Wi-Fi Security: Shaping Data Privacy Rules

Carla Voigt*

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2014.

I. INTRODUCTION

In a world of smartphones and tablets, the risk of revealing personal information never intended to be disseminated publicly is high. Wi-Fi[1] and other wireless communications technologies provide the ability to connect all of one's favorite content with a mobile phone, computer, or other devices easily and quickly.[2] This enables one to stay productive on the go by connecting to the Internet from remote locations.[3]

However, with this convenience comes great risk. For example, "[h]ackers snooping on unprotected or poorly protected Wi-Fi networks have been responsible for some of the biggest cyberheists in recent history, including numerous thefts from Seattle-area businesses from 2006 to 2011 and the 2007 TJX Companies data breach, which exposed 45 million credit card numbers."[4] Using Wi-Fi networks to send or receive confidential information could result in unauthorized disclosure of attorney-client privileged communications, trade secrets, or other confidential information—raising serious malpractice and ethical ramifications for attorneys. Because unencrypted private networks and public hotspots use public airwaves instead of wires for the transmission of communications, the interception of such unencrypted transmissions may not be within the reach of state or federal wiretap laws, even if such communications include user names, passwords, account numbers, credit card numbers, Social Security numbers, trade secrets, or attorney-client privileged communications.[5] Even more troublesome, "the mere use of such networks could call into question the status of such information as being confidential, privileged or trade secret," because exposing the information to an unencrypted network makes that information available for public consumption in its readable form.[6] Though "86% of internet users have taken steps online to remove or mask their digital footprints . . . [and] 55% of internet users have taken steps to avoid observation by specific people,

---

1. Wi-Fi is wireless transmissions that use 802.11b/g/n/ac specification and are used for wireless Internet access. *See* AIR802, IEEE 802.11 A/B/G/N WI-FI STANDARDS AND FACTS, *available at* http://www.air802.com/files/802-11-WiFi-Wireless-Standards-and-Facts.pdf. Wi-Fi devices use unlicensed spectrum governed by Part 15 of Title 47 of the FCC's rules. *See* 47 C.F.R. § 15 (2013).

2. *Discover and Learn*, WI-FI ALLIANCE, http://www.wi-fi.org/discover-and-learn (last visited Mar. 2, 2014).

3. *See id.*

4. Paul Wagenseil, *Google Spy Case Shows Why You Need to Encrypt Your Wi-Fi*, NBCNEWS.COM (Jan 21, 2012), http://www.nbcnews.com/technology/technolog/google-spy-case-shows-why-you-need-encrypt-your-wi-744411.

5. *See* Richard L. Ravin, *Using Public Wi-Fi Hotspots Can Land You in Hot Water by Risking Disclosure of Confidential Information*, 251 N.J. LAW. MAG., Apr. 2008, at 10, 10; *see also In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 888 (N.D. Ill. 2012).

6. Ravin, *supra* note 5, at 10.

organizations, or the government,"[7] cautious Internet users are often at the mercy of their less careful correspondents. For example, the sender of an email attachment containing sensitive personal information sent from a secure, encrypted Wi-Fi network is in no position to ensure that the recipient—be it a doctor, lawyer, accountant, priest, or spouse—has taken care to encrypt her own Wi-Fi network. Therefore, anyone parked outside her house with a packet sniffer while she downloads the attachment could intercept its contents because the *recipient's* Wi-Fi network was not encrypted.[8]

This Note examines the authority of the Federal Communications Commission ("FCC") to address such data privacy concerns under the Wiretap Act and finds that this outdated regulatory framework places the FCC at a regulatory disadvantage. Part II of this Note explains how Wi-Fi works and why many consumers who believe their private information is protected are actually vulnerable to attack. Part III discusses the FCC's authority to regulate the interception of Wi-Fi communications under the agency's general statutory jurisdiction over communications technologies. Part III also explores recent litigation that demonstrates the inconsistencies in statutory interpretation that have arisen as a result of new technology and the ambiguous existing statutory framework. Part IV examines recent FCC administrative litigation and why it is important for the FCC to regulate new technology so as to bolster information privacy. Part V argues that Congress should amend the Wiretap Act to better protect user privacy. Part VI weighs several possible FCC administrative solutions and combinations thereof. Part VII discusses the implications of these administrative and legislative reforms for consumers and corporations.

II. BACKGROUND

Wi-Fi networks wirelessly connect electronic devices such as laptop computers, tablets, video game consoles, and smartphones to the Internet and each other through wireless network access points.[9] These networks operate in the 2.4 and 5 GHz radio bands,[10] and typically have a range of several hundred feet, although performance varies depending on obstructions and interference from other sources.[11]

---

7. LEE RAINIE ET AL., PEW RESEARCH CTR., ANONYMITY, PRIVACY, AND SECURITY ONLINE 2, 4 (Sept. 5, 2013), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf.

8. *See* Joffe v. Google, Inc., 729 F.3d 1262, 1272 (9th Cir. 2013), *amended and superseded on reh'g*, 746 F.3d 920 (9th Cir. 2013), *cert denied*, 134 S. Ct. 2877 (2014).

9. *See Discover and Learn*, *supra* note 2.

10. *Id.*

11. *See* GIUSEPPE ANASTASI ET AL., WI-FI IN AD HOC MODE: A MEASUREMENT STUDY 5–6 (2004), *available at* http://pdf.aminer.org/000/538/456/wi_fi_in_ad_hoc_mode_a_measurement_study.pdf.

Today, 70.8% of Wi-Fi networks are estimated to be secured with encryption, leaving nearly 30% of Wi-Fi networks unsecured.[12] Collecting private information from these unsecured networks is easier than the average consumer might believe. Many hackers use packet-sniffing technology, which can unveil the contents of unencrypted network transmissions, to illegally break into networks and capture data including passwords, IP addresses, and other information that will help an attacker infiltrate the network.[13] Essentially, packet sniffing is to computer networks as wiretapping is to a telephone network.

According to Joel Gurin, former Chief of the Consumer and Governmental Affairs Bureau at the FCC, "[w]hether intentional or not, collecting information sent over WiFi networks clearly infringes on consumer privacy."[14] Since the FCC is the agency charged with promoting "safety of life and property" by "regulating interstate and foreign commerce in communication by wire and radio,"[15] the FCC can apply the substantive provisions of the Wiretap Act to emerging technologies such as Wi-Fi networks.

The FCC has examined the interception of private information over unencrypted Wi-Fi networks in the past. For example, in 2010, the agency opened an investigation into Google's Street View project, after the company admitted in May 2010 that its Street View cars had "mistakenly" collected samples of "payload data" including "e-mail and text messages, passwords, Internet usage history, and other highly sensitive personal information" from unsecured Wi-Fi networks.[16] Google subsequently explained that "while most of the data" it had collected was "fragmentary,

12. *See* WIRELESS GEOGRAPHIC LOGGING ENGINE, http://wigle.net/gps/gps/main/stats/ (last visited Mar. 2, 2014).

13. MOHAMMED ABDUL QADEER ET AL., IEEE COMPUTER SOC'Y, NETWORK TRAFFIC ANALYSIS AND INTRUSION DETECTION USING PACKET SNIFFER 313 (2010), *available at* http://eecs.wsu.edu/~nroy/courses/spring2013/cptsee555/papersbystudent/Network%20Traffic%20Analysis%20and%20Intrusion%20Detection%20using%20Packet%20Sniffer_Steven.pdf.

14. Joel Gurin, *Consumer View: Staying Safe from Cyber Snoops*, OFFICIAL BLOG OF THE FCC (June 11, 2010), http://reboot.fcc.gov/blog?entryId=493624.

15. 47 U.S.C. § 151 (2006).

16. Google, Inc., *Notice of Apparent Liability for Forfeiture*, DA 12-592, para. 1 (rel. Apr. 13, 2012) [hereinafter *Notice of Apparent Liability*], *available at* http://transition.fcc.gov/DA-12-592A1.pdf; *see also* Joffe v. Google, Inc., 746 F.3d 920, 922–23 (9th Cir. 2013), *aff'g In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067 (N.D. Cal. 2011) ("Payload data includes everything transmitted by a device connected to a Wi-Fi network, such as personal emails, usernames, passwords, videos, and documents."); *see also* Alan Eustace, *WiFi Data Collection: An Update*, GOOGLE OFFICIAL BLOG (May 14, 2010), http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

in some instances entire emails and URLs were captured, as well as passwords."[17]

Although the FCC's Google Street View investigation left observers with many unanswered questions, it also broke new ground for the agency in its role in policing consumer privacy.[18] The FCC's investigation into whether this interception of sensitive and personal information violated section 705(a) of the Communications Act[19] is examined in Part IV below. Since the FCC can enforce civil violations of the Wiretap Act involving Wi-Fi networks, what does that mean for companies and individuals moving forward? The penalty for this type of invasion of privacy was not established in the FCC's Google investigation in part because the agency lacked sufficient information.[20] The FCC issued nothing more than a slap on the wrist in the form of a measly $25,000 fine[21] to Google (which generated revenue of $14,890,000,000 in the third quarter of 2013).[22] Although the Google case suggests that the FCC intends to enforce the Wiretap Act provisions against similar privacy violations in the future, Congress should also take notice of this issue and explore statutory reform.

Since the passage of the 1996 amendments to the Communications Act eighteen years ago, communications technology has evolved more rapidly than lawmakers could have imagined. It is time for Congress to realign the Communications Act and the Wiretap Act with present technological realities. Congress must expand the FCC's authority to regulate emerging technologies. Doing so will allow the FCC to keep up with the "rapid deployment of new technology" it has been asked by Congress to promote.[23] In a world where the unofficial slogan of Silicon Valley is "[b]etter to seek forgiveness than permission,"[24] the FCC's ability

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

18. In addition to the FCC, the Federal Trade Commission ("FTC") plays a major role in policing consumer privacy violations. Under federal law, the FTC is empowered to "prevent" most companies "from using . . . unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a) (2012).

19. 47 U.S.C. § 605(a) (2006).

20. *Id.*

21. *See* David Streitfeld & Edward Wyatt, *Unanswered Questions in F.C.C.'s Google Case*, N.Y. TIMES, Apr. 16, 2012, at B1, *available at* http://www.nytimes.com/2012/04/16/technology/fccs-google-case-leaves-unanswered-questions.html?pagewanted=all [hereinafter *Unanswered Questions*].

22. *See* Chris Velazco, *Google Beats the Street in Q3 with $14.89B in Revenue, Net Income of $2.97B, and EPS of $10.74*, TECHCRUNCH (Oct. 17, 2013), http://techcrunch.com/2013/10/17/google-q3-2013-earnings/.

23. *See* Elizabeth D. Lauzon, Annotation, *Construction and Application of Communications Act of 1934 and Telecommunications Act of 1996 – United States Supreme Court Cases*, 32 A.L.R. FED. 2D 125 § 2 (2008).

24. *See* David Streitfeld & Claire Cain Miller, *Google Hastens to Show Its Concern for Privacy*, N.Y. TIMES, Mar. 14, 2013, at B1, *available at* http://www.nytimes.com/

to address public concerns about privacy is essential to promoting confidence in new technology.

If Congress were to explicitly define the FCC's authority over new technologies—perhaps by clearly defining the phrases "readily accessible to the general public" and "radio communications," as discussed in Part III—it would remove obstacles to enforcement created by ambiguous language in the statute. Wi-Fi networks and similar technologies have become increasingly more common and in, therefore, merit greater FCC and judicial oversight. Consumer confidence is the backbone of the U.S. technology market, but recent events have caused a plunge in consumer confidence in information privacy and its regulators.[25] Congress must counteract this threat to innovation by overhauling obsolete privacy laws.

III. PRIVACY PROTECTION UNDER THE COMMUNICATIONS AND WIRETAP ACTS

In order to understand the scope of the FCC's jurisdiction over intercepted Wi-Fi communications, it is helpful to understand the two statutes that grant the FCC general jurisdiction over communications technologies and unlawful interceptions. The Communications Act of 1934 created the FCC, granting it "broad authority over interstate and foreign communication by wire or radio . . . ."[26] Congress has amended the Communications Act several times since 1934 in an effort to enable the FCC to regulate new technologies that have rendered old statutory provisions obsolete.[27] In 1968, the Wiretap Act broadened the scope of FCC jurisdiction through an additional grant of authority over electronic communications in addition to the already existing FCC jurisdiction over wire and radio communications.[28] The Wiretap Act, which is cross-referenced through the Communications Act, grants the FCC general authority to regulate emerging technologies, including Wi-Fi networks. The following discussion examines both statutes and their implications in turn.

2013/03/14/technology/google-focuses-on-privacy-after-street-view-settlement.html?pagewanted=all [hereinafter *Concern for Privacy*].

25. *See e.g.*, DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 1, 2 (Aug. 2013); Sam Gustin, *NSA Spying Scandal Could Cost U.S. Tech Giants Billions*, TIME BUS. & MONEY (Dec. 10, 2013), http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/.

26. Lauzon, *supra* note 23.

27. *See, e.g.*, Cable Communications Act of 1984, Pub. L. No. 98-549, 98 Stat. 2780; Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No. 102-385, 106 Stat. 1460; 47 U.S.C. § 201 (2006); Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, Title VI, 125 Stat. 156.

28. Wiretap Act, 18 U.S.C. § 2510(12) (2012).

A. The Communications Act of 1934

The Communications Act of 1934 established the FCC "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio" in the United States.[29] The Act stripped the Interstate Commerce Commission of its jurisdiction over telecommunications carriers and gave that authority to the newly created FCC.[30] By enacting this statute, Congress intended to make available "a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities" and to promote "safety of life and property through the use of wire and radio communications, and for the purpose of securing a more effective execution of this policy."[31]

The Communications Act also confers broad authority to the FCC to protect the public interest through rules and regulations. The FCC's rulemaking authority comes from section 4(a) of the Act, which provides that "[t]he Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."[32] Congress' ultimate purpose in establishing the FCC was to set up an expert agency capable of coping with the ever-changing and constantly increasing problems of "a booming industry,"[33] to secure and protect the public interest,[34] and to ensure uniformity of regulation.[35]

In order to address changes in technology and further its effort to preserve and protect the integrity of communications by wire and radio in the United States, Congress enacted the Telecommunications Act of 1996 ("Telecommunications Act").[36] The Telecommunications Act overhauled the Communications Act to provide the FCC with additional authority to promote competition in the telecommunications industry, encourage the rapid deployment of new technology, and regulate nearly all radio communications in the United States.[37]

The FCC's authority to regulate communications intercepted over unencrypted Wi-Fi networks comes from the prohibitions outlined in section 705(a) of the Communications Act. Section 705(a) regulates the unauthorized publication or use of communications, prohibiting certain acts

---

29. 47 U.S.C. § 151 (2006).

30. The FCC replaced the Federal Radio Commission, which regulated radio use from 1926 to 1934. FCC MAX D. PAGLIN, A LEGISLATIVE HISTORY OF THE COMMUNICATIONS ACT OF 1934, at 3 (1989).

31. 47 U.S.C. § 151 (2006).

32. 47 U.S.C. § 154(i) (2006).

33. American Broadcasting Co. v. FCC, 191 F.2d 492, 498 (D.C. Cir. 1951).

34. WOKO, Inc. v. FCC, 109 F.2d 665, 667 (D.C. Cir. 1939).

35. Lauzon, *supra* note 23.

36. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 47 U.S.C.).

37. *Id.*

such as using and intercepting communications without authorization, except under certain conditions denoted in the Wiretap Act.[38]

B. The Wiretap Act

In response to "congressional investigations and published studies that found extensive wiretapping had been conducted by government agencies and private individuals without the consent of the parties or legal sanction,"[39] Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly known as the "Wiretap Act"),[40] which originally covered only the unauthorized, nonconsensual interception of wire and oral communications by government agencies.[41]

By the 1980s, however, technology had evolved to offer wireless telephone services and communication through data transfer rather than voice.[42] Since the Wiretap Act applied only to voice communications over a wire or face to face, the need for Congressional action was clear.[43] The courts were still uncertain whether the Fourth Amendment protected communications over these new technologies, and the government argued that transmitting data through the computer of an Internet service provider waived any expectation of privacy.[44] According to some advocates, Congress faced the risk of "[a] ruling by the courts that wireless or data communications were not private, [which] would have stopped development of these technologies dead in their tracks."[45] Congress's response was to significantly revise the Wiretap Act by enacting the Electronic Communications Privacy Act ("ECPA").[46]

Title I of ECPA amended the Wiretap Act in 1986 to include "electronic communications" along with the communications by wire and radio already covered by the Wiretap Act.[47] As amended since, the current

---

38. 47 U.S.C. § 605(a) (2006). The exceptions are at chapter 119 of Title 18 of the United States Code.

39. *See Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, JUSTICE INFO. SHARING, http://www.it.ojp.gov/default.aspx?area=privacy&page=1284#contentTop (last visited Mar. 2, 2014).

40. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2520 (1968)).

41. 18 U.S.C. § 2511(1)(a) (1968).

42. *See Security and Surveillance*, CTR. FOR DEMOCRACY & TECH., https://www.cdt.org/issue/wiretap-ecpa (last visited Mar. 2, 2014).

43. *Id.*

44. *Id.*

45. *Id.*

46. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

47. S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557; *see also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002). Wi-Fi networks are an example of an "electronic communication," which is defined by Congress as a communication transmitted by transferring "signs, signals, writing, images, sounds, data or

Wiretap Act provides that, with certain exceptions, "any person who intentionally intercepts . . . any wire, oral, or electronic communication" shall be subject to criminal and civil liability.[48] The amendments also made it illegal for government agencies or private parties to wiretap telephones or install electronic "sniffers" that read Internet traffic.[49] The Wiretap Act gives a private right of action to individuals aggrieved by the unlawful wiretapping of any person "other than the United States."[50]

C. Applicable Statutes Outdated as a Result of Innovation

The gap between what technology is capable of doing and the farthest reaches of existing regulations is growing. "[T]he FCC's authority under Title I is, at best, uncertain."[51]

In *Konop v. Hawaiian Airlines, Inc*., the United States Court of Appeals for the Ninth Circuit tackled the issue of whether a particular communication was an "electronic communication" and, if so, whether an "interception" had occurred.[52] In its opinion, the court noted that the issue was unnecessarily complicated by the seriously outdated Wiretap Act, observing that "[c]ourts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results."[53] The *Konop* court, back in 2002, recognized the need for Congress to reform the "confusing and uncertain" area of law under the Wiretap Act.[54] Since then, technology has continued to evolve; it is time that Congress act to protect the privacy of the billions of people who transmit private information over Wi-Fi networks every day.

---

intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (2012).

48. 18 U.S.C. §§ 2511(1)(a), 2511(4)(a), 2520(a) (2012). "[I]ntercept" as defined by the Wiretap Act "means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (2012).

49. 18 U.S.C. § 2510(6) (2012).

50. 18 U.S.C. § 2520 (2012).

51. James B. Speta, *FCC Authority to Regulate the Internet: Creating It and Limiting It*, 15 LOY. U. CHI. L. J. 15, 22 (2004).

52. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

53. *See id.* (citing Robert A. Pikowsky, *Legal and Technological Issues Surrounding Privacy of Attorney Client Communication Via Email*, Advocate, Oct. 2000, at 17–19 (discussing the uncertainty over email privacy caused by ECPA and judicial interpretations thereof); *see also* LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See*, 46 A.F. L. REV. 155, 171–74 (1999) (same); Tatsuya Akamine, Note, *Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act*, 7 J.L. POL'Y 519, 521–29, 561–68 (1999) (criticizing the judiciary's interpretation of ECPA)).

54. *Konop*, 302 F.3d at 874 ("We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain . . . uncertain . . . .").

D. Exceptions to the Wiretap Act and Related Litigation

The Wiretap Act, as amended by ECPA, makes it illegal to intercept electronic communications, but it includes an important exception that is relevant to the interception of communications over Wi-Fi networks. The Wiretap Act exempts from liability the interception of communications "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." [55] Communications that fall within this exception may be intercepted legally regardless of whether or not they were *intended* to be made available to the public.[56] The phrase "readily accessible to the general public" is defined in section 2510(16) with respect to radio communication to mean that such communication is not "scrambled or encrypted," among other requirements.[57] The statute does not, however, specifically address when *electronic communications* are "readily accessible to the general public."[58] "The legislative history of ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards," as opposed to communications that are easily accessible to the general public.[59]

In 2010, several individuals brought a consolidated class action complaint against Google in the United States District Court for the Northern District of California regarding the company's collection of Wi-Fi payload data, alleging among other things that Google unlawfully intercepted their communications in violation of the Wiretap Act.[60] Google, in defense of its Street View data collection, argued that intercepting payload data transmitted on an unencrypted Wi-Fi network is not a

---

55. 18 U.S.C. § 2511(g)(i) (2012).

56. *But see* Orin Kerr, *District Court Rules that the Wiretap Act Does Not Prohibit Intercepting Unencrypted Wireless Communications*, VOLOKH CONSPIRACY (Sept. 6, 2012, 7:08 PM), http://www.volokh.com/2012/09/06/district-court-rules-that-the-wiretap-act-does-not-prohibit-intercepting-unencrypted-wireless-communications/.

57. 18 U.S.C. § 2510(16) (2012). It is important to note that section 2510(16) specifies radio communication when addressing whether something is "readily accessible to the public."

58. Joffe v. Google, Inc., 746 F.3d 920, 924 (9th Cir. 2013).

59. *Konop*, 302 F.3d at 874 (quoting S. REP. NO. 99-541, at 35–36, *reprinted in* 1986 U.S.C.C.A.N. at 3599 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public.") and H.R. REP. NO. 99-647 at 41, 62–63 (1986) ("[D]escribing the Committee's understanding that the configuration of the electronic communications system would determine whether or not an electronic communication was readily accessible to the public . . . .")).

60. Joffe v. Google, Inc., 746 F.3d 920, 924 (9th Cir. 2013). The consolidated class was comprised of all persons whose electronic communications were intercepted by Google Street View vehicles since May 25, 2007. For a discussion of Google's alleged conduct, see *infra* Part IV.

violation of the Wiretap Act because it falls into the exception in 18 U.S.C. section 2511(2)(g)(i)[61] ("G1"), which states as follows:

> (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person – (i) 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.[62]

The court thus faced the question whether the phrase "readily accessible to the general public" applies to *unencrypted* Wi-Fi networks and, accordingly, whether Wi-Fi networks fall into the G1 exception.[63]

The consolidated class action plaintiffs argued that the phrase "'readily accessible to the general public' applies solely to 'radio communications,' as specified [in the definition in 18 U.S.C. section 2510(16)], and thus would only apply to exemption G2 ('radio communications') [64] and not exemption G1 ('electronic communications')."[65] The court acknowledged in its opinion that this

> case of first impression as to whether the Wiretap Act imposes liability upon a defendant who allegedly intentionally intercepts data packets from a wireless home network . . . presents a novel question of statutory interpretation as to how the definition in Section 2510(16) of 'readily accessible to the general public' modifies exemption G1, if at all.[66]

---

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

62. 18 U.S.C. § 2511(2)(g)(i) (2012).

63. *See* Andrew Fong, *In re Google Inc. Street View Electronic Communications Litigation: Radio Communications and Privacy by Convention*, BERKELEY TECH. L.J. BOLT (July 4, 2011), http://btlj.org/2011/07/04/in-re-google-inc-street-view-electronic-communications-litigation-radio-communications-and-privacy-by-convention/.

64. 18 U.S.C. § 2511(2)(g)(ii) ("G2") states that:

> (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person – . . . (ii) to intercept any radio communication which is transmitted – (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by an marine or aeronautical communications system.

18 U.S.C. § 2511(2)(g)(ii) (2012).

65. *See In re Google*, 794 F. Supp. 2d at 1073.

66. *Id.* at 1074; *see also* 18 U.S.C. § 2510(16) (2012) ("'[R]eadily accessible to the general public' means, with respect to a radio communication, that such communication is not . . . (A) scrambled or encrypted.").

The court further noted that "Congress has not expressly declared its intent as to how Section 2510(16) should apply to exemption G1 in the plain text of the statute, nor has Congress defined 'radio communication' anywhere within the Act."[67] Therefore, courts "must ascertain the statute's plain meaning by looking to the particular language at issue and the language and design of the statute as a whole."[68] In doing so, the district court determined that an unencrypted *radio communication* is "readily accessible to the general public," so its interception does not give rise to liability under the Wiretap Act because of the combination of the G1 exemption and the section 2510(16) definition.[69] Because "radio communication" is not defined by the Wiretap Act, the court reasoned, "'radio communication' encompasses only 'traditional radio services,' and not other technologies that also transmit data using radio waves, such as cellular phones and Wi-Fi networks."[70] Therefore, the section 2510(16) definition of "readily accessible to the general public" does not apply to Wi-Fi networks because the definition is limited to electronic communications that are radio communications.[71] Acknowledging that the plain language of the statute is ambiguous, for it does not define the phrase "readily accessible to the general public" as it applies to an "electronic communication" that is not a "radio communication," the court denied Google's motion to dismiss the Wiretap Act claim.[72] "[W]ithout more," the court held, "merely pleading that a network is unencrypted does not render that network readily accessible to the general public and serve to remove the intentional interception of electronic communications from that network from liability under the [ECPA]."[73]

Google sought interlocutory review of the district court's ruling from U.S. Court of Appeals for the Ninth Circuit, arguing that the trial court had misconstrued the Wiretap Act.[74] Specifically, Google contended that the district court erred in finding that Congress did not intend for "electronic communications," such as Wi-Fi, to be included in the narrow G1 exception for electronic communications "readily accessible to the general public."[75] The Ninth Circuit held that the phrase "readily accessible to the general public" in section 2510(16) with respect to a radio communication does not apply to the exemption for an "electronic communication" that is "readily accessible to the general public" under the G1 exemption.[76]

---

67. *In re Google*, 794 F. Supp. 2d at 1075.
68. *See* K Mart Corp. v. Cartier, Inc., 486 U.S. 281, 282 (1988).
69. Joffe v. Google, Inc., 746 F.3d 920, 924 (9th Cir. 2013) (citing *In re Google*, 794 F. Supp. 2d at 1076–81).
70. *Id.*
71. *Id.*
72. *In re Google*, 794 F. Supp. 2d at 1084.
73. *Id*.
74. *See generally Joffe*, 746 F.3d at 920.
75. *See In re Google*, 794 F. Supp. 2d at 1068.
76. *Joffe*, 746 F.3d at 926.

Further, the court determined that the ordinary meaning of "radio communication" does not include data transmitted over a Wi-Fi network and that the payload data transmitted over unencrypted Wi-Fi networks that was captured by Google is not predominantly auditory and is therefore outside of the section 2510(16) definition.[77] In essence, the Ninth Circuit ruling determined that intercepting Wi-Fi communications can violate the Wiretap Act.

E. Inconsistencies in the Courts

In affirming the district court's denial of Google's motion to dismiss, the Ninth Circuit examined the provisions of the Wiretap Act by looking to the plain language of the statute,[78] congressional intent,[79] and the statute as a whole.[80] The district court, in determining that Wi-Fi transmissions are not radio communications, acknowledged that the data on an open Wi-Fi network is only accessible in plain text via sophisticated technology.[81]

However, in a different case—*In re Innovatio IP Ventures, LLC Patent Litigation*—Judge Holderman of the United States District Court for the Northern District of Illinois ruled otherwise.[82] In that case, the district court granted Innovatio's Rule 16(c)(2) motion, holding that Innovatio's use of commercially available Wi-Fi network analyzers to collect information about the wireless network users' allegedly infringing Wi-Fi networks was legal and not in violation of the Wiretap Act.[83] Innovatio argued, and the court agreed, that the Wiretap Act does not apply because

---

77. *Id.* at 926–28.

78. *See id.* at 926–29 (defining the ordinary meaning of the phrase "radio communications" to be (1) predominantly auditory and (2) broadcast and holding that the payload data collected by Google over unencrypted Wi-Fi networks cannot be classified as predominantly auditory).

79. *See id.* at 927–28 (identifying similar terms in the Wiretap Act that Congress chose to provide definitions for and noting that Congress refrained from providing a technical definition of "radio communication" that would have altered the notion that it should carry its common, ordinary meaning).

80. *See id.* at 928–36.

81. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011).

82. *See generally In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888 (N.D. Ill. 2012); *see also* Mike Masnick, *Judge Says Sniffing Unencrypted WiFi Networks is Not Wiretapping*, TECHDIRT (Sept. 10, 2012, 7:15 AM), http://www.techdirt.com/blog/wireless/articles/20120907/16331020314/judge-says-sniffing-unencrypted-wifi-networks-is-not-wiretapping.shtml.

83. *In re Innovatio*, 886 F. Supp. 2d at 889–90. ("The packet capture adapter can intercept data packets that are traveling wirelessly between the Wi-Fi router provided by the Wireless Network Users and any devices that may be communicating with it, such as a customer's laptop, smartphone, or tablet computer. Innovatio then uses Wireshark network packet analyzer software to analyze the data packets, revealing information about the configuration of the network and the devices in the network. The data packets also include any substantive information that customers using the Wi-Fi network may have been

> even assuming that Innovatio's proposed protocol intercepts Wi-Fi communications, Innovatio's proposed protocol falls into the exception to the Wiretap Act allowing a person 'to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.'[84]

The court noted, however, that "an individual's online activity can be chilled merely by the knowledge that a third party has the power to acquire, however briefly, the contents of his communication."[85] Thus, the real issue is not "whether the *networks* are 'readily accessible to the general public,' but instead whether the network is configured in such a way so that the *electronic communications* sent over the network are readily available."[86]

Judge Holderman held that the proposed sniffing protocol is permissible under the G1 exception to the Wiretap Act and that "[a]ny tension between that conclusion and the public's expectation of privacy is the product of the law's constant struggle to keep up with changing technology."[87] Judge Holderman also held that the sniffing technology involved in this case did not amount, in his opinion, to "*sophisticated* packet sniffer technology."[88] However, the Ninth Circuit in *Joffe* held just

---

transmitting during the interception of the data packets, including e-mails, pictures, videos, passwords, financial information, private documents, and anything else a customer could transmit to the internet.").

84. *Id.* at 892 (quoting 18 U.S.C. § 2511(g)(i) (2006)).

85. *Id.* (quoting Amati v. City of Woodstock, 829 F. Supp. 889, 1008 (N.D. Ill. 1993) ("holding that the privacy interests of an individual whose conversations come under the power of another are implicated 'even if the individual was assured no one would listen to his conversations, because the individual's privacy interests are no longer autonomous'") and United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) ("acquisition occurs 'when the contents of a wire communication are captured or redirected *in any way*'" (emphasis added))).

86. *Id.* It is important to note that the court here was only considering the sniffing of "Public-facing Networks" and declined to address "whether Innovatio should be allowed to sniff the defendants' private networks that are not available to the public," which was a central issue in *In re Google* and other Google Street View litigation. *Id.* at 894, n. 6.

87. *Id.* at 894.

88. *Id.* at 893 (emphasis added).

> Moreover, upon examination, the proposition that Wi-Fi communications are accessible only with sophisticated technology breaks down. As mentioned above, Innovatio is intercepting Wi-Fi communications with a Riverbed AirPcap Nx packet capture adapter, which is available to the public for purchase for $698.00. *See Riverbed Technology Product Catalog*, http://www.cacetech.com/products/catalog/ (last visited Aug. 21, 2012). A more basic packet capture adapter is available for only $198.00. *Id.* The software necessary to analyze the data that the packet capture adapters collect is available for download for free. *See Wireshark Frequently Asked Questions*, http://www.wireshark.org/faq. html#sec1 (last visited Aug. 21, 2012) ("Wireshark® is a network protocol analyzer. . . . It is freely available as open source. . . ."). With a packet capture

the opposite, noting that "'radio hobbyists' do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks" and a definition of "radio communications" that encompasses data transmitted over Wi-Fi networks "would obliterate Congress's compromise [89] and create absurd applications of the exemption for intercepting unencrypted radio communications."[90]

Though *In re Innovatio* and *In re Google* approach the same issue from different angles and appear to have opposite holdings, the two cases contain a common message: "[I]t is not the court's job to update the law to provide protection for consumers against ever changing technology. Only Congress, after balancing any competing policy interests, can play that role."[91] The uncertainty present in the current state of the law is evidenced by the different approaches taken by the courts in trying to determine whether the interception of private information transmitted on unencrypted Wi-Fi networks is a violation of the Wiretap Act. This murkiness stands as a barrier to enforcement and must be remedied so that consumers continue to believe that new technologies are safe and that their private information is protected.

IV. FCC PRIVACY LITIGATION

The major purpose of the FCC is to protect the public interest, which includes protecting the privacy of consumers. However, the agency currently faces the problem of how best to protect the public interest within the limitations of the Wiretap Act. If consumers lose confidence in new technology for fear of invasion of their privacy—and therefore forego using such technologies—innovation will suffer.[92] In order to change this outdated and confusing area of law into a viable framework from which effective regulation can flow, the FCC and Congress must address whether

---

> adapter and the software, along with a basic laptop computer, any member of the general public within range of an unencrypted Wi-Fi network can begin intercepting communications sent on that network. Many Wi-Fi networks provided by commercial establishments (such as coffee shops and restaurants) are unencrypted, and open to such interference from anyone with the right equipment. In light of the ease of "sniffing" Wi-Fi networks, the court concludes that the communications sent on an unencrypted Wi-Fi network are readily available to the general public.

Id. at 393.

89. The Ninth Circuit noted that in order to address concerns by radio hobbyists that traditional radio services can be easily and mistakenly intercepted, Congress modified the original language of the Wiretap Act as a compromise. Joffe v. Google, Inc., 746 F.3d 920, 931 (9th Cir. 2013).

90. *Id.* ("It seems doubtful that Congress wanted to emphasize that Google or anyone else could park outside of a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity.").

91. *In re Innovatio*, 886 F. Supp. 2d at 894.

92. *See e.g.*, CASTRO, *supra* note 25, at 1–2; Gustin, *supra* note 25.

Wi-Fi networks are "readily accessible to the general public"[93] and how the Wiretap Act will be applied to emerging technologies going forward. In 2010, the FCC attempted to do just that.

A. Google Street View Litigation

In 2010, the FCC opened an investigation into Google after the company admitted publicly that from 2007 to 2010, as part of its Street View project, it had collected private user data from Wi-Fi networks throughout the United States.[94] This unauthorized collection of data, which was alleged to be a violation of the Wiretap Act, included sensitive "payload" data, which Google did not need for the purposes of its project.[95] This "payload" data included the content of users' Internet communications, specifically personal information such as "e-mails and text messages, passwords, Internet usage history, and other highly sensitive personal information."[96] Google Street View cars collected this personal information through "wireless sniffer" technology concealed in its cars, which was added by Google engineers to "secretly capture[] data packets as they stream across Wi-Fi connections and then decode[] or decrypt[] the data packet and analyze[] the contents."[97] At first, Google claimed it did not have knowledge of the addition of wireless sniffers to the Street View cars.[98] However, it was later alleged that other people at Google were aware of the wireless sniffers and the data they were collecting.[99]

By the time the European privacy authority opened its investigation against Google in 2010, Google admitted to collecting "about 600 gigabytes of data from more than 30 countries."[100] As discussed in Part III, serious privacy concerns also prompted a series of class action lawsuits in the United States, as well as in Europe and Australia, all alleging that Google used this "Wi-Fi sniffer" technology to eavesdrop on unsecured Wi-Fi networks and thus unlawfully intercept users' private data.[101]

---

93. 18 U.S.C. § 2511(2)(g)(ii) (2012).

94. *See Notice of Apparent Liability*, *supra* note 16, at para. 1.

95. *Id.*

96. *Id.*

97. *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011); *see generally* ANASTASI ET AL., *supra* note 11, at 150.

98. *See Unanswered Questions*, *supra* note 21.

99. *See id.*

100. *In re Google*, 794 F. Supp. 2d at 1071; *see also* Joffe v. Google, Inc., 746 F.3d 920, 923 (9th Cir. 2013).

101. *See Investigations of Google Street View*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/streetview/ (last visited Mar. 2, 2014) ("As of 2012, investigations have gone forward in at least 12 countries, and at least 9 countries have found Google guilty of violating their laws."). The FCC noted that "several countries, including Canada, France, and the Netherlands, have determined that Google's collection of payload data violated their data protection, online privacy, or similar laws and regulations." *See Notice of Apparent*

B. FCC Decision

The well-established threat to privacy that drove Congress to pass ECPA was exemplified in the 2010 FCC investigation of Google's Street View project. Intercepting sensitive payload data from users who believe their data to be private and secure falls within the spirit of ECPA and the privacy invasions it seeks to prevent. Although the interception of payload information from private and residential Wi-Fi networks clearly invades consumer privacy,[102] the FCC declined to charge Google with violating the Communications Act after determining that there was no "clear precedent for applying Section 705(a) of the Communications Act to the Wi-Fi communications at issue."[103] Additionally, the FCC lacked a significant evidentiary basis for applying the Communications Act to Google's conduct due to a software developer's refusal to testify based on his Fifth Amendment right against self-incrimination.[104]

The FCC opted to fine Google $25,000 for "willfully and repeatedly violating an Enforcement Bureau directive to respond to a letter of inquiry."[105] Thus, because Google failed to produce evidence regarding whether the payload information was reviewed or accessed after it was collected, and because the agency lacked a precedent for applying section 705(a) in the context of Wi-Fi, the FCC did not find a violation of section 705(a).[106] By nonetheless publicly reprimanding Google for its conduct in this manner, the FCC has given Congress another example of how the Wiretap Act has not kept up with advances in digital communications.[107]

C. Why Regulation of Interceptions of Information Transmitted over Unencrypted Wi-Fi Networks Is Important

Google faced even more litigation over its Street View Program when thirty-eight state attorneys general brought an action against Google

---

Liability, *supra* note 16, at para. 15. The European investigations found that these violations were serious and have taken the issue of data privacy in the private sector much more seriously as compared to the United States. *See FCC Investigation of Google Street View*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/google/fcc_investigation_of_google_st.html (last visited Mar. 2, 2014); *PBS NewsHour: How Will FCC's Google Street View Fine Shape Data Privacy Rules?* (PBS television broadcast Apr. 16, 2012), *available at* http://www.pbs.org/newshour/bb/law/jan-june12/google_04-16.html.

102. *See FCC Investigation of Google Street View*, *supra* note 107; *PBS NewsHour*, *supra* note 101.

103. *Notice of Apparent Liability*, *supra* note 16, at para. 5.

104. *See id.*; *see also* David Kravets, *Contradicting a Federal Judge, FCC Clears Google in Wi-Fi Sniffing Debacle*, WIRED (Apr. 16, 2012, 6:41 PM), http://www.wired.com/threatlevel/2012/04/fcc-clears-google/.

105. *Notice of Apparent Liability*, *supra* note 16, at para. 54.

106. *Id.* at para. 53.

107. *See Unanswered Questions*, *supra* note 21.

for its violation of consumer privacy.[108] In a settlement reached by the parties, Google agreed to pay a $7 million fine to the states involved, to set up a privacy program, to hold an annual privacy week event for employees, to make privacy certification programs available to select employees, to provide refresher training for its lawyers overseeing new products, and to train its employees who deal with privacy matters.[109] A large part of the settlement involves outreach in the form of educational advertisements and educating the public as to how to encrypt their data on their wireless networks.[110] This settlement signifies the interest of the states' attorneys general in protecting the privacy rights of Internet users as information sharing technology evolves and their willingness to prosecute violations.[111]

The settlement, however, once again demonstrates the insufficiency of the current state of the law. Critics expressed skepticism about the efficacy of the settlement, voicing concerns that it will not make much of a difference in how Google behaves."[112] Bolstering these doubts, Google has made similar educational promises before, yet it continues to be involved in litigation over its privacy practices.[113] This $7 million dollar settlement is a trivial amount for the company, given its net income in 2013 of around $32 million per day.[114]

Even more troublesome, the *Innovatio* court effectively granted permission under the Wiretap Act to hackers and other malicious actors to *legally* use packet sniffing technology similar to that used by Google in its Street View Program to access personal passwords, financial records, and other sensitive information from unencrypted Wi-Fi networks.[115] The myriad of decisions and agreements coming from the FCC, the courts, and the states have only contributed to the unsettled state of the law. Although individuals harmed by the interception of their unencrypted Wi-Fi communications may be able to maintain causes of action based on common law and other statutes,[116] the Wiretap Act is uniquely in its clear-

108. *See* Press Release, George Jepsen, Office of the Attorney Gen., Attorney General Announces $7 Million Multistate Settlement with Google Over Street View Collection of WiFi Data (Mar. 12, 2013) [hereinafter Jepsen Press Release], *available at* http://www.ct.gov/ag/cwp/view.asp?Q=520518.

109. *See id.*

110. *Id.*

111. *Id.*

112. *Concern for Privacy*, *supra* note 24.

113. *Id.*

114. David Streitfeld, *Google Concedes that Drive-By Prying Violated Privacy*, N.Y. TIMES, Mar. 13, 2013, at A1, *available at* http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html [hereinafter *Drive-By Prying*].

115. *In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012).

116. *E.g.*, 18 U.S.C. § 1030 (2012) (criminalizing the act of knowingly accessing a protected computer without authorization or in excess of authorized access); RESTATEMENT (SECOND) OF TORTS § 652B (1977 & Supp. 2014) (imposing tort liability on the intentional, offensive intrusion upon the seclusion of another).

cut and consistent applicability to unauthorized interception of communications not intended to be made publicly available.

Technological innovation will suffer if consumers are unwilling to buy cutting-edge products for fear that their private information will be compromised. If information is legally accessible to anyone willing to purchase the technology needed to intercept private data from Wi-Fi networks, consumer privacy will suffer. Congress has attempted to update privacy protections in response to technological innovation multiple times through legislative endeavors such as the Telecommunications Act and ECPA.[117] Through ECPA, Congress sought to ensure that the "readily accessible to the general public" exception to the Wiretap Act included only those communications in which the operator makes it clear, through the volitional configuration of their device, that they intend that their communications be public.[118] It is inconsistent with the intent of ECPA to imagine that the operator of a wireless home network intends that their network be accessible to the general public,[119] so courts should not impute this intent on unsuspecting private network owners.

Although most consumers encrypt and protect their private Wi-Fi communications, many other consumers either do not know how to do so or do not realize the risk they are taking by failing to affirmatively act to protect their data. Google's new obligation to educate the public about data encryption is a step in the right direction,[120] but the privacy risk is far too severe for Congress to leave the statutory framework in its current, ambiguous form. The courts have attempted to protect users' rights and impose liability for privacy infringement. The FCC has also looked at the statutory framework and attempted to clarify this murky area of the law, for the most part to no avail.

V. A CALL FOR CONGRESSIONAL ACTION

The conflicting rulings and difficulties expressed by the courts and the FCC are evidence that Congress must clarify and provide an enforcement mechanism for the FCC and the judiciary to use in order to further the goals of the Communications Act and the Wiretap Act. Although challenges will arise in determining exactly where to draw the line between a reasonable expectation of privacy and communications that are readily accessible to the general public, a clear boundary is necessary so that the FCC and the judiciary have a clear understanding of and consistently apply the law going forward.

---

117. *See id.* at 9; *see also In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount purpose of the Wiretap Act is to protect effectively the privacy of communications.").

118. *See id.*

119. *Id.*

120. Jepsen Press Release, *supra* note 108.

To interpret this convoluted area of law, the FCC and the judiciary have relied primarily on statutory language and legislative intent, with little case law to guide them.[121] Today's outdated statutes create confusion and unpredictability in regulation, ultimately allowing an unsuspecting consumer's privacy to be violated legally.[122] On the one hand, the *In re Google* court suggested that Wi-Fi communications are not readily accessible to the general public, even if they are sent unencrypted.[123] Similarly, the FCC discussion of the Wiretap Act and current lack of evidence from Google in its investigation of the Street View Project implies that if the agency had information showing that Google intended to intercept the contents of Wi-Fi networks, the agency could construe the Wiretap Act as applying to such interceptions.[124] On the other hand, the *In re Innovatio* court ruled the opposite, holding that the technology needed to intercept the communications was not "sophisticated" enough to make the communications non-public.[125]

Legal scholars have taken to the blogs to speak out against all three of these decisions. For example, legal scholar Orin Kerr disagrees with Judge Holderman's reasoning in the *In re Innovatio* case, noting,

> No one suggests that unsecured wireless networks are set up with the goal that everyone on the network would be free to read the private communications of others. In my view, that ends the matter: the exception doesn't apply, and the interception of the contents of wireless communications is covered by the Wiretap Act.[126]

Kerr argues that the issue under G1 "is what the designers [of the network] intended users to be able to do, not what someone can do contrary to the designer's intentions."[127] Others point to the fact that the necessity of

---

121. *See e.g.*, *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1074 (N.D. Cal. 2011) (examining novel question of statutory interpretation and relying instead on legislative intent as a result of ambiguous statutory language as applied to new technology).

122. *But see supra* note 116.

123. *Id.*

124. *See generally Notice of Apparent Liability*, *supra* note 16.

125. *In re Innovatio*, 886 F. Supp. 2d at 893.

126. Kerr, *supra* note 56 (arguing that "'configured so that such electronic communication is readily accessible to the general public' focuses on the intent of the designer—the person who does the configuring of the network so that it works a particular way—to design the network so that the general public was supposed to be able to access them.").

127. *Id.* (discussing *In re Innovatio*, 886 F. Supp. 2d at 888); *but see* Brief for Elec. Privacy Info. Ctr. as Amicus Curiae Supporting Plaintiffs at 3, *In re Google*, 794 F. Supp. 2d 1067 (No. 5:10-md-02184-JW) ("The term 'configured' in the evaluation of those communications that are 'publicly accessible' reflects an intent by Congress to create a presumption in favor of confidentiality except in those circumstances where the *user* has knowingly chosen to broadcast communications to the general public." (emphasis added)).

specialized or sophisticated equipment to decode the intercept should not be a factor in its legality.

Many legal scholars have framed Google's conduct as a prime example of a failing statute in need of congressional attention. In an interview with PBS, legal scholar Jeffrey Rosen discussed Judge Ware's holding in *In re Google*, noting,

> [T]here's a strong case that this is illegal under existing law. Certainly, if it's not, it should be. And the fact that the FCC chose not to investigate shouldn't [be] seen as a clean bill of health for Google, because every other European regulator that has looked into this question has found unequivocal violations.[128]

This call to action to update the law is long overdue. By enacting ECPA in 1986, Congress sought to encourage the creation of new technologies by preserving "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[129] Now, twenty-eight years later, it is time for Congress to again pass an amendment to the Communications Act to expressly permit the FCC to impose liability to protect private information shared through new technologies that have emerged in the last three decades. Historically, Congress has done this by amending the Communications Act to accommodate the dramatic changes in communications technology that have taken place since the FCC's creation, including the introduction of television, satellite and microwave communications, cable television, the cellular telephone, and Personal Communications Services.[130]

Recently, former FCC Chairman Julius Genachowski recommended an amendment to the Communications Act during the hearing on the fiscal year 2013 FCC budget, and Senator Dick Durbin (D–IL) said that he would consider changes to the law if that is the necessary course of action.[131] Senator Durbin criticized the FCC for "decid[ing] to impose a fine of $25,000 on a company worth $111 billion," noting that the small fine is

---

128. Interview by Ray Suarez with James Rosen, Professor of Law, The George Washington Univ. Law Sch., and David Bennahum, Founder & CEO, Punch! Media (Apr. 16, 2012), *available at* http://www.pbs.org/newshour/bb/law/jan-june12/google_04-16.html.

129. H.R. REP. NO. 99-647, at 19 (1986); *see also* J. BECKWITH BURR, WILMERHALE, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986: PRINCIPLES FOR REFORM 1 n.3 (Mar. 30, 2010), *available at* http://digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

130. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–21 (1988).

131. *See generally Hearing on Expanding Broadband Access, Promoting Innovation, and Protecting Consumers in a Communications Revolution: FY 2013 Resource Needs for the FCC Before the Subcomm. on Fin. Servs. & Gen. Gov't of the S. Comm. on Appropriations*, 112th Cong. (2012) [hereinafter *FY 2013 Appropriations Hearing*] (hearing beginning at 32:20), *available at* http://www.appropriations.senate.gov/webcasts.cfm?method=webcasts.view&id=4eade537-0f2b-4280-84fa-c3a2bf8ded89.

"somewhere short of a tap on the wrist."[132] Genachowski explained that the FCC Enforcement Bureau and the General Counsel's office decided that, as a legal matter, because the information was collected from unencrypted Wi-Fi signals, it did not violate the law as written. The former Chairman suggested that Congress look at the law and that consumers encrypt their networks.[133] However, the FCC and the courts have reached opposite conclusions regarding the application of the Wiretap Act to unencrypted Wi-Fi networks. It is time that Congress clarifies the issue.

Congress should amend the Wiretap Act and Communications Act to clarify that private communications are protected regardless of their underlying technology so long as they are not intentionally configured to be "readily accessible to the general public." This amendment must allow for the imposition of liability for privacy violations involving new technology, thus ensuring that privacy protections are not eroded in the near future as technology continues to evolve. Congress should amend the Wiretap Act to expressly exclude Wi-Fi networks and similar technologies from the definition of radio communications, thus ensuring that these technologies are not included in the Wiretap Act's G1 exception for electronic communications readily accessible to the general public. This would make collection of information over Wi-Fi networks a violation of the Wiretap Act, regardless of whether the consumer acted to encrypt their network—subject only to the exceptions in G2. Congress should also include in the amendment a technology neutral explanation of this provision to address the intent of the amendment and the need for the provisions to evolve in accordance with technology.

Additionally, Congress should also change the definition of "readily accessible to the general public"[134] in section 1510(16) to better protect consumer privacy. This amendment should clarify that the legality of intercepting personal information over a Wi-Fi network does not depend on whether the Wi-Fi network is encrypted. Congress must draw a clear line between protected and unprotected communications so that consumers can more effectively protect themselves. Congress, through the Communications Act and the Wiretap Act, should protect private communications transmitted on private networks, encrypted or unencrypted, just as communications by telephone are protected even if transmitted insecurely. Thus, it should be illegal for persons to intercept data transmitted over a Wi-Fi network.

---

132. *See generally id.*

133. *See generally id.* (adding that the "educational purposes that have been served by this [FCC investigation], educating [Google] and other companies, educating Congress, [and] educating consumers, [are] certainly important benefits of [the] process."); *see also On Google Spy-Fi, Senator Durbin Calls for Update to Wiretap Law, FCC Chair Agrees Law Should Protect Unencrypted Communications*, ELEC. PRIVACY INFO. CTR. (May 11, 2012), http://epic.org/2012/05/on-google-spy-fi-senator-durbi.html.

134. 18 U.S.C. § 2510(16) (2012).

An interesting line drawing issue arises in the context of public versus private networks when defining the term "readily accessible to the general public" line. Public "Wi-Fi Hotspots," which are hotspots in places of public accommodation such as hotels, restaurants, and Starbucks, have become common throughout the world and should perhaps be treated differently than private residential networks. Users connecting to Wi-Fi hotspots in public places may not have the same expectation of privacy as users of residential networks; however, their communications should arguably still be protected. The data transmitted over both public and private networks is most often sent with an expectation that unauthorized parties will not collect or use the data. Naiveté should not warrant an invasion of privacy.

There are many approaches Congress could take to clarify the regulatory framework. If Congress were to exclude "public-facing networks" from Wiretap Act liability, hackers using sniffer technology would have the ability to *legally* access personal information and search history through the Wi-Fi connection and access personal data that can then be used for purposes contrary to the protections provided by the Wiretap Act.[135] Therefore, any exclusion regarding public-facing networks would need to be counterbalanced by consumer education programs designed to teach the public which types of networks are open and which provide protection for their private information. Neither approach is obviously more logical or fair than the other, but whether there is an exception for public-facing Wi-Fi hotspots is not as important as drawing a clear line. It is more important that the issue be settled than that it be settled in a particular way because, presently, consumers have a false sense of security on their networks—and the FCC and the judiciary have a morass of law they must untangle before protection can be provided. To encourage innovation, Congress must also encourage consumer confidence and trust in new technology.

VI. FCC PRIVACY AUTHORITY AND DUE PROCESS

Updating the Wiretap Act is necessary, and it will likely occur at some point—though the precise timeline is uncertain. In the meantime, however, the FCC faces the problem of how to administer the Wiretap Act to best protect users' Wi-Fi networks and prosecute hackers who collect and use private information. Regardless of the prospect of congressional action, the FCC should take to its interpretative powers to address the growing privacy concerns of the public.

Although many of the terms in the Wiretap Act are defined in the statute, those definitions have been expanded through FCC litigation and policy statements throughout the years. Title I of the Communications Act

135. *But see supra* note 116.

grants the FCC the authority to make policy through case-by-case adjudication, in addition to its rulemaking procedures.[136] This power is limited by the Due Process Clause of the Fifth Amendment as incorporated into administrative law, which prohibits the FCC from penalizing a person who has not been given adequate notice that their conduct violates a particular policy.[137] Nonetheless, the FCC is authorized to make policy decisions through adjudicatory proceedings even when applying statutory language to a new technology as a matter of first impression so long as the FCC complies with the due process notice requirement.[138]

A. Statutory Authority to Act

The FCC has the power under the Administrative Procedures Act ("APA") to engage in statutory interpretation through both adjudication and rulemaking.[139] Since the Communications Act authorizes the FCC to engage in adjudicatory proceedings but does not require that they be "on the record," the FCC is free to engage in adjudication subject only to the modest procedural restraints in APA section 555.[140] When an agency's adjudication relies on its interpretation of ambiguous terms in its enabling statute, the reviewing court will defer to the agency's reasonable interpretation of the statute.[141] The FCC may also act through notice and comment rulemaking, by issuing interpretative rules, and by issuing policy statements.[142]

The FCC is also constrained by constitutional limitations. Specifically, the FCC does not have the power to impose legal consequences without adequate notice at the time of the violation.[143] This presents an obstacle to case-by-case expansion of the Wiretap Act to include new technologies as they arise.

B. FCC Action: A Step by Step Plan

The FCC has the power to address the meaning of the Wiretap Act to protect consumer privacy in the absence of congressional action. Pursuant to the APA and the FCC's enabling statute, the Communications Act, the

136. *See* 47 U.S.C. § 151 (2006).
137. *See* Satellite Broadcasting Co., Inc. v. FCC, 824 F.2d 1, 3 (D.C. Cir 1987).
138. *See* SEC v. Chenery Corp., 332 U.S. 194, 203 (1947).
139. *See* 47 U.S.C. § 154(i) (2006); *see also* Aaron K. Brauer-Rieke, Note, *The FCC Tackles Net Neutrality: Agency Jurisdiction and the Comcast Order*, 24 BERKELEY TECH. L. J. 593, 599–601 (2009).
140. *See* 47 U.S.C. § 154(i) (2006).
141. Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842–44 (1984).
142. *Rulemaking Process at the FCC*, FCC ENCYCLOPEDIA, http://www.fcc.gov/encyclopedia/rulemaking-process-fcc (last visited Mar. 2, 2014).
143. *See* FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012).

FCC has the power to issue its own rules and regulations in order to further the provisions of the Act. The FCC may do this in one of three ways: (1) legislative rulemaking; (2) interpretive rulemaking and policy statements; or (3) case-by-case adjudication.

1. Legislative Rulemaking

The FCC's first option is to issue a Notice of Proposed Rulemaking and begin the process of issuing a legislative rule. The Communications Act grants the FCC the power to issue legislative rules through its broad grant of rulemaking power necessary to carry out the provisions of the Act.[144] Through "notice and comment" rulemaking, the FCC can propose a new interpretation of the Wiretap Act in order to correct a problem the agency has identified, such as "industry behavior that adversely affects consumers."[145] As in the case of Wi-Fi network regulation, the FCC "may have difficulties enforcing existing rules and this may provide evidence of a need to modify the rules . . . [o]r, changes in technology may suggest that it is time to update a rule."[146]

The FCC could issue a rule clarifying that unencrypted Wi-Fi networks do not fall under the "readily accessible to the general public" exception of 18 U.S.C. § 2511(g)(i).[147] The Wiretap Act's goal of protecting consumers and their private information provides a justification for an FCC interpretation of the statute to include a prohibition on the interception of data not that was not intended to be public.[148] A legislative rule would have the force of law and would allow the FCC, the expert agency most familiar with the issues at stake, to determine exactly where the "readily accessible to the general public" line should be drawn.[149]

2. Interpretive Rulemaking and Policy Statements

Additionally, the FCC could issue an interpretive rule or policy statement. Although this option would not create any binding legal effect, it

144. *See* 47 U.S.C. § 154 (2006).

145. *Rulemaking Process at the FCC*, *supra* note 142.

146. *Id.*

147. *See* 18 U.S.C. § 2511(g)(i) (2012).

148. *See* 18 U.S.C. § 2510 (2012); *see Konop*, 302 F.3d at 875 ("The legislative history of the [Wiretap Act] suggests that Congress wanted to protect electronic communications that are configured to be private, such as email."); *also In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.").

149. *See Rulemaking Process at the FCC*, *supra* note 142. However, a legislative rule passed through the notice and comment rulemaking procedure would not assist the FCC in addressing the issue at hand in the immediate future because the notice and comment procedure can take years to complete.

provides an instrument to interpret the binding statute and clarify the scope of pre-existing rights and duties.[150]

Pursuant to APA section 553(b), "interpretive rules, general statements of policy, or rules of agency organization, procedure, or practice" are all categories of rules that are exempt from procedural requirements, meaning the FCC can avoid the extensive notice and comment rulemaking procedures mandated by the APA for formal rulemaking and still succeed in putting the public on notice that they plan to exercise their jurisdiction under the statutes.[151] By declaring that the provisions of the Wiretap Act regarding unlawful interception of data seriously pre-date the current wireless Internet technologies available today, the FCC could interpret the plain language of the statute to give protection to data transmitted over Wi-Fi networks, thereby enabling the FCC to carry out the legislature's intent to protect the public interest.[152]

3. Case-by-Case Adjudication

Another means by which the FCC has the power to regulate interceptions of electronic and radio communications is on a case-by-case adjudicatory basis. Through adjudications, the FCC can exercise its enforcement jurisdiction as a Title I regulatory regime and place the public on notice of its interpretation of the Communications Act and its provisions as amended.

As discussed above, before the FCC can expand existing policies and regulations, it must first provide adequate notice as to what actions constitute violations of existing policies. An agency may not impose civil or criminal penalties when neither the regulation nor the Commission's related statements gave fair notice of that requirement.[153] The FCC order in *Google Street View* can be read as a warning to those that intercept data on Wi-Fi networks, and could thus have major implications for Internet users and companies gathering data both actively and passively.[154] Although the FCC declined to enforce the Wiretap Act against Google, the FCC extended the Wiretap Act to include data interception from unencrypted Wi-Fi networks.[155] The FCC explained in its *Notice of Apparent Liability for Forfeiture* that it declined to enforce section 705(a) of the Wiretap Act

150. *Id.*
151. *See* 5 U.S.C. § 553(b) (1966).
152. *See infra* Part III.A; *see also In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1076 (N.D. Cal. 2011) (citing 18 U.S.C. § 2511(5)(a)(i)(B) (2006)) (noting "the lack of any explicit reference to wireless internet technologies does not itself preclude an interpretation of 'radio communications' that would include these later-developed technologies.").
153. *See, e.g.*, Trinity Bd. of Fla., Inc. v. FCC, 211 F.3d 618, 619 (D.C. Cir. 2000).
154. *See generally Notice of Apparent Liability*, *supra* note 16.
155. *See id*. at para. 52.

against Google because it lacked both information[156] and Commission precedent addressing the application of section 705(a) to Wi-Fi communications.[157] This rationale implies that, in the future, if the FCC has evidence that information was collected from unencrypted Wi-Fi networks, it could choose to take enforcement action.

At this point, the state of the law includes inconsistent decisions by courts and the FCC interpreting the same statutory provisions. Congress has the power to amend the Communications Act to either override or adopt any of these interpretations. The FCC, as the expert agency tasked with regulation of communications technology, is perhaps in the best position to issue rules that adapt to new and emerging technologies.[158] The conflicting holdings between the FCC and the judiciary are confirmation that it is time that Congress step in and update the statutes to fit the times.

VII. IMPLICATIONS FOR THE FCC, CORPORATIONS, AND CONSUMERS

The full implications of the FCC decision to fine Google and the subsequent class action decisions concerning Google Street View remain to be determined. The Wiretap Act was enacted in 1968 and amended by ECPA in 1986. As technology has since changed, so too should the FCC's interpretation of its jurisdiction under the Act. When faced with a violation of the Wiretap Act in the future, the FCC may hold an extensive adjudication in which it declares that the agency has authority to pursue the interception of data over unencrypted Wi-Fi networks as announced in *Google Street View* and may at that point define the scope of that power in an enforcement proceeding. Alternatively, as discussed above, the FCC may issue an interpretive rule in the meantime, expanding its interpretation of the Wiretap Act to include interceptions over unencrypted Wi-Fi networks as violations of the Act, in order to protect users who are concerned about the security of their Wi-Fi enabled communications.

The approaches taken by the FCC and Congress will soon be relevant not only as Google revamps its Street View project, but in other mapping projects as well. The new privacy programs Google has agreed to implement over the next ten years and the company's recent admission it invaded consumer privacy will affect many of the products Google sends out to the market, including its most recent product, Google Glass.[159] As

156. *See id.* at para. 53 ("The Bureau's inability to compel an interview of Engineer Doe made it impossible to determine in the course of our investigation whether Google did make any use of any encrypted communications that it collected.").

157. *Id.*

158. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 980 (2005) (holding the Commission is free within the limits of reasoned interpretation to change course if it adequately justifies the change).

159. *See Drive-by Prying*, *supra* note 114.

companies such as Apple and Google update their maps applications in the future, they will have to be especially careful to collect only authorized data, leaving the personal payload data behind. These companies should interpret the Google Street View litigation at the FCC and in the courts to as a warning that any interceptions of unencrypted Wi-Fi networks may violate the Wiretap Act. In addition, educating consumers so that they have a realistic idea of how easy it is to become a victim of Wi-Fi sniffers should be a priority for both Congress and the FCC moving forward.

VIII. CONCLUSION

In the last decade, the world has seen incredible advancements in communications technology and witnessed how entrepreneurship and innovation can spur economic growth.[160] Unfortunately, the laws governing communications interception in the United States are seriously outdated. The FCC, the judiciary, legal scholars, and the public have all called upon Congress to update the Wiretap Act in order to accommodate innovation in communications technology. To further the public interest, the FCC should encourage technological innovation while ensuring the safety and privacy of consumers. For the FCC to effectively carry out this mission, Congress should amend the Wiretap Act to clarify the definition of radio communications so that Wi-Fi networks and other new technologies carry the privacy protections of the Wiretap Act, whether or not their transmissions are encrypted. In the meantime, the FCC should interpret the Wiretap Act to include this unencrypted Wi-Fi communication by exercising the broad rulemaking powers granted to it by the Communications Act. In addition, the FCC's decision in *Google Street View* constitutes notice that the FCC can take enforcement action against interceptions of data over Wi-Fi networks—including unencrypted networks—to protect the public and its privacy in future adjudications. Unfortunately, the FCC can only stretch the Communications Act so far; the rest is up to Congress.

When a crisis emerges in the United States, Congress should look to the underlying causes of that crisis and seek a solution that benefits the country as a whole. The current privacy crisis in the United States is a result of outdated statutes and new technology. Unfortunately, only one of these two phenomena can survive—either Congress updates the Communications Act to keep up with technology, or consumers will lose faith and trust in technology, causing innovation in the United States to experience a decline. The time to act is now.

---

160. *See generally FY 2013 Appropriations Hearing*, *supra* note 131 (statement of Sen. Moran, Member, S. Comm. on Appropriations).