack of clarity . . . ." Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

146. Joffe v. Google, Inc., No. 11-17483, slip op. at 17 (9th Cir. Sept. 10, 2013).

147. *See Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 112th Cong. 130 (2011) (addressing new concerns of user privacy); *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on*

introduced in response to concerns raised by industry and privacy groups.[148]

Given that there is conflicting case law on how to categorize unsecured Wi-Fi communications, it is Congress's job to step in and clarify. Congress possesses a comparative advantage over the courts in crafting effective policy through its ability to legislate. This advantage is particularly acute in the area of new and emerging technology. Where Congress can create comprehensive and prospective policy regimes from scratch, the Supreme Court must address issues of privacy on a case-by-case basis, making the judicial system incapable of addressing privacy problems involving technological advancements until issues arise. Even then, the court is constrained by the specific facts of a case.[149] In trying to address new technology issues, the Supreme Court has made hasty, and sometimes improper, decisions, prompting Congress to react with legislation. For example, in *Olmstead v. United States*,[150] the Supreme Court initially held that an individual has no expectation of privacy in communications conducted over telephone wires under the Fourth Amendment. However, in 1934, Congress enacted the CA, which stated the contrary.[151]

Removing the uncertainties surrounding Wi-Fi communications protections in the statutory language allows for users to better protect themselves under clearly defined regulations. Such clarity also allows for Wi-Fi technology to continue developing,[152] especially in an economy where users are becoming more and more dependent on exchanges of information.[153] One of the issues that Congress needs to address is whether unsecured Wi-Fi communications are "readily accessible to the general public," that is, do such communications fall under the exceptions of subsection 2510(16), thereby entitling them to protection under the FWA. *In re Innovatio* suggests that "readily accessible to the general public" is an

the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 81, 85, 93-94 (2010) (statement of Stephen Wm. Smith, United States Magistrate Judge) (discussing privacy concerns of user data); *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 29 (2010) (statement of Albert Gidari, Partner, Perkins Coie LLP) (discussing user privacy concerns of user data).

148. *See* S. 1212, 112th Cong. (2011) (discussing privacy of geolocation data); H.R. 2168, 112th Cong. (2011) (geolocation data privacy); S. 1011, 112th Cong. (2011) (discussing privacy of electronic communications).

149. *See* Greely, *supra* note 44 (discussing how the Supreme Court addresses new technology problems on a case-by-case basis).

150. 277 U.S. 438 (1928).

151. 47 U.S.C. § 151-609 (2006).

152. *See, e.g.*, *supra* notes 29 and 30 (differentiating WEP from WPA and discussing new technology).

153. HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 15 (rev. ed. 2006).

issue of cost,practicality, and availability in whether an average user could simply buy a device to intercept communications. Congress could strengthen the intent element by requiring a user to have affirmatively configured his or her device to allow members of the public to monitor the communications in order to meet the "readily accessible to the general public" exception.[154] Note that the FWA already has a strong "intent" requirement in another area, preventing any accidental interceptions from resulting in liability.[155] Another issue that Congress needs to resolve is whether "readily accessible to the general public" applies to electronic *communications* (the data transmitted, email passwords, browsing history, etc.) or to the electronic *system* (having a secure or unsecure Wi-Fi network).

Educating users may be the long-term solution in protecting data privacy over Wi-Fi networks, since many of Congress's actions may again become outdated. As mentioned above, there seems to have been an increase in the promotion of network education with many articles available on the Internet explaining the step-by-step processes of setting up various security mechanisms. Such "education" has not definitively decreased instances of interception. Even after users have been educated, more sophisticated intercepting or hacking technology may be developed. Legislation to clearly protect all Wi-Fi communications decreases the gap between users' hypothetical ability to protect themselves and practical realities of doing so.

While new regulations and definitions are needed, it is important not to overregulate. Interception of unsecured Wi-Fi communications should not necessarily be completely illegal. System administrators should be able to regulate their own networks to detect any hacking attempts or inappropriate traffic on their networks. Such administrative activities should be allowed by having clear carve-out exemptions from liability. The FWA already contains two important exceptions and a carve-out. First, consent immediately removes a subject from the statute's protections.[156] A second exception allows communications service providers "to intercept, disclose, or use . . ." the communication in question "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . ."[157]

154. *See generally* Part II.A.2 (discussing configuration requirement for exemption of FWA protection).

155. *See* 18 U.S.C. § 2511 (2006) (stating guidelines for default open network configurations).

156. 18 U.S.C. § 2511(2)(c) (2006).

157. 18 U.S.C. § 2511(2)(a)(i) (2006).

An additional carve-out limits the reach of the statute. In the case of criminal activity, a service provider is authorized to provide intercepted communications to the appropriate authorities.[158]

Extending protections to unsecured Wi-Fi communications could arguably expand the reach of federal power if the stance is taken that the current act does not cover such communications, where users could instead protect themselves by enabling the security features on their own Wi-Fi networks or avoiding using unsecured public Wi-Fi networks. Presumably, the general public did not realize that interceptions of the magnitude by those like Google were possible. Furthermore, legal protections can bridge the gap in protecting users' privacy until limitations in technology and consumer awareness can be overcome.

In amending the FWA, a sunset provision could be included to alleviate concerns about federal overreach and account for progressing technology that could render a present amendment to later become obsolete. Congress could require the FCC or a similarly technically competent body to submit periodic reports on the status of Wi-Fi technology and the evolving need for privacy protections.

CONCLUSION

That two courts would have opposite rulings on what "readily accessible to the general public" means and differing analysis to reach their respective results is evidence that Congress needs amend and clarify the protections afforded to unsecured Wi-Fi communications. The current electronic privacy laws, including the CA, provide for an unclear roadmap in how to analyze such possible protections.

As our society becomes increasingly dependent on using Wi-Fi communications for various aspects of our lives, there is a parallel expectation of privacy. The fact that users do not fully understand Wi-Fi technology and the shortcomings of current security mechanisms is not a justification to violate their privacy, but instead is a call to Congress to amend the FWA to reflect their reasonable expectations. Clear statutory protections will allow for the continued progression of Wi-Fi technology. Society's dependency on Wi-Fi networks and public hotspots both economically and personally requires expansion of the FWA to ensure national uniformity. Leaving these decisions to judicial discretion has created and will continue to create disparity in the law on a case-by-case basis.

158. 18 U.S.C. § 2511(3)(b)(iv) (2006).