Michigan Law Review

Volume 111 | Issue 1

2012

Limits of the Federal Wiretap Act's Ability to Protect against Wi-Fi Sniffing

Mani Potnuru
University of Michigan Law School

NOTE

LIMITS OF THE FEDERAL WIRETAP ACT'S ABILITY TO PROTECT AGAINST WI-FI SNIFFING

*Mani Potnuru**

Adoption of Wi-Fi wireless technology continues to see explosive growth. However, many users still operate their home Wi-Fi networks in unsecured mode or use publicly available unsecured Wi-Fi networks, thus exposing their communications to the dangers of "packet sniffing," a technique used for eavesdropping on a network. Some have argued that communications over unsecured Wi-Fi networks are "readily accessible to the general public" and that such communications are therefore excluded from the broad protections of the Federal Wiretap Act against intentional interception of electronic communications.

This Note examines the Federal Wiretap Act and argues that the current Act's treatment of Wi-Fi sniffing might protect unsecured Wi-Fi communications under some circumstances, but that any such protections are incidental, unsystematic, and uncertain. This Note further argues that the current statute's "readily accessible to the general public" language should be interpreted in a way that addresses concerns about Wi-Fi sniffing and users' expectations of privacy. Users' current expectations stem from their limited understanding of the underlying Wi-Fi technology and the accompanying security risks and, more importantly, from the fact that private communications cannot be intercepted without specialized tools and knowledge not readily available to the general public. Finally, this Note advocates for amending the Federal Wiretap Act to remove uncertainty regarding protections against Wi-Fi sniffing. Clear protections against Wi-Fi sniffing would avoid the private and social cost of data theft resulting from sniffing and could close the gap between users' theoretical ability to protect themselves by using security mechanisms and their reduced practical ability to take any such protective measures.

TABLE OF CONTENTS

---

* J.D., May 2012, University of Michigan Law School. I would like to thank Kevin Bankston for introducing me to this topic during my internship at the Electronic Frontier Foundation. I also would like to thank my Notes Editors Matthew Miller, Emily Huang, and Adam Teitelbaum, and the *Michigan Law Review*'s Notes office for their excellent substantive and editorial advice. I am also very grateful to Professors Sonja B. Starr, Nina A. Mendelson, and Margaret Jane Radin for their extremely helpful feedback on earlier drafts.

INTRODUCTION

When Google Street View[1] first became publicly available, people were fascinated by the ability to zoom into a particular location and see real pictures of homes or businesses from the comfort of their homes. To offer these features, Google deployed a fleet of cars equipped with a global positioning system ("GPS"), high-resolution 360-degree cameras, and radio scanners to roam neighborhoods and photograph the publicly visible environs. Most were unaware that, while scouring neighborhoods, Google's cars were also scanning the airwaves for active Wi-Fi[2] networks.[3]

In May 2010, Google admitted that since initiating its Street View program in 2007, it had collected upwards of 600 gigabytes of payload[4] data—including private information like emails, voice communications, passwords, and financial and medical records—from "open" (i.e., unsecured)

1. Google Street View, a technology featured in the Google Maps application, provides panoramic views of places from various street positions around the world. *See Street View for Google Maps*, GOOGLE MAPS, http://maps.google.com/help/maps/streetview/ (last visited Feb. 20, 2012).

2. "Wi-Fi" is a shorthand term for "Wireless Fidelity" and is the current industry standard for most wireless data networks. *See infra* Part I.

3. Google's cars mapped the available Wi-Fi networks in cities across the country to help mobile devices determine their location. *See Location Source and Accuracy*, GOOGLE, http://support.google.com/gmm/bin/answer.py?hl=en&answer=81873 (last visited Feb. 20, 2012). Google is certainly not the only company using cars equipped with radio scanners to create a Wi-Fi network database; companies such as Skyhook use similar techniques. *See Coverage Area*, SKYHOOK, http://www.skyhookwireless.com/location-technology/coverage.php (last visited Feb. 12, 2012).

4. Data packets transmitted over a Wi-Fi network include both "payload," which contains a user's private information, and information that identifies the source and destination of the payload. *See Payload*, TECHTERMS.COM, http://www.techterms.com/definition/payload (last visited Feb. 12, 2012). This Note focuses on protecting users' privacy interest in payload data, instead of addressing information contained in data packets. *See infra* note 110.

wireless networks.[5] This admission raised serious concerns about privacy and potential Federal Wiretap Act[6] violations. Google used "packet sniffing," a technology used to eavesdrop on a network by intercepting and decoding network communications[7] and to collect users' private data transmitted over unsecured networks.[8] Google claimed that any use of technology capturing payload data from unsecured wireless networks was accidental,[9] and it firmly denied using any of the private data it had captured.[10]

The Google incident demonstrates the rising privacy risks to users' private Wi-Fi communications posed by "sniffing." As open Wi-Fi network usage becomes even more popular, the threat to consumers' private data continues to rise.[11] There has been an explosive growth in the adoption of wireless data networking technology, allowing users to connect to the internet wirelessly in private homes, offices, and public places. To meet the increased demand for wireless connectivity, more wireless access points, known as "hotspots," are becoming readily available in public places like airports, restaurants, and parks—and even on buses, trains, airplanes, and freeway rest stops.[12] Intentionally or unintentionally, many individuals and

---

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

6. 18 U.S.C. §§ 2510–2522 (2006).

7. Prabhaker Mateti, *Hacking Techniques in Wireless Networks*, *in* THE HANDBOOK OF INFORMATION SECURITY 85–87 (Hossein Bidgoli ed., 2005), *available at* http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.doc.

8. *See* Eustace, *supra* note 5.

9. There are two kinds of scanning techniques that can be used to discover Wi-Fi Access Points. In the "passive" scanning technique, the radio antenna listens for any and all wireless signals and records any data transmitted, including payload data. But most passive scanners are set specifically *not* to record payload data. To avoid any possibility of collecting payload data, other wireless mapping companies, such as Skyhook, use "active" scanning—for example, Skyhook's scanning equipment sends out a probe signal to determine whether any Wi-Fi access points are in range. Access points recognize that signal and return their own message with basic network identification information that basically says "Here I am, here is how to find me." This is also how a typical computer or phone finds an available Wi-Fi network. Google has admitted to using the "passive" scanning technique instead of the "active" scanning method. According to Google, it inadvertently failed to configure the wireless scanning software to discard payload data. *See* Tom Krazit, *Deciphering Google's Wi-Fi Headache (FAQ)*, CNET NEWS (June 1, 2010, 4:00 AM), http://news.cnet.com/8301-30684_3-20006342-265.html.

10. Eustace, *supra* note 5.

11. *See* Press Release, *Make Security a Priority in 2011: Protect Your Personal Data on Wi-Fi® Networks*, WI-FI ALLIANCE (Feb. 2, 2011), http://www.wi-fi.org/news_articles.php?f=media_news&news_id=1039 ("With an estimated 201 million households using Wi-Fi networks[] and as many as 750,000 Wi-Fi hotspots available worldwide, more personal data is being carried by these networks, making Wi-Fi security paramount in importance.").

12. *See AmtrakConnect Wi-Fi®*, AMTRAK, http://www.amtrak.com/servlet/ContentServer/AM_Content_C/1246044325520/1237405732514 (last visited Feb. 18, 2012); Danny King, *WiFi in the Sky: Airlines Bring More Internet Access on Board*, DAILYFINANCE (Aug. 28, 2010, 10:00 AM), http://www.dailyfinance.com/story/wifi-airplanes-airlines-internet/19611600; *Greyhound's New Low-Cost Buses, with Wi-Fi*, BUDGET TRAVEL (Mar. 4, 2008, 11:22 AM),

businesses operate their Wi-Fi networks as unsecured, open networks.[13] This allows hackers and other malicious actors to use packet-sniffing technology—the same technology Google used to build its Street View program—to access personal passwords, financial records, and other sensitive information, thereby facilitating crimes like identity theft. In addition to the violation of users' privacy, the social and economic costs of identity theft resulting from Wi-Fi sniffing are significant. For example, a recent study found that on average an identity theft victim loses approximately $5,000.[14] Moreover, the Congressional Research Service has found that identity theft "is the fastest growing type of fraud,"[15] while the Federal Trade Commission estimates that identity theft costs consumers approximately $50 billion annually.[16]

Google's extensive collection of users' private data is one of the more high-profile incidents of Wi-Fi sniffing. In response, several consumers across the country filed class action lawsuits, alleging that Google had violated the Federal Wiretap Act, the principal law protecting electronic communications from unauthorized interception.[17] Google has responded to these actions by arguing that unsecured Wi-Fi communications are excluded from the Act's broad protections against intentional interception because communications over unsecured networks are "readily accessible to the general public" and therefore fall within an exception to the Act's protections.[18]

This Note contends that at least some Wi-Fi communications may be protected by the Federal Wiretap Act so that intercepting those communications would violate the Act. Part I briefly introduces Wi-Fi technology, the types and functions of various Wi-Fi deployments, and the security issues involved in the varying network setups. Part II then argues that the Act's current treatment of Wi-Fi sniffing may protect unsecured Wi-Fi communi-

---

http://blog.budgettravel.com/budgettravel/2008/03/greyhounds_new_lowcost_buses_w.html; Aaron Reed, *Wi-Fi on the Highway: Rest Stops Go High-Tech*, ROADTRIP AMERICA (Jan. 18, 2008), http://www.roadtripamerica.com/dashboarding/Wi-Fi-On-The-Highway.htm.

13. *See, e.g.*, John E. Dunn, *A Quarter of WiFi Networks Unsecured, Finds Survey*, TECHWORLD (Oct. 14, 2010, 1:03 PM), http://news.techworld.com/security/3244175/a-quarter-of-wifi-networks-unsecured-finds-survey.

14. Jolie O'Dell, *How Much Does Identity Theft Cost?*, MASHABLE (Jan. 29, 2011), http://mashable.com/2011/01/29/identity-theft-infographic.

15. KRISTIN M. FINKLEA, CONG. RESEARCH SERV., R40599, IDENTITY THEFT: TRENDS AND ISSUES 1 (2010), *available at* http://www.fas.org/sgp/crs/misc/R40599.pdf.

16. *Id.*

17. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 733 F. Supp. 2d 1381 (J.P.M.L. 2010) (consolidating eight class action lawsuits in the Northern District of California); Complaint, Myhre v. Google, Inc., No. 10CV01444 (W.D. Wash. Sept. 9, 2010).

18. *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1073 (N.D. Cal. 2011); *see also* Letter from Pablo Chavez, Dir. of Pub. Policy, Google Inc., to Henry A. Waxman et al., Chairman, House Energy & Commerce Comm. 1, 5 (June 9, 2010) [hereinafter Google's Response], *available at* http://republicans.energycommerce.house.gov/Media/file/News/060910_Google-Response.pdf (claiming that Google "believe[s] [that] it does not violate U.S. law to collect payload data from networks that are configured to be openly accessible (*i.e.*, not secured by encryption and thus accessible by any user's device)").

cations under some circumstances, but that any such protections are incidental, unsystematic, and uncertain. Next, Part III argues that the current statute's "readily accessible to the general public" language, which allows the interception of electronic communications on systems configured in a way that makes those communications readily available to the general public, should be interpreted in a manner that addresses concerns about Wi-Fi sniffing and users' expectations of privacy. Part III also contends that these expectations stem from users' limited understanding of the underlying Wi-Fi technology and the accompanying security risks, and, more importantly, from the fact that private unsecured Wi-Fi communications cannot be intercepted without specialized tools and knowledge not readily available to the general public. Finally, Part IV advocates amending the Federal Wiretap Act to make Wi-Fi sniffing clearly prohibited under the statutory language. Clear and uniform protections against Wi-Fi sniffing can address the private and social costs of data theft resulting from Wi-Fi sniffing and provide reasonable safeguards for Wi-Fi users.

I. THE WI-FI TECHNOLOGY LANDSCAPE

Wi-Fi has come to mean any kind of wireless network that operates using the common standards, collectively referred to as 802.11 protocols, set by the Institute of Electrical and Electronics Engineers ("IEEE").[19] The basic network setup involves a Wireless Access Point ("WAP"), often referred to as a "wireless router," which is typically connected to the user's Internet Service Provider's ("ISP") network through a wired connection and communicates over radio frequencies with any device that is equipped with a Wi-Fi adapter, such as a laptop or a smartphone. One can think of the WAP as a small, short-range cell phone tower, and the Wi-Fi adapters in the users' devices as radio receivers.

Though the Federal Communications Commission ("FCC") regulates most radio communications in the United States, Wi-Fi networks operate in the unregulated frequency ranges known as Industrial, Scientific and Medial ("ISM") radio bands.[20] This part of the radio spectrum can be used by anyone, even persons without a license from the FCC. Devices such as microwaves, cordless phones, wireless garage door openers, wireless microphones, vehicle trackers, and amateur radios all operate in one of the ISM bands.[21] Wi-Fi networks use different frequency ranges of the ISM bands

19. IEEE COMPUTER SOCIETY, WIRELESS LAN MEDIUM ACCESS CONTROL (MAC) AND PHYSICAL LAYER (PHY) SPECIFICATIONS (2007) [hereinafter IEEE], *available at* http://standards.ieee.org/getieee802/download/802.11-2007.pdf.

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

21. *Id.* The 2.4 GHz band was initially used for devices such as microwave ovens that emit radio frequencies, but not for radio communications. In 1985, the FCC opened up the ISM bands for wireless and mobile communications. *See Definition of: ISM Band,*

depending on the particular protocol being used.[22] Each of the above ranges is further divided into channels, just as radio and TV broadcast bands are subdivided into channels, and each Wi-Fi network is configured to operate on one of these channels.[23]

Despite revolutionizing how people connect to the internet, Wi-Fi technology raises a host of security concerns. Wi-Fi equipment allows users to protect their network using a password, which enables users to restrict access to their network. Once Wi-Fi networks are password protected, any information transmitted over them is encrypted, making interception of transmitted private data highly difficult, if not impossible.[24] Notwithstanding the available security mechanisms, many Wi-Fi networks are not secured for various reasons.[25] First, the factory default settings for the Wi-Fi equipment typically are set to operate the network in open mode.[26] For example, many wireless modems provided by Comcast and other ISPs are set to operate in this unsecured mode by default.[27] Unless the Wi-Fi network owner affirmatively enables the security mechanisms, these Wi-Fi networks continue to operate in open mode. This status quo creates a bias towards unsecured networks and tends to impede users' ability to change default rules.[28] Consumers

---

PCMAG.COM ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia_term/0,2542,t=unlicensed+band&i=45467,00.asp (last visited June 22, 2011).

22. The 802.11b and 802.11g protocols operate in the 2400–2495 MHz frequency range, but the 802.11a protocol operates in the 5150–5825 MHz range. *See* WLAN Protocols, BLUE EAGLE TECHNOLOGIES, http://www.blue-eagle-technologies.com/protocols.html (last visited March 29, 2012).

23. For example, the 2.4000–2.495 GHz band of 802.11b/g protocols is divided into eleven legally allowed channels with channel 1 centered on 2.412 GHz and channel 11 on 2.462 GHz. *See 802.11b WiFi Frequency Channels*, MOONBLINK, http://www.moonblinkwifi.com/2point4freq.cfm (last visited June 22, 2011). Though the channels overlap, adjacent networks using different channels can operate without interference if the particular networks are operating on different nonoverlapping channels, such as channels 1, 6, and 11. *Id.*

24. A network administrator could also configure the wireless routers to not broadcast the service set identifier ("SSID") for improved security and thus let in only users who already know the network name, thereby preventing access to the network by unauthorized users. *See Wi-Fi (802.11) Security*, GETNETWISE, http://security.getnetwise.org/tips/wifi (last visited June 22, 2011). For improved security, the wireless router could also be configured to allow access to the network to only certain computer Media Access Control ("MAC") addresses. *Id.* But simply not broadcasting the SSID or limiting access to a certain set of MAC addresses, without turning on encryption protocols such as Wi-Fi Protected Access ("WPA"), does not prevent interception of data by more sophisticated interceptors. *See id.*

25. *See* Matt Hines, *Worried About Wi-Fi Security?*, CNET NEWS (Jan. 19, 2005, 4:00 AM), http://news.cnet.com/Worried-about-Wi-Fi-security/2100-7347_3-5540969.html (predicting that some 80 percent of U.S. residential wireless local area networks, or WLANs, would be "unsecured" by 2007); *see also infra* notes 78–80 and accompanying text.

26. *See infra* note 68 and accompanying text.

27. *See Comcast-Supported Routers, Gateways, and Adapters*, COMCAST CUSTOMER CENTRAL, http://customer.comcast.com/help-and-support/internet/comcast-supported-routers-gateways-adapters/ (last visited March 29, 2012).

28. *See generally* Russell Korobkin, *Inertia and Preference in Contract Negotiation: The Psychological Power of Default Rules and Form Terms*, 51 VAND. L. REV. 1583 (1998)

also might not enable the security features due to technological intimidation or because of the cumbersome process.[29] Moreover, they might lack awareness of the risks involved in operating an unsecured network.[30] Or they simply might not be concerned about the threats unsecured networks pose,[31] perhaps because they choose to share internet access with others and thus leave the network open. Current technology does not easily provide a secure shared Wi-Fi network to a large section of the general public. This limitation forces public libraries, cafes, airports, and other hotspots to operate networks in unsecured mode.[32]

II. THE FEDERAL WIRETAP ACT

The Federal Wiretap Act's treatment of unsecured Wi-Fi communications is unsystematic and might only protect some private Wi-Fi communications. The Act might afford some protection to unsecured Wi-Fi communications under certain Wi-Fi network configurations, but any such protection is purely incidental, because the statutory language is not specifically aimed at these types of communications. Further, the Act's ill-defined "readily accessible to the general public" exception leaves the protection of unsecured private Wi-Fi communication uncertain.

The Wiretap Act prohibits intentionally[33] intercepting or disclosing wire, oral, or electronic communications.[34] Initially, as enacted in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Wiretap Act protected only wire and oral communications from unauthorized interception.[35] Congress amended the Wiretap Act in 1986 to prohibit the interception of "electronic" as well as oral and wire communications. The Act

---

(discussing the ramifications of the status quo bias in contract negotiation and the motivational basis for the preference of inaction); William Samuelson & Richard Zeckhauser, *Status Quo Bias in Decision Making*, 1 J. RISK & UNCERTAINTY 7 (1988) (asserting the existence of a substantial status quo bias in many important real decisions).

29. *See infra* Section III.A.

30. *See infra* note 78 and accompanying text.

31. Matthew Bierlein, Note, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 OHIO ST. L.J. 1123, 1131 (2006).

32. *See also infra* notes 90–91 and accompanying text. For example, T-Mobile, which operates one of the biggest nationwide networks of hotspots, acknowledges this limitation: "WEP is based on 'shared secret' encryption. Shared secret encryption means that the 'secret' (the key to the encryption) must be shared with all other WLAN users. Consequently, we believe that this type of security solution is neither practical nor meaningful when used on a public network." *T-Mobile HotSpot Security Statement*, T-MOBILE HOTSPOT, https://selfcare.hotspot.t-mobile.com/security.htm (last visited June 22, 2011).

33. The Wiretap Act only prohibits intentional interception of electronic communications. 18 U.S.C. § 2511(1)(a) (2006). Investigation of the "intentionality" requirement of the Act is beyond the scope of this Note. Instead, this Note assumes that Google acted intentionally and focuses on whether data transmitted over unsecured wireless networks even qualify for the Wiretap Act's protections against interception. Google claims that it does not, an argument that has implications far beyond Google's present litigation.

34. 18 U.S.C. §§ 2510–2522.

35. *See* S. REP. NO. 90-1097 (1968).

specifically protects radio communications.[36] In addition to authorizing and regulating electronic surveillance for law enforcement purposes, the Act regulates private conduct. The amended, post-1986 Wiretap Act imposes civil liability and criminal penalties[37] on anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[38] The Act defines "electronic communication" to include "any transfer of signs, 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."[39] Since data is transmitted over a Wi-Fi network using radio signals, private data—including emails, passwords, financial or medical records, as well as other web traffic—qualifies as electronic communication within the meaning of the Act.

The Wiretap Act provides a set of exceptions to its broad prohibitions on the interception of electronic communications.[40] Google relies on the "readily accessible to the general public" exception, arguing that unsecured Wi-Fi communications fall under this exception and that, as a result, its Street View program did not violate the Act.[41] The "readily accessible to the general public" exception provides that 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 communication is *readily accessible to the general public*."[42] The terms "readily accessible to the general public" and "configured" are the two key terms to understanding the reach of this exception. This Part analyzes these two prongs of the exception and argues that not all unsecured Wi-Fi communications are excluded from the Act's protections.

---

36. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(a)(6)(C), 100 Stat. 1848, 1849.

37. 18 U.S.C. §§ 2520–22 (authorizing any person to recover damages and to seek an injunction against illegal interception); *id.* § 2511(4)(a) ("[W]hoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.").

38. 18 U.S.C. § 2511(1)(a).

39. 18 U.S.C. § 2510(12).

40. Most of these exceptions do not apply to intentional sniffing of Wi-Fi networks. One of these exceptions is the 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). Similarly, 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 law," such interceptions are excluded from the prohibition. 18 U.S.C. § 2511(2)(c).

41. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067 (N.D. Cal. 2011) (denying Google's motion to dismiss); Google's Response, *supra* note 18.

42. 18 U.S.C. § 2511(2)(g)(i) (emphasis added).

A. *"Readily Accessible to the General Public" Exception*

Subsection 2510(16) of the Act defines "readily accessible to the general public" with respect to "a radio communication" as any communication that is *not*:

> (A) scrambled or encrypted;
>
> (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention 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.[43]

The legislative history makes clear that "[r]adio 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 . . . subsection 2510(16) are afforded privacy protections under [the Act] unless another exception applies."[44] Section II.A.1 below analyzes the applicability of subsection 2510(16) to Wi-Fi communications. Assuming that subsection 2510(16) applies to Wi-Fi communications, Section II.A.2 argues that not only are secure Wi-Fi communications clearly protected under subsection 2510(16)(A) but some unsecured Wi-Fi communications may also be protected under subsection 2510(16)(E).

1. Applying Subsection 2510(16) to Wi-Fi Communications Generally

The statutory definition of "readily accessible to the general public" in subsection 2510(16) applies only to radio communications. However, it is not clear whether this definition applies to communications over Wi-Fi networks, despite the fact that Wi-Fi networks use radio waves to transmit data. This Section explores the arguments for and against applying subsection 2510(16) to Wi-Fi communications.

The District Court for the Northern District of California in *In re Google Inc. Street View Electronic Communications Litigation* has thus far refused

---

43. 18 U.S.C. § 2510(16).

44. S. REP. No. 99-541, at 14–15 (1986).

to apply subsection 2510(16)'s definition to Wi-Fi communications.[45] The court ruled that the statutory definition specifically applies to a "radio communication" and construed the term "radio communication" narrowly to include only "traditional radio services," such as "public-directed radio broadcast communication."[46] Since the term "radio communication" was not defined in the Act (as compared to "electronic communication," which is defined), the court relied on legislative history indicating that Congress added the definition in subsection 2510(16) to alleviate radio hobbyists' concerns and thus only to clarify that "intercepting traditional radio services is not unlawful."[47] The court also reasoned that the five exceptions within subsection 2510(16) "are drafted for the particular technology of traditional radio broadcast mediums and do not address any broader radio-based communications technology."[48] To summarize, the court ruled that even though Wi-Fi networks 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 exception to liability for intercepting *all* electronic communications.[49]

The *In re Google* court's ruling that subsection 2510(16)'s definition of "readily accessible to the general public" does not apply to Wi-Fi communications is not conclusive.[50] Communications transmitted by radio, as in the case of Wi-Fi networks, are a specific type of electronic communication, as the statutory definition of electronic communication indicates.[51] Hence, "electronic communications" and "radio communications" are not mutually exclusive. In short, the court's ruling leads to the technologically counterintuitive result that Wi-Fi communications are not "radio communications." Further, a plain reading of the subsection's language ("with respect to a radio communication") does not indicate that the statutory definition should only apply to one very specific type of radio communication (i.e., "traditional radio broadcasts").[52] Section 2510's opening language ("As used in this chapter") makes it clear that subsection 2510(16)'s definition of "readily accessible to

45. *In re* Google St. View, 794 F. Supp. 2d 1067 (denying Google's motion to dismiss).

46. *Id.* at 1080.

47. *Id.* at 1079 (quoting 132 CONG. REC. 14,601 (1986)) (internal quotation marks omitted).

48. *Id.* at 1080.

49. *Id.* at 1081.

50. Google moved for an interlocutory appeal, and the district court granted the motion for certification. Further, this is just one district court's conclusion; other courts might come to a different conclusion.

51. 18 U.S.C. § 2510(12) (2006) (defining electronic communication as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, *radio* . . ." (emphasis added)).

52. *See* Supplemental Brief for Defendant at 2, *In re Google St. View*, 794 F. Supp. 2d 1067.

the general public" should apply wherever the term appears, unless the definition was explicitly confined to specific subsections.[53]

If subsection 2510(16)'s definition of "readily accessible to the general public" *does* apply to Wi-Fi communications, it is not conclusive that only secured Wi-Fi communications would be unprotected. Under subsection 2510(16), if a Wi-Fi network is secured with any security protocol, communications over that network would be "scrambled or encrypted" and the "readily accessible to general public" exception to the Wiretap Act's protections would not apply to Wi-Fi communications made over that network.[54] However, this still leaves protections afforded to unsecured Wi-Fi communications unclear.

Conversely, if the definition in subsection 2510(16) *does not* apply, the term "readily accessible to the general public" would be left without any statutory definition with respect to electronic communications not related to "traditional radio services," including Wi-Fi communications.[55] If this is the case, courts would have to consider more general arguments about whether unsecured Wi-Fi communications are "readily accessible to the general public" within the meaning of the statute.[56]

Although the issue of applicability of subsection 2510(16) to Wi-Fi communications remains unsettled, for the sake of completeness, the next Section of this Note reviews the applicability of one particularly relevant category of the "readily accessible to the general public" definition in subsection 2510(16).[57] Section II.A.2 argues that while some unsecured Wi-Fi communications might fall under the "readily accessible to the general public" exception, not all unsecured Wi-Fi communications may be excluded from the Wiretap Act's protections.

---

53. 18 U.S.C. § 2510. For example, in the same section of the statute the term "foreign intelligence information" is defined in subsection 2510(19), but it is explicitly confined to a specific portion of the statute. *See* 18 U.S.C. § 2510(19) (confining subsection 2510(10)'s definition of "foreign intelligence information" to subsection 2517(6) of Title 18).

54. 18 U.S.C. § 2510 (16)(A).

55. But, as discussed *infra* Section II.A.2, application of the current subsection 2510(16) definition to Wi-Fi communications might lead to odd results. However, unfettering the protections from the statutory language is not necessarily preferable.

56. At the motion to dismiss stage, the *In re Google* court has only ruled that subsection 2510(16)'s narrow definition of "readily accessible to the general public" does not apply to Wi-Fi communications. *In re Google St. View*, 794 F. Supp. 2d at 1082. The court did not make any ruling on whether unsecured Wi-Fi communications fall under subsection 2511(2)(g)(i)'s "configured so that such electronic communication is readily accessible to the general public" exception. *Id.* at 1082–83. For how courts might interpret "readily accessible to the general public" language in the context of unsecured Wi-Fi communications, see *infra* Part III.

57. Section 2510(16)(B) ("communication[s] . . . transmitted using modulation techniques whose essential parameters have been withheld from the public"), section 2510(16)(C) ("communication[s] . . . carried on a subcarrier or other signal subsidiary to a radio transmission"), and section 2510(16)(D)("communication[s] . . . transmitted over a communication system provided by a common carrier") do not appear to be particularly relevant to Wi-Fi communications. *See* 18 U.S.C. §§ 2510(16)(B)–(D).

2. Applying Subsection 2510(16) to Unsecured Wi-Fi Communications

An alternative source of protection for secured and especially unsecured wireless communications is subsection 2510(16)(E). The plain reading of subsection 2510(16)(E) indicates that at least some communications over certain Wi-Fi radio frequencies are not excluded from the Act's protections under the "readily accessible to the general public" exception. Subsection 2510(16)(E) specifies that radio communications transmitted on 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 definition of "readily accessible to the general public."[58] The Senate Report clarifies the purpose behind this provision: "These communications include satellite communications, auxiliary broadcast services and private microwave services, each of which routinely carries private business or personal communications."[59]

The frequencies allocated under parts of FCC rules, specified in subsection 2510(16)(E), partly overlap with the Wi-Fi operating frequencies, and thus communications over these Wi-Fi networks might be covered within this exception to the "readily accessible to the general public" definition. As discussed in Part I, Wi-Fi networks divide their operating frequency bands into channels.[60] Since only certain parts of the frequency range of the 802.11b protocol are allocated under the FCC rules, only communications over channel 11 and parts of channels 7, 8, 9, and 10 of 802.11b protocol are covered for privacy protections by subsection 2510(16)(E).[61] Channel 11 is the only commonly used 802.11b protocol channel that might be fully protected under subsection 2510(16)(E).[62] 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" so that interception of such communications could still violate the Act. 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 Act.[63]

One criticism of this statutory interpretation is that Congress might never have intended to protect unsecured Wi-Fi communications. Although the frequencies listed under subsection 2510(16)(E) do correspond to frequencies used in Wi-Fi transmissions, on the one hand, they are mostly discussed

---

58. 18 U.S.C. § 2510(16)(E).

59. S. REP. No. 99-541, at 15 (1986).

60. *See supra* notes 22–23 and accompanying text.

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

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

63. 802.11a, which operates in the 5170–5815 MHz frequency range, uses twelve official channels. Since only the 5091–5250 MHz frequency range is allocated by the FCC under part 25 of its rules, only communications over the channels 36, 40, 44, and 48 of the 802.11a networks are covered by subsection 2510(16)(E). *See* 47 C.F.R. § 25.202 (2010).

in the context of radio broadcasting technology.[64] On the other hand, the legislative history does not indicate that Congress intended to completely exclude unencrypted wireless communications from the Act's protections. In fact, the Senate Report accompanying subsection 2510(16)(E), which restores the Act's protections to certain radio communications, seems to indicate that the Senate's main concern was protecting "private business or personal communications," even when such communications are not encrypted.[65]

Further, in practical terms, the privacy protections afforded by subsection 2510(16)(E) are limited because the statutory language does not cover all Wi-Fi frequencies. This leaves liability for intercepting users' private data communicated over unsecured Wi-Fi networks contingent on the exact channel that the particular Wi-Fi network was operating at the time of interception. At best, under this statutory construction, ordinary consumers' protection from interception turns not only on reading the "with respect to a radio communication" language of subsection 2510(16) to apply to Wi-Fi communications, but also on what frequency or channel the user's Wi-Fi equipment was using when transmitting the private data—a fact that users are surely unaware of in the vast majority of cases. From a policy perspective, this result is completely arbitrary. This kind of piecemeal protection is practically useless for users. As discussed later in Part IV, the statute should ultimately be amended to remove the uncertainty of protections against Wi-Fi sniffing.[66]

B. *The Configuration Issue*

Even if unsecured Wi-Fi communications are indeed "readily accessible to the general public," the exclusion from the Wiretap Act's protection still does not apply unless the "configuration" requirement is also satisfied. Subsection 2511(2)(g)(i) specifies 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."[67] But neither the Act nor the Senate Report clarifies whether the system needs to be configured by the user himself to fall under the "readily accessible to the general public" exception or whether a default configuration can deprive the user of privacy protection.

This is particularly relevant in the Wi-Fi context since many off-the-shelf Wi-Fi routers come with default factory settings geared to operate the network in open mode. Though manufacturers include instructions to set a password and secure the network in accompanying product manuals, the

64. *See* 47 C.F.R. §§ 24, 74 (2010); 47 C.F.R. § 94 (1995).

65. 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.").

66. *See infra* Part IV.

67. 18 U.S.C. § 2511(2)(g)(i) (2006) (emphasis added).

onus is on the user to activate the security mechanism of the Wi-Fi router.[68] If a user does not make these security adjustments, communications over such Wi-Fi networks will continue to be unsecured. One interpretation of subsection 2511(2)(g)(i) might provide that if the user never changed the default settings of the Wi-Fi router, communications over such a network might still be protected under the Act. But another interpretation might provide that if the network was configured by *someone* other than the user himself, such as the manufacturer, and if the security mechanisms were not enabled, communications over such a network would not be protected by the Act. Yet there is no statutory text explicitly requiring the network to be configured by the user himself in order for communications from the network to be "readily accessible to the general public."

The legislative history of the "configured" language[69] suggests that Congress intended to protect all electronic communications unless the user has knowingly chosen to make the communications available to the general public. The Senate Report explained that it is lawful to intercept "public communications" such as the closed-captioning data transmitted along with TV programming data.[70] Unlike the closed captioning of TV programming, it is not the intent of the home Wi-Fi owner to make his private Wi-Fi communications available "for the use of the general public." Similarly, when the general public uses an unsecured Wi-Fi network at the local Starbucks or the public library, even if the network itself is publicly accessible, users' private communications transmitted using that public network are not meant to be "public communications."

The Senate Report accompanying the 1986 amendments to the Act also noted that the term "configure[d] is intended to establish *an objective standard of design configuration* for determining whether a system receives privacy protection."[71] This language indicates that if the electronic communications system provides public communications by design, then communications transmitted through such a system are not protected under

---

68. For example, the very popular Belkin F5D7230 router ships to the user with security mechanisms turned off. BELKIN WIRELESS G ROUTER USER MANUAL 56 (2004), *available at* http://www.belkin.com/support/dl/p74559-a_f5d7230-4_man_6-04.pdf ("Your Router is equipped with WPA (Wireless Protected Access), the latest wireless security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy). *By default, wireless security is disabled.* To enable security, you must first determine which standard you want to use." (emphasis added)) (last updated Mar. 15, 2011); *see also Security*, WI-FI ALLIANCE, http://www.wi-fi.org/security (last visited Mar. 15, 2011) ("Most Wi-Fi equipment is shipped with security disabled to make it very easy to set up your network.").

69. 18 U.S.C. § 2511(2)(g)(i) ("[E]lectronic communication *made through* an electronic communication system that is *configured so that* such electronic communication is readily accessible to the general public." (emphasis added)).

70. S. REP. NO. 99-541, at 18 ("Under this provision, it would not be unlawful to intercept subcarrier and UBI communications that are transmitted *for the use of the general public.* Such *'public' communications* would include the stereo subcarrier used in FM broadcasting or data carried on the VBI to provide closed-captioning of TV programming for the hearing-impaired." (emphasis added)).

71. *Id.* (emphasis added).

the Act. However, a home Wi-Fi network is not designed to provide a public communications system. The purpose of such an electronic communications system is to enable various home electronic devices to connect to the internet. A few home Wi-Fi network operators may choose to enable their system for public access, but even in those circumstances the system is configured for public "access," not for the communications themselves to be public. Similarly, a public Wi-Fi hotspot at the local Starbucks is configured to enable public access to the Internet, but that does not mean that private communications transmitted using that network are intended for the general public's consumption.[72]

At least one district court has addressed the issue of "configuration" to some extent. In *United States v. Ahrndt*,[73] the defendant operated an unsecured Wi-Fi network at his home and had his iTunes program[74] configured to publicly share his video library, including a collection of child pornography. A police officer accessed the video files in the defendant's iTunes library by using the defendant's unsecured Wi-Fi network. The district court held that since "the wireless network and iTunes software were configured so that the general public could access them," the police officer's access of defendant's video files was lawful under the Wiretap Act.[75] The court noted that even though operating the open Wi-Fi network did not require any positive action by the defendant, since the default factory configuration of the wireless router was to operate in unsecured mode, sharing an iTunes library *did* require positive action by the defendant. The court decided that the act of sharing the iTunes library on an open Wi-Fi network made such communications "readily accessible to the general public" under subsection 2511(2)(g)(i).

In light of this holding, perhaps communications over open Wi-Fi networks might not be considered "readily accessible to the general public" if the user does not take some sort of affirmative action in configuring the wireless router to be open. But the decision to share a video library is distinguishable from the decision to use an unsecured Wi-Fi network. Factual circumstances of individual Wi-Fi routers will undoubtedly influence court rulings, and no court has conclusively held that the Wi-Fi network must be specifically configured to be open by the owner of the network to fall under the definition of "readily accessible to general public" under subsection 2511(2)(g)(i). A colorable argument could be made that if the network owner himself did not configure the wireless router to operate in unsecured mode, subsection 2511(2)(g)(i)'s exception should not apply.

---

72. *See supra* note 70 and accompanying text.

73. No. 08-468-KI, 2010 WL 373994 (D. Or. Jan. 28, 2010).

74. 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 May 23, 2012).

75. *Ahrndt*, 2010 WL 373994, at *8.

C. *Summary*

Though there is limited case law interpreting the "readily accessible to general public" exception to liability for intercepting Wi-Fi communications, some have concluded that this exception to the Act removes all unencrypted Wi-Fi networks from the Act's protection.[76] Google relied on this theory in trying to dismiss the class action suit against it. However, such a broad conclusion need not be drawn.

As discussed in Section II.A above, the purely textual statutory interpretation of "readily accessible to the general public" as defined in subsection 2510(16) could be read to provide protection to all secured and some unsecured Wi-Fi communications. Or, as the court in *In re Google* reasoned, the statutory definition of "readily accessible to the general public" could be read as not applying to Wi-Fi communications at all, leaving the meaning of that term completely undefined in that setting. In either case, a colorable argument, as laid out in Section II.B, can be made that unless the user himself configures the Wi-Fi network to operate in unsecured mode, subsection 2511(2)(g)(i)'s "readily accessible to the general public" exception does not apply to Wi-Fi communications over such unsecured networks. The legislative history of the "configured" requirement also indicates that unless electronic communications are intended to be public communications, such communications do not lose the Act's protections.

III. INTERPRETING "READILY ACCESSIBLE TO THE GENERAL PUBLIC"

Since the statutory definition of "readily accessible to the general public" in subsection 2510(16) might not apply—and even if it did apply, it might lead to bizarre results—courts might have to interpret the term "in accordance with its ordinary or natural meaning."[77] The concept, at a basic level, might mean that the user has put the information out into the public sphere in a way that should be understood as effectively relinquishing an expectation of privacy. But many users of unsecured Wi-Fi networks do not think of their private Wi-Fi communications as existing in the public sphere and do expect a level of privacy in the data that they transmit on these networks. This Part examines the reasons behind these expectations and argues that the term "readily accessible to the general public" should be interpreted in a way that conforms to the general public's expectations of privacy and addresses concerns about Wi-Fi sniffing.

---

76. *See, e.g.*, Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 138 (2004).

77. FDIC v. Meyer, 510 U.S. 471, 476 (1994).

A. *Wi-Fi Users' Expectations*

A large percentage of ordinary users seem to lack an appreciation for the risks associated with operating and using an unsecured Wi-Fi network.[78] Even if operators and users of unsecured wireless networks understand that unauthorized users might be able to gain access to their wireless network, they are typically unaware that data transmitted over such unsecured Wi-Fi networks can still be intercepted unless the data is somehow encrypted.[79] This mostly stems from the fact that most users of Wi-Fi networks do not understand how the technology works.[80] Wi-Fi networks transmit data over invisible radio waves, and since the transmitted data cannot be "sensed" through ordinary senses, ordinary users may believe that their data is private and secure even if it is not encrypted.

The distinction between users' expectations regarding accessing and using an unsecured Wi-Fi network and users' expectations that whatever private data they send on these networks is still private is crucial. Users do not shy away from "borrowing" others' unsecured Wi-Fi networks. For example, a recent survey found that as many as 32 percent of respondents admitted to using their neighbors' unsecured Wi-Fi networks.[81] In this case, users know that the Wi-Fi network they are using is unsecured and hence that others can access the same network. But at the same time, because of the limited understanding of the underlying technology and the concomitant security risks, users still expect that their own private communications over these unsecured Wi-Fi networks are themselves secure. Similarly, a user accessing the unsecured Wi-Fi network at her local Starbucks knows that others are accessing the same network but still expects that whatever private information she is sending to her bank over that Wi-Fi network remains private. The widespread "seemingly innocuous use of public Wi-Fi hot spots"[82] further tends to reaffirm the sense of privacy and security.

This distinction between the public accessibility of an unsecured Wi-Fi network and the privacy of communications transmitted over such a network is also clear from the language of the Wiretap Act's "readily accessible to the general public" exception. The exception exempts interception of an electronic communication if that communication was "made through an

---

78. For example, a student survey, based on door-to-door interviews in three different neighborhoods in Boca Raton, Florida, recently found that many residents were surprised to learn of the security risks and threats to their unsecured home Wi-Fi networks. *See* RAFAEL LACHOWSKI ET AL., UNSECURED RESIDENTIAL WIRELESS NETWORKS 18 (2009), *available at* http://itom.fau.edu/jgoo/sp09/ISM4220/mrk.pdf. The same survey also found a negative correlation between the average income of the community and the level of awareness of security risks, and a negative correlation between the average income of the community and the number of unsecured wireless networks. *Id.*

79. *Id.*

80. *See, e.g., id.*

81. Byron Acohido, *Survey: 32% Admit Mooching Neighbor's Wi-Fi*, USA TODAY, Feb. 4, 2011, www.usatoday.com/tech/news/2011-02-04-wifimoochers04_ST_N.htm.

82. *Id.*

electronic communication system that is configured so that *such electronic communication* is readily accessible to the general public."[83] To trigger the exemption, it should not simply be sufficient for the "electronic system" (i.e., the Wi-Fi network) to be accessible to the general public, which is true in the case of an unsecured Wi-Fi network since anyone can access the network without a password. Instead, the "electronic communication" itself (i.e., the user's private data being transmitted over the radio waves) should have to be easily accessible to the general public.

To be sure, users have some ability to protect themselves by only using secured Wi-Fi networks. They could secure their home Wi-Fi networks and refuse to use unsecured public Wi-Fi hotspots. Though implementing a secured network through the use of encryption can mitigate security risks from over-the-air sniffing, use of security technologies continues to be challenging for many ordinary users. Unfortunately, security features designed to protect users are not enabled by default by the equipment manufacturers, contrary to what users might expect.[84] This further adds to the false sense of privacy and security among the general public.[85]

Even if the users are aware of Wi-Fi security risks and available security mechanisms, ordinary home users find it difficult to enable these features.[86] In response to these difficulties, manufacturers have started offering various products that attempt to simplify security setup by changing design features on Wi-Fi routers.[87] In fact, the Wi-Fi Alliance—a body that promotes Wi-Fi technology and certifies products that conform to Wi-Fi industry standards—recognized consumer difficulty in enabling security features and, in response, developed a new mechanism called Wi-Fi Protected Setup

---

83. 18 U.S.C. § 2511(2)(g)(i) (2006) (emphasis added).

84. *See supra* note 68 and accompanying text. A few commentators have suggested creating civil liability against Wi-Fi router manufacturers for failure to provide necessary security (i.e., failing to enable the security mechanism by default) that later results in exploitation by hackers. *See, e.g.*, Michael L. Rustad & Thomas H. Koening, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553 (2005).

85. The term "general public" refers to society at large in broad terms. To be sure, the technological awareness and comfort with technology varies widely based on socioeconomic status, education level, et cetera. There is also a "generational gap" in technological savvy and ability to use complex security technology. *See generally* Larry D. Rosen, *Understanding the Technological Generation Gap*, NATIONAL PSYCHOLOGIST, Mar. 2004, *available at* http://www.csudh.edu/psych/tnp45.htm.

86. *See, e.g.*, WI-FI ALLIANCE, WI-FI CERTIFIED™ FOR WI-FI PROTECTED SETUP: EASING THE USER EXPERIENCE FOR HOME AND SMALL OFFICE WI-FI® NETWORKS 2 (2007), *available* at http://www.wi-fi.org/files/wp_18_20070108_Wi-Fi_Protected_Setup_WP_FINAL.pdf ("While consumers have become increasingly aware of the importance of Wi-Fi security and have been enabling it more frequently, many networks remain unsecured, often due to the difficulty of traditional security configuration. Recent Wi-Fi Alliance research indicates that 44 percent of Wi-Fi users report that enabling security features on their Wi-Fi networks is moderately to very difficult.").

87. For instance, the "SecureEasySetup" feature provided by Broadcom simply requires a user to push a button on the wireless router and a corresponding button on the client device. *See SecureEasySetup Software*, BROADCOM, http://www.broadcom.com/products/secureeasysetup.php (last visited Feb. 12, 2012).

("WPS"), which serves "to ease setup of Wi-Fi networks and encourage consumers to always enable security features."[88] But these measures have not had overwhelmingly positive results, and a significant number of Wi-Fi networks continue to operate in unsecured mode.[89]

Further, most public hotspots whether free or commercial, continue to operate in unsecured mode due to technology limitations.[90] Most free public hotspots leave their networks "open" and do not require users to authenticate before using the network. This is chiefly because the technology to set up an authenticated Wi-Fi hotspot is cumbersome, and even when such an authentication mechanism is set up, the data transmitted between the wireless router and the user's device still might not be secure.[91] Commercial hotspot providers such as Gogo, Boingo, and T-Mobile require users to authenticate (and pay) over an encrypted channel before using their networks, but they do not encrypt the users' data transmissions and instead advise their customers to use other encryption mechanisms.[92] Even though these commercial Wi-Fi hotspots do not offer security for their users' private

88. Press Release, *Wi-Fi Alliance® to Ease Setup of Home Wi-Fi Networks with New Industry-Wide Program*, WI-FI ALLIANCE (Jan. 8, 2007), http://www.wi-fi.org/news_articles.php?f=media_news&news_id=263 ("Wi-Fi Protected Setup's simple, standardized approaches allow typical Wi-Fi users to set up and expand their Wi-Fi networks with security enabled, even if they do not understand the underlying technologies or processes involved.").

89. *See supra* notes 13, 25; *see also* Steve Ragan, *Financial and Business Wi-Fi Easy to Crack or Non-existent*, TECH HERALD (May 14, 2009, 5:20 p.m.), http://www.thetechherald.com/article.php/200920/3679/Financial-Wi-Fi-easy-to-crack-or-non-existent (discussing a survey that found that 57 percent of Wi-Fi networks detected in the financial districts of several cities were either using the weak form of security or no security at all).

90. For example, McDonald's, in announcing free Wi-Fi services at its restaurants, stated that "WEP encryption is not yet practical for a public access network, due in part to the absence of a standardized method for relaying encryption keys between different manufacturers' equipment." *Free Wi-Fi @ McDonald's*, MCDONALDS.COM, http://www.mcdonalds.com/us/en/services/free_wifi.html (last visited Mar. 6, 2012).

91. Some Wi-Fi Hotspots use software applications called "Hotspot Management Systems" to authenticate users. These systems might be able to implement the WEP security scheme to encrypt individual users' data, but WEP has proven to be ineffective in protecting against packet sniffing by other users of the same Wi-Fi network, because all users' data is encrypted using the same shared key. Security mechanisms such as WPA and WPA2 are able to protect users from sniffing, but the Hotspot Management Systems are ill equipped to handle WPA or WPA2. *See, e.g.*, *Can I Setup an Encrypted Wireless Network with Your System?*, HOTSPOT SYSTEM HELPDESK, http://www.hotspotsystem.com/deskpro/kb_article.php?ref=1364-WLXB-3087 (last visited Feb. 16, 2012).

92. *See, e.g.*, *Terms of Use*, GOGO INFLIGHT INTERNET, http://www.gogoair.com/gogo/cms/term.do#term7 (last visited Mar. 17, 2012) ("The connection through which you purchase Gogo is an SSL-encrypted link. However, following such purchase, due to multiple users of our inflight Wi-Fi access point, Gogo does not provide an encrypted communication channel (Wired Equivalency Protection known as 'WEP') or (Wi-Fi Protected Access known as 'WPA') between our in-flight Wi-Fi access point and your computer. . . . You should be aware, however, that data packets from un-encrypted Wi-Fi connections can be captured by technically advanced means when they are transmitted between a user's device and the Wi-Fi access point."); *Frequently Asked Questions*, BOINGO WIRELESS, http://www.boingo.com/boingo-faq.php (last visited Mar. 17, 2012); *T-Mobile HotSpot Security Statement*, *supra* note 32.

communications, their ubiquity and widespread use tend to create a false sense of privacy and security. There must be some sense of security, because so many people continue to pay for and use those networks.[93]

Security mechanisms such as Virtual Private Network ("VPN")[94] and Secure Sockets Layer ("SSL")[95] technology provide a way for users of unsecured Wi-Fi networks to encrypt their private communications irrespective of the underlying Wi-Fi network settings, but this technology is even more complicated and cumbersome to use for unsophisticated users. VPN technology is normally used by businesses and government agencies,[96] and it remains beyond the reach of most ordinary users, both from technical and financial perspectives. Further, "most major providers of web-based email and other sensitive web-based services do not even give their users the option of using SSL, let alone turn it on by default."[97] Until websites and all other online service providers adopt SSL technology broadly and *make it the default behavior*, so that even users who do not understand the security concepts will be protected, reliance on the availability of SSL to secure data transmissions over unsecured Wi-Fi networks is misplaced because this technology does not completely protect users.[98]

Despite these security limitations, for many people, using a public Wi-Fi network at libraries, coffee shops, and other such places continues to be an important and convenient way of connecting to the internet while away from their homes or offices. Free public Wi-Fi networks also provide a means to the internet for people who do not have, or cannot afford, a personal internet

---

93. Perhaps the general public's sense of privacy with respect to private data is unreasonable when using a free unsecured Wi-Fi network at the local Starbucks. One could also imagine a clearly visible sign at the local Starbucks claiming that private communications over the unsecured Wi-Fi network can be intercepted. In such a case, if the users continue to expect privacy in their data, such expectations might not be reasonable. However, when the general public uses commercial Wi-Fi providers, they might reasonably expect that their communications are private. The fact that these providers state in their "Terms of Use" that they do not provide encrypted communication channels does not change these expectations, particularly because most users do not read the "Terms of Use."

94. 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 secured access to their organization's network. *See* GARY P. SCHNEIDER, ELECTRONIC COMMERCE 86 (9th ed. 2011).

95. SSL is an industry standard used by several websites to encrypt data transmitted between a web server and a user's browser. Traditionally, websites that require authentication or accept payment and other such sensitive information use the SSL technology to protect data exchanged between the website and the user from eavesdroppers. *See What is SSL?*, SSL.COM, http://info.ssl.com/article.aspx?id=10241 (last visited June 22, 2011).

96. *See, e.g.*, Roger Cheng, *Lost Connections*, WALL ST. J., Dec. 11, 2007, http://online.wsj.com/article/SB119717610996418467.html.

97. Peter Eckersley, *FTC to Internet Companies: Start Using SSL*, ELECTRONIC FRONTIER FOUNDATION (Mar. 18, 2010), http://www.eff.org/deeplinks/2010/03/ftc-internet-companies-start-using-ssl.

98. Recently, the "outgoing FTC Commissioner Pamela Jones Harbour called on Web services like Yahoo!, Facebook and Hotmail to start using HTTPS/SSL encryption" and "put these companies on-notice." *Id.*

connection. Given that we are becoming an increasingly mobile society reliant on internet connectivity, users might continue to use public Wi-Fi networks for private communications even if we were to make all Wi-Fi users aware of the security risks.[99]

B. *The Fourth Amendment and "Reasonable Expectations of Privacy"*

An approach to interpreting "readily accessible to the general public" that takes into account users' expectations, their understanding of technology, and the current state of security technology is consistent with notions of "reasonable expectations of privacy" under the Fourth Amendment. The Fourth Amendment doctrine only applies to government searches, and thus has no bearing as a formal matter on the Wiretap Act's statutory protections against interception of electronic communications.[100] Nonetheless, this doctrine can help clarify what it means for something to be configured to be readily accessible to the general public. The "reasonable expectation of privacy" test can also verify whether the notions advanced above about users' privacy expectations are consistent with notions of reasonableness regarding expectations of privacy in other areas of law.[101] If users have a "reasonable expectation of privacy" in unsecured private Wi-Fi communications, the Fourth Amendment would prevent the police from intercepting such communications without a warrant.[102] If the Constitution and our intuitions say that the police cannot and should not be able to intercept unsecured private Wi-Fi communications without a warrant, this would be consistent with finding that a private party like Google is also prohibited from intercepting such communications. The Fourth Amendment protects citizens "against unreasonable searches and seizures" in order to "guard against the arbitrary use of Government power to maintain surveillance over citizens."[103] The often cited "reasonable expectations of privacy" test, first formulated in *Katz v. United States*,[104] provides that "[i]n order to benefit from Fourth Amendment

99. Rik Fairlie, *Coffee, TV or Wi-Fi?*, N.Y. TIMES GADGETWISE (Oct. 8, 2010, 4:10 PM), http://gadgetwise.blogs.nytimes.com/2010/10/08/coffee-tv-or-wi-fi/ (discussing survey results showing "a desire for constant connectivity" through Wi-Fi).

100. Briggs v. Am. Air Filter Co., 630 F.2d 414, 417 (5th Cir. 1980) ("[I]nterception (as defined by the statute) of wire communications is forbidden regardless of the speaker's expectation of privacy."); United States v. Harpel, 493 F.2d 346, 349 (10th Cir. 1974) (noting lack of "reasonable expectation of privacy" requirement with regard to intercepted wire communications).

101. To this end, this Note does not exhaustively analyze Fourth Amendment case law.

102. This assumes that society might be willing to compromise and lose some privacy interests in exchange for police protections when a police search with a warrant is allowed. However, this compromise argument is weaker when private parties invade users' privacy interests.

103. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."); S. REP. No. 99-541, at 12 (1986).

104. 389 U.S. 347, 361–62 (1967) (Harlan, J., concurring).

protections, an individual must demonstrate a subjective expectation that his activities would be private, and . . . that his expectation was one that society is prepared to recognize as reasonable."[105]

In *Kyllo v. United States*, the Supreme Court applied the "reasonable expectation of privacy" test to modern technology, holding 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.[106] Similar to thermal imaging, Wi-Fi sniffing can be thought of as monitoring radio waves emanating from inside the home. The *Kyllo* Court held that to use "technology . . . not in general public use" to detect information from inside the home that could not otherwise be obtained except by actually entering the home constitutes a Fourth Amendment search.[107] The Court's reference to technology that is not in "general public use" is illustrative in its application of the objective prong of the *Katz* test—an expectation of privacy that society recognizes as reasonable.[108] Thus, if the technology used to monitor the activities inside a person's home is not generally accessible to the general public, that person may maintain a reasonable expectation of privacy in those activities.[109]

Kyllo's reasoning indicates that the current understanding of users' expectations that unsecured private Wi-Fi communications are immune from sniffing is reasonable.[110] Though Wi-Fi packet-sniffing tools are available on

---

105. United States v. Young, 573 F.3d 711, 715–16 (9th Cir. 2009) (internal citations omitted).

106. 533 U.S. 27 (2001).

107. *Kyllo*, 533 U.S. at 34.

108. *Id.* at 33. The Court gave other examples of technologies that it considered not to be in general public use: "But just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house." *Id.* at 35.

In a recent case, *United States v. Jones*, though the Supreme Court had the opportunity to apply the "reasonable expectation of privacy" test in the context of modern technology, it avoided the issue by holding on narrower grounds that the police's act of physically attaching a tracking device to a car constituted a search within the meaning of the Fourth Amendment. 132 S. Ct. 945 (2012). However, the opinion in no way changed the application of the "reasonable expectation of privacy" doctrine in electronic surveillance cases not involving physical trespass, as is commonly the case with Wi-Fi sniffing. *Id.* at 947 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."); *id.* at 954 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."); *id.* at 957 (Sotomayor, J., concurring) ("Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision.").

109. *Id.* at 34; Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) ("It may well be . . . that surveillance of private property by using highly sophisticated surveillance equipment *not generally available to the public*, such as satellite technology, might be constitutionally proscribed absent a warrant." (emphasis added)).

110. Users probably do not have reasonable expectations of privacy in the addressing information contained in data packets transmitted over Wi-Fi networks. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[E]ven if petitioner did harbor some subjective

the internet for free, the technical expertise necessary to use these tools is anything but common knowledge among the general public.[111] To illustrate, courts refused to recognize an expectation of privacy in cordless phone conversations as reasonable since, in the early stages of cordless phone technology, conversations "could be intercepted easily with *readily available technology*, such as an AM radio."[112] For the same reason, the Wiretap Act initially did not protect cordless phone conversations.[113] However, later when cordless phone technology improved to make it more difficult to intercept these communications, Congress amended the Wiretap Act to extend protection to cordless phone conversations.[114] In the case of unsecured Wi-Fi communications, specialized sniffing tools and expertise are needed for interception but, unlike AM radios, are not commonly available. Thus, the current state of Wi-Fi sniffing technology may support *Kyllo*'s reasoning and the general public's reasonable expectations in unsecured Wi-Fi communications.[115] Further, the fact that most operators of home Wi-Fi networks never intentionally configure their networks to operate in unsecured mode (it is the manufacturer's default configuration) indicates that these users have not taken any steps to indicate that they have relinquished any reasonable expectations of privacy.

Reasonable expectations of privacy in unsecured Wi-Fi communications need not be limited to home Wi-Fi networks; expectations in private

---

expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as reasonable.' " (quoting Katz v. United States, 389 U.S. 347, 361 (1967))). However, users may still have "reasonable expectations of privacy" in the private information contained in data packets (i.e., payload data) transmitted over Wi-Fi networks.

111. Arguably, sniffing technology may get simpler as technology progresses. Once this technology becomes widely accessible to the common public, then perhaps the private Wi-Fi communications themselves will become more easily accessible to the general public. For example, a recently developed sniffing tool, "Firesheep," an extension available for the popular Firefox web browser, makes sniffing private data on open Wi-Fi networks very easy. Evelyn Rusli, *Firesheep in Wolves' Clothing: Extension Lets You Hack into Twitter, Facebook Accounts Easily*, TECHCRUNCH (Oct. 24, 2010), http://techcrunch.com/2010/10/24/firesheep-in-wolves-clothing-app-lets-you-hack-into-twitter-facebook-accounts-easily.

112. Price v. Turner, 260 F.3d 1144, 1148 (9th Cir. 2001) (emphasis added) (quoting S. REP. No. 99-541, at 12 (1986)) (internal quotation marks omitted).

113. *Id.*

114. *Id.*

115. Based on the "open fields" doctrine of *Oliver v. United States*, one may argue that once the Wi-Fi signals have escaped into the "open fields" (i.e., outside of the home and the immediately surrounding area called "curtilage"), the user cannot have a reasonable expectation of privacy in the information contained in those signals. 466 U.S. 170, 180 (1984). However, the *Oliver* Court did not abandon the *Katz* "reasonable expectation of privacy" test and held only that because open fields are accessible to the public and police in ways that a home or commercial structure would not be, and because fences or "No Trespassing" signs do not effectively bar the public from *viewing* open fields, an asserted expectation of privacy in open fields is not one that society recognizes as reasonable. *Id.* at 179. In the case of Wi-Fi communications transmitted over *invisible* radio waves—waves that might have escaped the home—*Kyllo*'s approach to evaluating reasonableness of expectations of privacy is still the relevant inquiry.

communications transmitted using an unsecured Wi-Fi network available at a public place, such as Starbucks, may also be reasonable. *Kyllo* focused on expectations of privacy for information emanating from within a home, and "home" has a special place in our society in terms of privacy expectations.[116] However, Fourth Amendment case law has never necessarily limited reasonable privacy expectations to the home.[117] In fact, *Katz*—the progenitor of the "reasonable expectation of privacy" test—held that "the Fourth Amendment protects people . . . not simply 'areas.' "[118] *Katz* held that a person using a *public* telephone booth may rely on Fourth Amendment protections, because, regardless of the location, a private communication is protected as long as it is made with a "reasonable expectation of privacy."[119] Because of the need for specialized technology to intercept unsecured private Wi-Fi communications, the general public's expectations of privacy in personal communications made using a Starbucks Wi-Fi network are not necessarily diminished,[120] even though the network is public.[121]

As discussed in Section II.B, the district court in *United States v. Ahrndt* applied the *Katz* test to rule that evidence of child pornography found on the defendant's computer through his open Wi-Fi network and shared iTunes library could be used against him in court, even absent a warrant.[122] The court concluded that "society recognizes a lower expectation of privacy in

---

116. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

117. *See, e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 248–49 (1986) (Powell, J., concurring in part and dissenting in part) (citing Marshall v. Barlow's, Inc., 436 U.S. 307, 311–13 (1978)) ("[O]ur cases holding that Fourth Amendment protections extend to business property have expressly relied on our society's historical understanding that owners of such property have a legitimate interest in being free from unreasonable governmental inspection.").

118. Katz v. United States, 389 U.S. 347, 353 (1967).

119. *See id.* at 352; *Dow Chem.*, 476 U.S. at 247 (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.").

120. In *United States v. Knotts*, the Supreme Court held that the police's use of beeper technology to monitor the presence of a driver's automobile does not violate Fourth Amendment, since expectations of privacy do not extend to visual surveillance from public places. 460 U.S. 276, 282 (1983). More specifically, the Court found that increased efficiency of police surveillance using new technology is not unconstitutional. *See id.* at 284. However, in the case of sniffing Wi-Fi networks at public places, the technology is not merely increasing surveillance efficiency; without the sniffing technology, surveillance would not be possible in the first place.

121. When people have a conversation at Starbucks, they might understand that any expectation of privacy in the contents of their conversation is minimal. Similarly, they might understand that others might look over a laptop user's shoulder, so that privacy expectations in the information displayed on the user's computer screen might also be diminished. But the general public using the unsecured Starbucks Wi-Fi network may not understand the packet-sniffing technology enough to reasonably expect diminished privacy in the information they are transmitting over the Wi-Fi network.

122. *See* No. 08-468-KI, 2010 WL 373994 (D. Or. Jan. 28, 2010).

information broadcast via an unsecured wireless network router" because "accidental unauthorized use of other people's wireless networks is a fairly common occurrence" and that "[p]urposeful unauthorized use is perhaps equally ubiquitous."[123] However, the court seems to have ignored the distinction between society's expectations regarding accessing and using an unsecured Wi-Fi network and users' expectations that the private data they send on these networks is still private. For example, a user posting comments on a publicly accessible blog using a secured or unsecured network has no reasonable privacy expectation in the comments once they are posted on the public forum,[124] but this is not equivalent to the user's privacy expectations in those same comments *while* they are transmitted over the network.

In sum, users expect that their private data communications over Wi-Fi networks, including communications over unsecured Wi-Fi networks, remain private. These expectations mostly stem from users' limited understanding of the underlying Wi-Fi technology and the corresponding security risks, and more importantly, from the fact that private data cannot be intercepted without specialized tools and knowledge.[125] Though the Fourth Amendment "reasonable expectation of privacy" test is not a requirement of the Wiretap Act, the analysis verifies that users' privacy expectations in unsecured Wi-Fi communications are consistent with notions of reasonable expectations of privacy in other areas of law. Moreover, in enacting the Wiretap Act, Congress was "[u]nsure whether the flexible approach to determining the extent of Fourth Amendment protections as announced in *Katz* . . . would extend to electronic communications" and intended to create "a baseline level of protection" for electronic communications.[126] Even though the Fourth Amendment doctrine is informative, it does not suggest limits to the Wiretap Act's protections.[127] In the absence of clear statutory guidance on the

123. *Ahrndt*, 2010 WL 373994, at *4–5.

124. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient." (citation omitted)).

125. It is important to note that society's privacy expectations may change with time and technological progress. In a remarkably forward looking opinion, Justice Alito recently worried about technology and privacy intrusions:

> But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.

United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).

126. Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349 (2009).

127. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 850–51 (2004); *see also supra* note 100.

meaning of "readily accessible to the general public" term, the term should be interpreted in a manner that accords with the expectations of general Wi-Fi users while addressing the concerns and dangers of Wi-Fi sniffing.

IV. NEED FOR AMENDING THE WIRETAP ACT

The statutory interpretation of Wiretap Act provisions advanced in Part II leaves protections for unsecured Wi-Fi communications too unsystematic and uncertain. Though the interpretation of the "readily accessible to the general public" exception advanced in Part III might address concerns about users' expectations of privacy, an amendment to the Wiretap Act would reflect these concerns more explicitly and remove any unpredictability in protecting users' expectations.[128] Given that the Act is the predominant law protecting the privacy of electronic communications, the statute should expressly address concerns about Wi-Fi sniffing. This Part advocates amending the statute to explicitly protect all Wi-Fi communications, whether secured or unsecured, from intentional interception.

While the long-term solution to protecting data privacy over Wi-Fi networks might lie in educating users and addressing technology limitations, the Wiretap Act still has an important role to play in protecting users in the interim. In addition, even after users have been educated, more sophisticated sniffing technology might be developed to evade privacy protections. Amending the Act to clearly protect all Wi-Fi communications can bridge the gap between users' hypothetical ability to protect themselves and the practical realities of doing do, while also anticipating more sophisticated sniffing technologies.[129] Wi-Fi technology plays a very important role in society, and the social and private costs of data and identity theft resulting from Wi-Fi sniffing are too high for the law to ignore shortcomings in security technology and in users' ability to protect themselves.[130]

Removing the uncertainty in legal protections against Wi-Fi sniffing also has other benefits. Given the current pace of Wi-Fi adoption, it may seem that no additional incentives are necessary to encourage adoption of wireless technologies. However, a robust Wiretap Act protecting users from unwarranted and intentional packet sniffers could boost the adoption of new and

---

128. This Note assumes that the nature of the right to privacy in electronic communications tracks some notion of "reasonable expectation of privacy," at least to the extent that the United States Constitution protects such a right. It is beyond the scope of this Note whether there is any fundamental right to privacy stemming from various Bill of Rights amendments that does not depend on whether people reasonably expect their information to be private.

129. The Wiretap Act could easily be amended by clarifying the applicability of subsection 2510(16)'s "readily accessible to the general public" definition and explicitly removing unsecured Wi-Fi communications from the definition. 18 U.S.C. § 2510(16) (2006).

130. Some members of the government acknowledge the need to expand and enhance federal and state laws to protect people from data interception. *See, e.g.*, Scott Morrison, *Connecticut to Lead Multistate Probe of Google*, WALL ST. J., June 21, 2010, http://online.wsj.com/article/SB10001424052748704895204575320802269077146.html (Connecticut Attorney General Richard Blumenthal acknowledging that there is such a need).

upcoming wireless technologies.[131] For example, several cities and municipalities have been operating or attempting to operate municipal Wi-Fi networks with the goal of making wireless access to the internet available citywide.[132] While addressing security concerns is vital to the success of these technologies, clear legal protections against unauthorized data interceptions could likewise encourage the development of improvements to these technologies.

At the same time, it is important to recognize legitimate uses of Wi-Fi sniffing and not to overregulate. Network administrators and security researchers use packet sniffers to find troublesome computers that use too much bandwidth, have the wrong network settings, or are virus infected.[133] System administrators also sniff their own networks to detect hacking attempts or inappropriate traffic on their networks.[134] This genuine need for sniffing can be addressed by carving out clear exemptions from liability for such activities. The Act already has such an exemption for troubleshooting purposes: it is not unlawful "to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference."[135] Current law also includes a consent provision, where if "one of the parties to the communication has given prior consent to such interception," intercepting electronic communications is not a violation of the Act, "unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[136] Further, the existing Act has a strong "intent" requirement, so that any accidental, unintended interception of Wi-Fi communications does not result in liability. Thus, privacy protections for unsecured Wi-Fi communications can be extended through the Act without compromising legitimate uses of packet sniffing in research and network administration.

We must also be cognizant of the collateral effects of any policy extending protections to unencrypted Wi-Fi communications. One commentator has noted the following:

---

131. Referring to a gap in federal statutory standards for protecting the privacy of communications transmitted by new forms of technology, a similar concern was expressed by the Senate in its report accompanying the 1986 amendments to the Wiretap Act:

> This gap results in legal uncertainty. It may unnecessarily discourage potential customers from using innovative communications systems. It probably encourages unauthorized users to obtain access to communications to which they are not a party. It may discourage American businesses from developing new innovative forms of telecommunications and computer technology.

S. REP. NO. 99-541, at 5 (1986).

132. Tracy V. Wilson, *How Municipal WiFi Works*, HOWSTUFFWORKS, http://computer.howstuffworks.com/municipal-wifi.htm (last visited Mar. 23, 2012).

133. *See, e.g.*, Karen J. Bannan, *Sniff Out Trouble*, PCMAG.COM (May 22, 2001), http://www.pcmag.com/article2/0,2817,27054,00.asp.

134. *Id.*

135. 18 U.S.C. § 2511(2)(g)(iv) (2006).

136. 18 U.S.C. § 2511(2)(d).

> [A] statute that makes it a crime to obtain information only when it is encrypted will likely prompt victims to encrypt their information and may encourage manufacturers to change the default settings on wireless access products to ensure encryption. A statute with no encryption prerequisite would unlikely have these collateral incentive effects.[137]

But even if the law affords protections to unencrypted communications, users will still want to prevent their data privacy from being violated in the first place, instead of relying on the law's post-hoc remedies for such violations. The general public is most likely unaware of the Act's protections. Therefore, it is not credible to expect that users will be completely discouraged from encrypting their Wi-Fi communications because of the statutory language.

It could also be argued that extending protections to unsecured Wi-Fi communications will unnecessarily expand the reach of federal power, particularly when users can protect themselves by enabling the security features on their personal Wi-Fi networks or by avoiding any unsecured public Wi-Fi networks. While users can protect themselves to some extent by various technical means, legal protections can bridge the gap in protecting users' privacy until limitations in technology and consumer awareness can be overcome. In ten to twenty years, users may become so educated about privacy risks, or sniffing technology may become so pervasive, that users will not have any expectations of privacy in unsecured private Wi-Fi communications. The security technology might also make significant advances in simpifying the securing of home Wi-Fi and public Wi-Fi networks at places such as Starbucks.

If federal overreach is a concern, a sunset provision could be part of any amendment to the Wiretap Act. Congress could require the FCC or a similar regulatory body with relevant technical expertise to submit periodic comprehensive reports on the state of Wi-Fi technology and the need for continued statutory privacy protections for unencrypted Wi-Fi communications. The sunset provision could mandate that any provision extending the privacy protections to unencrypted Wi-Fi communications would expire after a specific time period unless Congress finds a continued need for such a provision.

CONCLUSION

If a court finds that Google intentionally intercepted users' private data when its Street View cars scoured the airwaves for Wi-Fi networks, should the court hold Google liable under the current Federal Wiretap Act? The answer remains unclear. The statutory language of the Act indicates that at least a subset of Wi-Fi communications may be protected from intentional interception, even if Congress might not have specifically intended to cover those types of communications when it amended the Act in 1986. Under a different interpretation, the statutory definition of the term "readily accessi-

137. Brian M. Hoffstadt, *The Voyeuristic Hacker*, 11 J. INTERNET L. 1, 15 (2007).

ble to the general public" might not apply at all. In that case, whether unsecured Wi-Fi communications are excluded from the statutory protections against intentional interception remains uncertain.

Regardless of the result, the high profile nature of *In re Google* has raised important questions regarding Wi-Fi sniffing and electronic privacy law. *In re Google* highlights the gaps in consumer understanding of network technology and security risks, and the shortcomings of current security technology. But electronic privacy laws have not adequately responded to this gap. Congress should clarify the existing electronic privacy law, which has not been substantively updated since its passage in 1986, to reflect the widespread use of new technologies and extend uniform protections to all Wi-Fi communications.