"I'LL HAVE A LATTE, SCONE, AND YOUR ONLINE DATA, PLEASE"

STEVE MARTYN

INTRODUCTION

Jane walks into her local coffee shop. She orders a drink, then sits at her usual table and opens her laptop. The coffee shop offers free Wi-Fi, and over the next 90 minutes Jane reads some e-mails, downloads some pictures, and checks the balance of her bank account.

Meanwhile, another patron sits quietly in the coffee shop with his own laptop. He's not surfing the web or watching YouTube videos. Instead, he's using a combination of hardware and software to capture data as it is transmitted on the coffee shop's unencrypted Wi-Fi network. He is not a hacker or an identity thief. He is an employee of an intellectual property company that holds patents on Wi-Fi technology, patents the company believes are being violated by the coffee shop and

other businesses. The only way to prove infringement is to gather data about the coffee shop's network, a process that incidentally captures other information like Jane's e-mail password and financial information. Jane eventually leaves the coffee shop, never knowing that her online privacy was compromised.

Jane's situation is not just a cautionary tale about the vulnerability of private information on unencrypted Wi-Fi. In August 2012, the United States District Court for the Northern District of Illinois ruled on the admissibility of information collected from the wireless networks of hotels, coffee shops, restaurants, and other businesses.[1] The information is part of a patent infringement lawsuit launched by Innovatio IP Ventures, LLC (hereinafter "Innovatio").[2] The court's decision highlights a gaping hole in online privacy that many internet users are unaware of.

Part I of this note provides an overview of wireless internet technology. It will explain how that technology has been standardized by the Wi-Fi Alliance, a nonprofit organization comprised of technology companies. It will also review wireless encryption standards.

Part II describes Innovatio and its wireless internet technology patents. This section will explain how Innovatio obtained those patents and how it has defended them through litigation. Part III focuses on an evidentiary ruling arising from Innovatio's patent litigation. The section will describe how Innovatio "sniffed" the unencrypted Wi-Fi networks of numerous businesses and captured information about the online activities of patrons in the process. This section will also describe how the court found Innovatio's actions to fall within an exception to a privacy law, the federal Wiretap Act.

Part IV will survey federal privacy laws. These include the Fourth Amendment, the original Wiretap Act of 1968, and the updates made to the Wiretap Act by the 1986 Electronic Communications Privacy Act. Section IV will also briefly recite the shortcomings of the Wiretap Act.

Part V begins with analysis of the implications of the *Innovatio* decision. These implications include the unethical use of patrons' online data by businesses, warrantless surveillance of patrons using unencrypted Wi-Fi by federal and state law enforcement, and the risk of hackers. This section will then examine four ways to address the privacy gap identified by *Innovatio*. These include Congressional updates to the Wiretap Act or regulation of the Wi-Fi industry, state action to protect online privacy, implementation of new encryption standards by the Wi-Fi industry, and judicial interpretation of the Wiretap Act that removes unencrypted Wi-Fi from the law's exception language.

1. *In re* Innovatio IP Ventures, 886 F.Supp.2d 888, 890 (N.D. Ill. 2012).
2. *Id.*

Finally, Part VI will review the solutions outlined above and recommend the best way to protect the privacy of data sent over unencrypted Wi-Fi. Thanks to the availability of Wi-Fi encryption standards and an ongoing shift toward simplified encryption, new industry standards are the most promising solution.

I. WI-FI: STANDARDIZING WIRELESS LOCAL AREA NETWORKS

When a patron walks into a coffee shop and wirelessly accesses the internet on their tablet or smartphone, they probably are not thinking about the different steps making that access possible. First, the patron's device connects to a wireless router, which is broadcasting a radio signal. When the patron's device connects to this radio signal, the device is routed to a connected modem. The modem, by means of a high-speed connection, allows the patron to access the internet, which is provided by an Internet Service Provider, or ISP. This entire network of a wireless router, modem, and connection to an ISP is a wireless local area network, or WLAN.[3]

The term "Wi-Fi" is used in common parlance to refer to WLAN, but it is more than a generic term for wireless internet. Wi-Fi, short for wireless fidelity,[4] is a term indicating the interoperability of products ranging from wireless routers to smartphones, tablets, and computers.[5] Wi-Fi encompasses a set of standards for wireless networking that was first developed in 1997 by the Institute of Electrical and Electronics Engineers,[6] or IEEE (pronounced "Eye-triple-E").[7] The first set of standards was known as IEEE 802.11.[8] These standards have been updated as new wireless technology is developed. For example, IEEE 802.11b amended the original standards in 1999. It specifies a radio signal broadcast at a frequency of 2.4 GHz and has a maximum data rate of 11 megabits per second. The 802.11b standard became "the definitive

3. *See What is WiFi®?*, WISEGEEK, http://www.wisegeek.org/what-is-wifi.htm (last visited Oct. 1, 2014).

4. Press Release, Wi-Fi Alliance, Six Wi-Fi Interoperability Certifications Awarded By The Wireless Ethernet Compatibility Alliance (WECA) (July 19, 2000) *available at* https://www.wi-fi.org/news-events/newsroom/six-wi-fi-interoperability-certifications-awarded-wireless-ethernet.

5. *See generally Wi-Fi Certified Makes it Wi-Fi: What Retailers Need to Know*, WI-FI ALLIANCE, http://www.wi-fi.org/file/wi-fi-certified™-makes-it-wi-fi®-what-retailers-need-to-know-2009 (last visited Oct. 1, 2014).

6. *Wireless LAN 802.11 Wi-Fi*, IEEE GLOBAL HISTORY NETWORK, http://www.ieeeghn.org/wiki/index.php/Wireless_LAN_802.11_Wi-Fi (last visited Jan. 31, 2014).

7. *About IEEE*, IEEE, http://www.ieee.org/about/index.html (last visited Jan. 31, 2014).

8. IEEE GLOBAL HISTORY NETWORK, *supra* note 6.

wireless LAN technology" in the early years of WLAN.[9]

More recent standards include 802.11g, ratified in 2003, and 802.11n, enacted in 2004.[10] The 802.11n standard has been updated since 2004 and provides data rates of up to 600 megabits per second[11] and radio frequencies at 2.4 GHz, 5 GHz, or both.[12] A new standard, IEEE 802.11ac, was introduced in 2014[13] and provides data rates of up to a gigabit per second.[14] Some predict there will be up to a billion 802.11ac-compatible devices on the market by 2015.[15]

When a product is designed to comply with an IEEE 802.11 standard, it is tested by a nonprofit organization called the Wi-Fi Alliance. Founded in 1999,[16] the Wi-Fi Alliance embraced IEEE 802.11 and sought to unify WLAN behind it. The Wi-Fi Alliance today boasts hundreds of member companies including Apple, Cisco, Motorola, and Microsoft,[17] and has certified over 15,000 products since 2000 that meet the various IEEE 802.11 standards.[18] The Wi-Fi Alliance tests products "for interoperability, security, and a range of application specific protocols."[19] Certified products are allowed to feature the Wi-Fi trademark.

Data broadcast between devices on a WLAN are vulnerable to interception by third parties. All Wi-Fi products include some form of data encryption to combat this vulnerability. The original IEEE 802.11 standard included an encryption mechanism known as Wired Equivalent Privacy (WEP). By 2001, studies revealed that WEP was flawed and left Wi-Fi networks vulnerable to intruders.[20] An interim encryption standard

9. *Id.*

10. *Id.*

11. Stephen Shankland, *Study: Expect a Billion 802.11ac Wi-Fi Devices in 2015*, CNET (Feb. 8, 2011, 5:44 AM), http://news.cnet.com/8301-30685_3-20030964-264.html?part=rss&subj=news&tag=2547-1_3-0-20.

12. *Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi Networks*, WI-FI ALLIANCE, https://www.wi-fi.org/file/wi-fi-certified%E2%84%A2-n-longer-range-faster-throughput-multimedia-grade-wi-fi%C2%AE-networks-2009 (last visited Oct. 1, 2014).

13. NEW IEEE 802.11AC™ SPECIFICATION DRIVEN BY EVOLVING MARKET NEED FOR HIGHER, MULTI-USER THROUGHPUT IN WIRELESS LANS, *available at* http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html.

14. Shankland, *supra* note 1111.

15. *Id.*

16. *Who We Are*, WI-FI ALLIANCE, https://www.wi-fi.org/who-we-are (last visited Jan. 31, 2014).

17. *Member Companies*, WI-FI ALLIANCE, http://www.wi-fi.org/who-we-are/member-companies (last visited Jan. 31, 2014).

18. *Become a Member*, WI-FI ALLIANCE, http://www.wi-fi.org/become-member (last visited Jan. 31, 2014).

19. *Certification*, WI-FI ALLIANCE, http://www.wi-fi.org/wi-fi-certified%E2%84%A2-products (last visited Feb. 24, 2013).

20. WI-FI ALLIANCE, WI-FI PROTECTED ACCESS: STRONG, STANDARDS-BASED,

called Wi-Fi Protected Access (WPA) was implemented by the Wi-Fi Alliance in 2003 while a permanent solution was developed by the IEEE.[21] In 2004, IEEE 802.11i was adopted, establishing a more robust encryption format known as WPA2.[22] As of 2006, the Wi-Fi Alliance requires certified products to include WPA2 encryption.[23]

Although Wi-Fi equipment is required to comply with WPA2 encryption, most Wi-Fi routers are "shipped with security disabled to make it very easy to set up [a] network."[24] The Wi-Fi Alliance estimates that setting up a home Wi-Fi network that includes WPA2 protection can take five to fifteen minutes. The person setting up the network must select a network name, or SSID, that identifies the network on devices like smartphones and tablets; enable WPA2 encryption and set a password that users enter before their device can connect to the router; and change the administrative credentials that are used to make further adjustments to the router's configuration.[25] Some routers include Wi-Fi Protected Setup, an option that simplifies encrypted network configuration.[26] In either case, however, the person setting up the network must proactively enable encryption.

II. PATENT POWER: INNOVATIO'S PATENT INFRINGEMENT LAWSUITS

Innovatio is a Delaware corporation that commands a mixed reputation in the intellectual property community.[27] Innovatio does not sell products, but "is in the business of enforcing and licensing patents."[28] Its portfolio consists of 31 patents covering wireless internet technology.[29] One patent litigator described Innovatio as a company

INTEROPERABLE SECURITY FOR TODAY'S WI-FI NETWORKS (hereinafter "*White Paper*") (Apr. 29, 2003), *available at* http://www.ans-vb.com/Docs/Whitepaper_Wi-Fi_Security4-29-03.pdf.

21. *Id.*

22. IEEE GLOBAL HISTORY NETWORK, *supra* note 6.

23. *The State of Wi-Fi Security: Wi-Fi Certified WPA2 Delivers Advanced Security to Homes, Enterprises and Mobile Devices*, WI-FI ALLIANCE, http://www.wi-fi.org/file/the-state-of-wi-fi%C2%AE-security-wi-fi-certified%E2%84%A2-wpa2%E2%84%A2-delivers-advanced-security-to-homes (last visited Oct. 1, 2014).

24. *Security*, WI-FI ALLIANCE, http://www.wi-fi.org/discover-wi-fi/security (last visited Jan. 31, 2014).

25. *Id.*

26. *Id.*

27. Gregory Thomas, *Innovatio's Infringement Suit Rampage Expands to Corporate Hotels*, PATENT EXAMINER BLOG (Sept. 30, 2011, 6:00 AM), http://patentexaminer.org/2011/09/innovatios-infringement-suit-rampage-expands-to-corporate-hotels/.

28. Complaint at 2, Cisco Systems, Inc. et al. v. Innovatio IP Ventures, LLC, No. 1:11-CV-425 (D. Del. May 13, 2011).

29. Thomas, *supra* note 27.

seeking to enforce legitimate patents through legal means,[30] while a writer for Law Technology News branded Innovatio as an "infamous patent troll."[31]

Innovatio's patents were developed during the 1990s and 2000s.[32] Some of those patents trace back to the work of Robert Meier and Ronald Mahany, the "Fathers of Radio Frequency Local Area Networking Technology."[33] These patents were originally owned by Broadcom, a major communications technology company, but were eventually transferred to Innovatio in February 2011.[34]

Within months of receiving the patents, Innovatio launched a salvo of lawsuits against businesses allegedly infringing its wireless internet patents. Instead of pursuing wireless router manufacturers, Innovatio targeted "users, such as hotels, bakeries, cafes, and grocery stores."[35] It appears all of these companies were using Wi-Fi products to provide wireless internet to their patrons.[36] Innovatio probably targeted users instead of Wi-Fi technology companies because it could potentially extract licensing fees from every business it sued without actually going to trial.[37] Moreover, this strategy could reduce the risk of head-to-head litigation against major companies who have experience defending patents in court.[38]

The scope of Innovatio's lawsuits has expanded since 2011, with defendants now including Starbucks, Barnes & Noble, Caribou Coffee, Cosí, Panera Bread, Marriott Hotels, Best Western, and an array of

30. Raymond P. Niro, *Setting the Record Straight on the Innovatio Patent Portfolio*, IPWATCHDOG BLOG (Mar. 21, 2012, 3:41 PM), http://www.ipwatchdog.com/2012/03/21/setting-the-record-straight-on-the-innovatio-patent-portfolio/id=22964/.

31. Brendan McKenna, *Innovatio: Attack of the Wi-Fi Patent Troll*, LAW TECH. NEWS (Oct. 6, 2011), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202517839522.

32. Complaint at 4–7, Innovatio IP Ventures, LLC v. Comfort Inn O'Hare et al., No. 1:11-CV-6481 (N.D. Ill. Sept. 16, 2011).

33. Niro, *supra* note 3030.

34. Thomas, *supra* note 27.

35. Innovatio IP Ventures, LLC v. MEI-GSR Holdings, LLC, No. 3:11-CV-00343-LRH-WGC, 2011 WL 6812541, at *1 (D. Nev. Dec. 27, 2011).

36. *See In re* Innovatio IP Ventures, 886 F.Supp.2d 888, 889 (N.D. Ill. 2012).

37. Mike Masnick, *Cisco, Motorola, Netgear Team Up To Expose Wifi Patent Bully*, WIRELESS NEWS BLOG (Oct. 9, 2012, 12:35 pm), http://www.techdirt.com/blog/wireless/?company=innovatio (last visited Feb. 22, 2014).

38. For example, Wi-Fi technology company Cisco Systems holds over 2,500 U.S. patents. *Patent Reform*, CISCO SYSTEMS, http://www.cisco.com/web/about/gov/issues/patent_reform.html (last visited Nov. 9, 2012). Additionally, Motorola recently fended off Apple's patent infringement lawsuit against it. Greg Sandoval, *Federal judge tosses Apple patent lawsuit against Motorola*, CNET (Nov. 5, 2012), http://news.cnet.com/8301-13579_3-57545283-37/federal-judge-tosses-apple-patent-lawsuit-against-motorola/.

others.[39] Despite Innovatio's user-focused strategy, Cisco and Motorola, who manufacture Wi-Fi routers, returned fire by seeking a declaratory judgment that their products do not infringe any patents and that Innovatio's patents are invalid.[40] These various legal actions were eventually consolidated before the United States District Court of the Northern District of Illinois.[41]

III. A MATTER OF PRIVACY: THE *INNOVATIO* DECISION

A. "Sniffing"

As litigation proceeded, Innovatio asked the court to rule on the admissibility of evidence it had been collecting, evidence that it hoped would prove its patent infringement claims.[42] Innovatio was using a data collection process known as sniffing. It sent agents armed with laptops to the premises of the defendant businesses. The agents used packet capture adapters to intercept data as it traveled between the Wi-Fi routers and whatever devices were communicating with the routers (laptops, smartphones, etc.).[43] The agents would then decipher the data using packet analyzer software, "revealing information about the configuration of the network and the devices in the network."[44]

Incidentally, the data packets that Innovatio was capturing and deciphering also included users' data payload, or "any substantive information that customers. . .may have been 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."[45] The court agreed to rule on the admissibility of Innovatio's evidence, but ordered Innovatio to describe its sniffing protocol, warning that it might run afoul of the federal Wiretap Act, 18 U.S.C. §§ 2510-2522 (2012).[46]

B. The Federal Wiretap Act

On August 22, 2012, the court ruled on Innovatio's motion. The

39. Complaint, Innovatio IP Ventures, LLC v. Starbucks Corp., No. 12-CV-3872 (N.D. Ill. May 18, 2012); Complaint, Innovatio IP Ventures, LLC v. Barnes & Noble, Inc., No. 12-CV-3856 (N.D. Ill. May 18, 2012); Thomas, *supra* note 27.

40. Thomas, *supra* note 27; Complaint at 1, Cisco Systems, Inc. et al. v. Innovatio IP Ventures, No. 1:11-CV-425 (D. Del. May 13, 2011).

41. *In re* Innovatio IP Ventures, 886 F.Supp.2d at 888.

42. *Id.*

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.* at 890.

court ruled that information gathered by Innovatio about the commercial Wi-Fi networks was admissible. This ruling flagged a serious gap in online privacy.

Much of the court's ruling addressed whether Innovatio's sniffing violated federal law. The Wiretap Act states that anyone who intercepts "wire, oral, or electronic communication" may face penalties.[47] The Wiretap Act is part of a broader piece of legislation known as the 1986 Electronic Communications Privacy Act (ECPA).[48] The court ultimately concluded that Innovatio's sniffing operations fell within one of the Wiretap Act's exceptions, which states that it is not unlawful "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."[49] The court reasoned that since the networks in question were not configured to encrypt data and were susceptible to sniffing using readily available equipment, the information sent across those networks was not protected. As a result, Innovatio could use the evidence it had gathered while sniffing the defendants' unencrypted Wi-Fi networks.

One hurdle that the court faced in reaching its decision was a case involving Google Street View. Google Street View was launched in May 2007. Google outfitted cars with cameras that captured 360-degree views of roads, first in major cities and then in increasingly rural areas. The cars were also outfitted with equipment that "sampled, collected, decoded and analyzed all types of data broadcast through [unencrypted] Wi-Fi connections."[50] Google initially denied collecting any digital payload from the connections it intercepted, but eventually admitted it "had intercepted whole emails, usernames, passwords and other private data."[51] In essence, Google was employing the same sniffing tactics that Innovatio used years later as it prepared for its patent infringement lawsuits.

In defending its actions, Google argued (like Innovatio) that its sniffing activities were not subject to the Wiretap Act, but covered by the exemption for communications that are "readily accessible to the general public."[52] After analyzing the Wiretap Act and applying various canons of construction to the language of the statute, the United States District

47. 18 U.S.C. § 2511(1)(a); 18 U.S.C. § 2520(a) (2012).

48. Leong v. Carrier IQ, No. CV 12-01562, 2012 WL 1463313 at *1 (C.D. Cal. Apr. 27, 2012).

49. 18 U.S.C. § 2511(g)(i).

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

51. *Id.* at 1071-72.

52. *Id.* at 1073, quoting 18 U.S.C. § 2511(g)(i).

Court for the Northern District of California rejected Google's argument. It reasoned that although the networks sniffed by Google were unencrypted, "the networks were themselves configured to render the data packets, or electronic communications, unreadable and inaccessible without the use of rare packet sniffing software; technology allegedly outside the purview of the general public."[53] As a result, Google's sniffing was not exempted from the Wiretap Act.

The *Innovatio* court acknowledged that the *Google* decision was the only published case on point[54] but declined to follow *Google* for three reasons. First, the *Google* case was not precedential because it was decided by the U.S. District Court for the Northern District of California, whereas the *Innovatio* litigation is before the U.S. District Court for the Northern District of Illinois. *Google* is therefore persuasive authority that the *Innovatio* court is not bound to follow.[55] Second, the *Innovatio* court noted that in *Google*, the court was called upon to rule on a motion to dismiss, which carries a standard deferential toward the opposing party.[56] Finally, the *Innovatio* court explicitly rejected the *Google* court's reasoning about the unavailability of sniffing technology to the general public.[57]

The court noted that Innovatio was sniffing Wi-Fi networks using a packet capture adapter that cost approximately $700, and that similar devices were available for as little as $200. Moreover, the software used to decode the captured packets is available as a free download. The court observed that, using this commercially available technology, "any member of the general public within range of an unencrypted Wi-Fi network can begin intercepting communications sent on that network."[58] This assessment differed from the *Google* court's view, which described packet capture devices as "sophisticated technology."[59] As a result, the *Innovatio* court declined to follow the *Google* decision and found Innovatio's sniffing to fall within the bounds of the Wiretap Act exception.

53. *Id.* at 1083.

54. *In re* Innovatio IP Ventures, 886 F.Supp.2d at 892.

55. *See* Buzek v. Pepsi Bottling Group, Inc., 501 F.Supp.2d 876, 885 (S.D. Tex. 2007) (stating that "district court opinions…have no precedential effect" and present other district courts with "no obligation to conform to their holdings.")

56. *Id.*

57. *Id.*

58. *Id.*

59. Google Inc. Street View Elec. Commc'ns Litig., 794 F.Supp.2d at 1084.

IV. THE EVOLVING RIGHT TO PRIVACY AND THE INTERNET

. *The Fourth Amendment*

The starting point for Americans' right to privacy is the Fourth Amendment to the U.S. Constitution. The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[60] The Amendment further mandates that search warrants will not be issued "but upon probable cause."[61]

The meaning of the Fourth Amendment has changed over time. When the Supreme Court decided *Katz v. United States* in 1967, some thought that the Fourth Amendment primarily protected places, such as the home;[62] moreover, law enforcement did not need to obtain a warrant to tap communications over phone lines.[63] These factors weighed against Charles Katz, who used public phone booths[64] to place bets on sporting events.[65] The FBI affixed listening devices to the outside of the phone booths, captured Katz's conversations,[66] and arrested him.[67] He was later convicted of violating a federal law prohibiting the use of wire communications for betting on sporting events.[68]

Katz appealed his conviction to the Supreme Court and argued that the FBI violated his Fourth Amendment rights.[69] The government maintained that public phone booths were not protected places under the Fourth Amendment, and so Katz had no expectation of privacy to the phone calls he conducted in them.[70] Moreover, the government argued that since the FBI never intruded into the phone booths, but only attached listening devices to their exterior, no Fourth Amendment analysis was warranted. Finally, the government insisted that the FBI did not need a search warrant to listen to Katz's calls because the surveillance was limited in scope and duration and began only after a strong likelihood of illegal gambling had been established.[71]

The Court rejected the government's place-specific formulation of

60. U.S. CONST. amend. IV.
61. *Id.*
62. Katz v. U.S. (Katz II), 389 U.S. 347, 351–52 (1967).
63. *Surveillance Self-Defense*, ELECTRONIC FRONTIER FOUND., https://ssd.eff.org/wire/govt/wiretapping-protections (last visited Feb. 23, 2014).
64. *Katz II*, 389 U.S. at 348.
65. *See* Katz v. U.S. (Katz I), 369 F.2d 130, 131 n.1 (1966), *rev'd*, 389 U.S. 347 (1967).
66. *Katz II*, 389 U.S. at 348.
67. *Katz I*, 369 F.2d at 132.
68. *Id.* at 131–32.
69. *Katz II*, 389 U.S. at 348–49.
70. *Id.* at 351.
71. *Id.* at 354.

the Fourth Amendment, holding that "the Fourth Amendment protects people, not places." The court elaborated that what a person "seeks to preserve as private. . .may be constitutionally protected."[72] It did not matter that the phone booths used by Katz were public because his conversations were intended to remain private. Additionally, the Court concluded that whether the FBI physically intruded into the phone booths was irrelevant; simply listening to phone calls constituted a search and seizure under the Fourth Amendment.[73] As a result, a search warrant from a magistrate should have been obtained by the FBI before its surveillance of Katz began.[74] Absent a search warrant, the FBI's surveillance was "per se unreasonable under the Fourth Amendment."[75] The *Katz* decision strengthened Fourth Amendment rights and placed a greater burden on law enforcement agencies before they may begin a search and seizure.

B. Privacy Legislation

Advances in technology have raised difficult questions about privacy in the years since *Katz*, especially in the field of communications. To address the tension between privacy and the need for law enforcement to intercept some communications, Congress included the federal Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968.[76] The Wiretap Act sought to protect communications and explained when law enforcement could obtain a warrant to intercept communications.[77] These wiretap orders are sometimes referred to as super-warrants because they are more difficult to obtain than basic search warrants.[78] Super-warrants have "additional requirements beyond probable cause"[79] including a showing "that 'normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous'."[80]

Congress modified the Wiretap Act in 1986.[81] The Electronic

72. *Id.* at 351.
73. *Id.* at 353.
74. *Id.* at 354.
75. *Id.* at 357.
76. Shana K. Rahavy, Note, *The Federal Wiretap Act: the Permissible Scope of Eavesdropping in the Family Home*, 2 J. ON TELECOMM. & HIGH TECH. L. 87, 88 (2003).
77. *Id.*
78. Surveillance Self Defense, *supra* note 63.
79. *In re* Application of United States, 727 F.Supp.2d 571, 573 (W.D. Tex. 2010).
80. *In re* Application of the United States, 396 F.Supp.2d 294, 305 (E.D.N.Y. 2005) (quoting 18 U.S.C. §2518(3)(c) (2012)).
81. *About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163

Communications Privacy Act, or ECPA, updated the Wiretap Act to accommodate advancements in computer technology.[82] The Wiretap Act was considered out of date—it was originally written to cover the interception of communications over traditional telephone lines—and there was concern that the Wiretap Act would not fully protect new forms of electronic communication.[83]

The ECPA consists of two separate pieces of legislation. The first piece, also known as the Electronic Communications Privacy Act, is the portion that updated the Wiretap Act of 1968. Title I of the ECPA (18 U.S.C. §§ 2510-22) prohibits the intentional interception or attempted interception, use, disclosure, or procurement of "any wire, oral, or electronic communication."[84] Title I also contains 18 U.S.C. § 2511(g)(i), the exceptions section that protected Innovatio's sniffing operations.[85] Finally, Title I sets forth the standards for obtaining super warrants and "prohibits the use of illegally obtained communications as evidence."[86]

The second piece of the ECPA is the Stored Communications Act. It established Title II of the law.[87] It protects information stored by service providers, including subscriber data like names, billing records, and IP addresses.[88] Title III of the ECPA relates to pen register devices (used to capture information about outgoing phone calls) and trap and trace devices (devices that capture information about incoming telephone calls).[89]

Unfortunately, there have been no significant changes to the Wiretap Act since 1986. This is problematic when one considers the tremendous progress made in telecommunications since that time. To be fair, legislators could not have anticipated the pervasiveness of e-mails, social media, or GPS data emitted by cell phones, let alone complimentary, unencrypted Wi-Fi in coffee shops. Nevertheless, the data comprising these and other technologies enjoy mixed protection under the Wiretap Act. Courts face the difficult job of applying outdated

(last visited Nov. 9, 2012).

82. *Id.*

83. *Privacy & Civil Liberties: Federal Statutes*, U.S. DEP'T. OF JUSTICE, http://www.it.ojp.gov/default.aspx?area=privacy&page=1285#contentTop (last visited Nov. 9, 2012).

84. *Id.*, quoting 18 U.S.C. § 2511(1).

85. *In re* Innovatio IP Ventures, 886 F.Supp.2d 888 (N.D. Ill. 2012); *Privacy & Civil Liberties: Federal Statutes*, *supra* note 83.

86. *Privacy & Civil Liberties: Federal Statutes*, *supra* note 8383; 18 U.S.C. § 2515 (2012).

87. *Privacy & Civil Liberties: Federal Statutes*, *supra* note 83.

88. *Id.*

89. *Id.*

statutory standards to modern technology, leading to confusion and inconsistency.

V. LESSONS LEARNED

The issue at the heart of the *Innovatio* court's decision is whether sniffing unencrypted Wi-Fi networks falls within the general public accessibility exception of the Wiretap Act. As explained above, the court decided that unencrypted Wi-Fi networks are configured in such a way that data sent across them is readily accessible to the general public. The data sent over unencrypted Wi-Fi is thus exempt from protection thanks to 18 U.S.C. § 2511(g)(i) of the Wiretap Act, and Innovatio may sniff the networks to collect data. This ruling not only highlights the Wiretap Act's weakness, but also suggests several ways that weakness can be addressed.

A. Implications

Innovatio claims that it overwrote the data packets it intercepted, scrubbing substantive user data and documenting only network data needed to prove its patent infringement claims. The *Innovatio* court gave its blessing to this sort of behavior. This has significant implications for both business conduct and law enforcement data collection tactics.

At the outset, it is important to note that companies like Starbucks are already monitoring the online activities of their patrons. When a patron uses Starbucks' unencrypted, complimentary Wi-Fi, they accept an expansive privacy policy. This policy allows Starbucks to acquire names, addresses, email address, financial information, passwords[90]—in effect, everything Innovatio collected when it sniffed unencrypted Wi-Fi. This information may also be shared with third parties.[91]

Starbucks clearly sees value in the information is gathers from patrons. Its privacy policy allows information to be shared with credit card processors, mailing houses, website hosts, and email vendors.[92] Other companies could also see unencrypted Wi-Fi as a source of valuable information and sniff those networks like Innovatio did. Although companies could face criminal liability for abusing this data (for example, using passwords and usernames to perpetrate identity theft), it is currently legal for companies to routinely sniff networks to compile extensive internet profiles on users.

90. *Privacy Policy*, STARBUCKS, http://www.starbucks.com/about-us/company-information/online-policies/privacy-policy (last visited Feb. 24, 2014).

91. *Id.*

92. *Id.*

Databases that log extensive user information not only pose a serious privacy problem, but also expose users to potential threats. For example, the hacker group Anonymous has compromised banks, stolen credit card numbers, and published sensitive emails.[93] If companies like Starbucks amass databases that log user information, they may attract the interest of Anonymous and other hackers whose goals extend beyond commercial advertising. This poses a serious risk to patrons who use unencrypted Wi-Fi.

The Wiretap Act's public accessibility exemption may also provide law enforcement with a way to monitor online activities without the need for a warrant. Federal and state authorities could routinely sniff unencrypted Wi-Fi at commercial hotspots, searching emails for signs of criminal activity, monitoring web sessions for copyright infringement, and perusing bank transactions to make sure people are not evading taxes. While this may aid authorities in enforcing the law, it also opens the door for perpetual surveillance of people who are not suspected criminals. This could also generate extensive law enforcement databases logging the activities of Wi-Fi users, regardless of whether those activities have any real value to law enforcement efforts.

B. Solutions

There are several ways to address the privacy concerns revealed by the *Innovatio* decision. These include federal legislation, state-based privacy laws and business regulations, industry standards requiring network encryption, and judicial interpretation of the Wiretap Act that removes sniffing from the public accessibility exception.

1. Changes to Federal Law

The first option is to update federal privacy law, which is outdated in many respects. There have been efforts to update privacy law in recent years. For example, legislation was introduced in 2011 to protect GPS data and require a warrant before GPS data could be collected by the government.[94] Another piece of legislation was introduced in 2012 that would require warrants rather than mere subpoenas to retrieve online

93. Dominic Rushe, *Anonymous hackers release Bank of America emails*, THE GUARDIAN (Mar. 14, 2011, 9:59 AM), http://www.guardian.co.uk/business/2011/mar/14/anonymous-hackers-release-bank-america-emails; *see also* Lee Moran, *Anonymous hackers to publish U.S. security firm's 2.7m client emails…'providing a smoking gun for a number of crimes,'* MAIL ONLINE (Feb. 29, 2012, 4:00 PM), http://www.dailymail.co.uk/news/article-2079262/Anonymous-hackers-publish-U-S-security-firms-2-7m-client-emails--providing-smoking-gun-number-crimes.html.

94. Geolocational Privacy and Surveillance Act of 2011, S. 1212, 112th Cong. (2011).

data like emails.[95] Indeed, the Supreme Court of the United States even weighed in on warrantless collection of GPS data, ruling in January 2012 that the FBI violated the Fourth Amendment when it attached a GPS device to a suspected criminal's car without a warrant.[96]

One way to address the Wiretap Act's deficiencies is to update the law's exceptions section. That section currently states that it is lawful "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."[97] A sentence could be inserted here stating that all electronic communications on WLAN, whether encrypted or unencrypted, shall not be considered readily accessible to the general public. This would fill the privacy gap highlighted by the *Innovatio* decision and foreclose future sniffing operations of all WLAN absent a warrant.

Congress could also protect online privacy by imposing security regulations on wireless router manufacturers. Congress could enact a law requiring all Wi-Fi routers manufactured after a certain date be preset to broadcast using WPA2 encryption. This would save users (citizens, coffee shops, cafes, hotels, etc.) the effort of setting up secure networks while simultaneously removing their networks from the public accessibility exception contained in the Wiretap Act.

Such legislation would pass Constitutional muster as an exercise of Congress' power to regulate interstate commerce.[98] In *U.S. v. Lopez*, the Supreme Court identified three categories of interstate commerce that Congress can regulate. First, Congress "may regulate the use of the channels of interstate commerce."[99] Second, Congress can regulate "instrumentalities. . .or persons or things in interstate commerce."[100] Finally, Congress can regulate "activities having a substantial relation to interstate commerce."[101] Wireless routers arguably fall into all three categories, but are assuredly a "thing" within interstate commerce, thus subjecting them to Congressional regulation.

95. Video Privacy Protection Act Amendments Act of 2012, H.R. 2471, 112th Cong. (2012).

96. David S. Savage, *Supreme Court: Police need warrant to use GPS tracking on cars*, L.A. TIMES (Jan. 23, 2012, 8:28 AM), http://latimesblogs.latimes.com/nationnow/2012/01/supreme-court-gps-tracking.html.

97. 18 U.S.C. § 2511(g)(i).

98. *See* U.S. CONST. art. I, § 8.

99. United States v. Lopez, 514 U.S. 549, 558 (1995).

100. *Id.*

101. *Id.* at 558–59.

2. State Options

States have their own ways of addressing the Wiretap Act's shortcomings. One option is for states to incorporate protections for unencrypted Wi-Fi into their own comprehensive privacy regimes. All states except Vermont have enacted wiretap statutes.[102] For example, California's Invasion of Privacy Act makes it illegal to "willfully and without the consent of all parties to the communication, or in any unauthorized manner, read[], or attempt[] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable."[103]

Language like this prevents sniffing, regardless of whether a given Wi-Fi network is encrypted. This would offer a state remedy to patrons whose privacy is compromised by sniffing.

This option is not without risk. For example, some United States District Courts in California have found the state's privacy act to be preempted by the Wiretap Act.[104] Another has found that the California law is not preempted since the Wiretap Act simply establishes a minimum standard for privacy that states can expand upon.[105] This disagreement indicates that states should be aware of the risk of federal preemption and plan for the effects it could have on the privacy of their citizens.

If state privacy regimes are preempted, legislatures have a fallback option: they could pass laws requiring businesses to encrypt their complimentary Wi-Fi. Preemption should not pose an issue here since this would constitute a simple business regulation and not a privacy law. By requiring all businesses to provide encrypted Wi-Fi, the online security of patrons would be preserved and the Wiretap Act's public accessibility exception defeated.

3. Industry Solutions

The third set of solutions resides with the wireless router industry. Most Wi-Fi equipment is shipped with security features disabled,[106] and many Wi-Fi users either do not understand encryption and its benefits or are unwilling to take the extra steps needed to configure their router to broadcast an encrypted signal.[107] As a result, millions of people use

102. Rahavy, *supra* note 76.

103. CAL. PENAL CODE § 631 (West 2012).

104. Leong v. Carrier IQ Inc., No. CV 12-01562, 2012 WL 1463313 at *1 (C.D. Cal. Apr. 27, 2012).

105. *Id.*

106. WI-FI ALLIANCE, *supra* note 24.

107. Samara Lynn, *10 Wireless Router Features You Should Be Using but Aren't*,

unencrypted Wi-Fi.[108] To address this, the Wi-Fi Alliance could begin certifying only wireless routers that either include default WPA2 settings or require users to input WPA2 encryption settings before a router can broadcast. This would ensure that more Wi-Fi networks are encrypted and not subject to the public accessibility exception.

Alternatively, if the Wi-Fi Alliance does not implement default or mandatory encryption, its member companies could. Some Wi-Fi router manufacturers are already simplifying the encryption process for their customers. Netgear, for example, sells routers that offer encrypted protection with the push of a button.[109] Cisco, on the other hand, sells the Linksys EA4500 that automatically configures itself to broadcast strongly encrypted internet upon initial setup.[110]

In either scenario, the cost of implementing default or mandatory WPA2 encryption should be small for the router industry and for consumers. Wi-Fi equipment is already required to meet WPA2 standards before it is certified by the Wi-Fi Alliance, and many routers are using Wi-Fi Protected Setup or automatic WPA2 setup. And although encryption can slow performance in older routers, most new routers include hardware designed to support WPA or WPA2 encryption, minimizing any decrease in performance.[111] If encryption continues to become an industry default, consumer privacy will be maintained and the risk of legal network sniffing will be eliminated.

4. Judicial Interpretation

Finally, a fourth way of addressing the privacy concerns raised by *Innovatio* is for courts to interpret the Wiretap Act to protect unencrypted wireless communications. *Google* and *Innovatio* indicate that courts have disagreed about the ECPA's exception language. The *Innovatio* court found that the sniffing operations at issue were encompassed by the Wiretap Act's exception for communications sent across a system that "is readily accessible to the general public," whereas the *Google* court

PCMAG.COM (June 20, 2012), http://www.pcmag.com/article2/0,2817,2405996,00.asp.

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

109. *See Wireless 300 Modem Router and USB Adapter*, NETGEAR, http://www.netgear.com/home/products/wirelessrouters/work-and-play/DGNB2100.aspx#one (last visited Jan. 29, 2014).

110. This router will automatically broadcast a signal with WPA2 encryption. Lynn, *supra* note 107107.

111. Jeff Bertolucci, *How to Improve the Performance of Your Home Wi-Fi*, TECHWORLD (May 18, 2011, 1:30 PM), http://howto.techworld.com/personal-tech/3280551/how-to-improve-the-performance-of-your-home-wi-fi/.

found that unencrypted Wi-Fi networks are not readily accessible.[112] If higher courts follow *Google's* interpretation, the privacy of unencrypted Wi-Fi communications will be preserved even if the Wiretap Act remains unchanged. Several arguments can be made for why courts should follow *Google's* lead.

Google launched its Street View project in May 2007 with the goal of allowing "users to view and navigate within 360 degree street level imagery of various cities in the US."[113] The program had expanded internationally by 2009.[114] In 2010, the German government discovered that Google's Street View vehicles were not only taking pictures, but also scanning and gathering data about Wi-Fi networks.[115] This revelation led to lawsuits and government investigations around the world.[116]

One entity involved in the ensuing Google litigation is the Electronic Privacy Information Center, or EPIC. Among other things, EPIC filed an amicus brief in a privacy case before the U.S. Ninth Circuit Court of Appeals.[117] EPIC identified two ways the court could interpret the Wiretap Act to protect unencrypted Wi-Fi.

First, EPIC maintains that Wi-Fi networks enable private communications that are not readily accessible to the general public.[118] It explains that typical Wi-Fi networks broadcast a radio signal at frequencies and power levels that differ greatly from "traditional radio broadcasts like AM, FM, and Citizens Band (CB) radio."[119] These differences affect "the degree to which the communications are publicly available."[120] AM radio stations can broadcast a signal up to 100 miles, whereas Wi-Fi devices broadcast a signal to only 70-300 feet.[121]

112. 18 U.S.C. § 2511(g)(i) (2012); *In re* Innovatio IP Ventures, 886 F.Supp.2d 888 (N.D. Ill. 2012).

113. *Google Announces New Mapping Innovations at Where 2.0 Conference*, GOOGLE (May 29, 2007), http://googlepress.blogspot.com/2007/05/google-announces-new-mapping_29.html.

114. Richard Wray, *Google Launches Street View in UK*, THE GUARDIAN (Mar. 19, 2009), http://www.guardian.co.uk/business/2009/mar/19/google-street-view-uk.

115. *Google-Street-View Tours also Used for Scanning WLAN-networks*, THE FED. COMM'R FOR DATA PROT. & FREEDOM OF INFO. (Apr. 23, 2010), http://www.bfdi.bund.de/cln_134/sid_74A4D9FE1F85492D36F74BB3443C41EA/EN/PublicRelations/PressReleases/2010/GoogleWLANScan.html.

116. *Investigations of Google Street View*, EPIC.ORG (last visited Nov. 10, 2012), http://epic.org/privacy/streetview/ (last visited Jan. 29, 2014).

117. Brief for Electronic Privacy Information Center (EPIC) as Amicus Curiae Supporting Appellees, Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013), *amended and superseded on reh'g* (No. 11-17483), 2013 WL 6905957 at *1.

118. *Id.* at *11–12.

119. *Id.* at *13–15.

120. *Id.* at *16.

121. *Id.* at *17.

Moreover, electronics communicating with a Wi-Fi device must first be authenticated by the network.[122] This means that data is sent to specific destinations within a network "and is not intended to be available to other devices," let alone the general public.[123] Thus, communications sent over unencrypted Wi-Fi would fall outside the Wiretap Act's public accessibility exception.

EPIC articulates policy reasons that should lead courts to grant greater protection to unencrypted wireless communications. Even strong Wi-Fi encryption like WPA2 is vulnerable to attack, suggesting that no consumer can maintain a signal that is completely safe from interception and decryption.[124] Additionally, many users own electronics with unencrypted default settings, or own older electronics that are incompatible with newer encryption.[125] Forcing Wi-Fi users to maintain the highest available encryption standards would subject them to "unreasonable burdens."[126] Consequently, policy favors protecting even unencrypted Wi-Fi.

In summary, there are four actors who can address the privacy risks identified by the *Innovatio* decision. First, Congress can update the Wiretap Act and eliminate the exception that allows for unencrypted Wi-Fi sniffing. Additionally, Congress can use its interstate commerce power to require Wi-Fi router manufactures to include default or mandatory encryption settings. Second, states can address the privacy risk by passing their own privacy regimes or by requiring businesses to offer only encrypted Wi-Fi to customers. States should be wary that their privacy regimes may be susceptible to federal preemption. Third, the Wi-Fi industry could implement default or mandatory encryption settings, as some have already decided to do. Finally, the courts can interpret the Wiretap Act so that wireless communications are not subject to the statute's public accessibility exception.

VI. RECOMMENDATION: THE WI-FI INDUSTRY HOLDS THE IDEAL SOLUTION

Of the four solutions detailed above, new encryption requirements within the Wi-Fi industry are the most promising way to address the privacy gap identified by the *Innovatio* decision. Implementing default or mandatory WPA2 encryption is simpler and quicker than federal, state, and judicial solutions, and the technology already exists to implement it

122. *Id.* at *23.
123. *Id.* at *24.
124. *Id.* at *26, 28–30.
125. *Id.* at *30.
126. *Id.* at *33.

with little added cost to the industry.

As stated above, two kinds of federal action could be taken to address the unencrypted Wi-Fi problem. First, Congress could update the Wiretap Act to protect both encrypted and unencrypted Wi-Fi. Alternatively, Congress could impose regulations on Wi-Fi manufacturers pursuant to congressional commerce power. Unfortunately, neither option is likely to be implemented in the near future.

Efforts have already been made to update the Wiretap Act, but to no avail. For example, Senator Patrick Leahy of Vermont introduced a bill in 2011 to update portions of the ECPA.[127] The Wiretap Act is a part of this legislation. The bill was referred to the Senate Committee on the Judiciary, where it languished until the end of the 112th Congress.[128] Additionally, Congress was mired in an ongoing saga of fiscal cliff crises[129] and debt ceiling debates[130] that continued into 2013.[131] Congress' unwillingness to modify the Wiretap Act, combined with ongoing economic battles, suggests that congressional action to mandate Wi-Fi protection is highly unlikely.

State action to either bolster privacy regimes or require businesses to offer encrypted Wi-Fi has its own limitations. First, even if states implement privacy laws to protect Wi-Fi, there is virtually no chance the laws will be uniformly crafted or consistently applied by courts from state to state. Wi-Fi users can only hope for a patchwork of privacy laws and business regulations. The application of these laws and regulations may be further changed by judicial interpretation. Moreover, the risk of federal preemption of state privacy regimes remains a possibility. As a result, state privacy laws and business regulations cannot hope to uniformly protect data sent over unencrypted Wi-Fi.

Favorable interpretation of the Wiretap Act by the judiciary also has limitations. For one, federal district courts already disagree over whether the Wiretap Act protects data sent over unencrypted Wi-Fi.[132] If federal

127. S. 1011, 112th Cong. (as introduced by Senate, May 17, 2011).

128. *See* Bill Summary and Status, S. 1011, 112th Cong. (as referred to by S. Comm. on the Judiciary, May 17, 2011).

129. Dana Bash, Dana Ford & Josh Levs, *House Approves Senate's Fiscal Cliff Deal*, CNN (Jan. 1, 2013, 11:08 PM), http://www.cnn.com/2013/01/01/politics/fiscal-cliff/index.html.

130. Jeanne Sahadi, *Debt Ceiling: What the Deal Will Do*, CNN MONEY (Aug. 2, 2011, 12:43 PM), http://money.cnn.com/2011/08/01/news/economy/debt_ceiling_breakdown_of_deal/index.htm.

131. Jeanne Sahadi, *Debt Ceiling FAQs: What You Need to Know*, CNN MONEY (Jan. 15, 2013, 10:46 AM), http://money.cnn.com/2013/01/10/news/economy/debt-ceiling-faqs/.

132. *Compare In re* Innovatio IP Ventures, 886 F. Supp. 2d 888 (N.D. Ill. 2012), *with* Google Inc. Street View Elec. Commc'ns Litig., 794 F.Supp.2d 1067 (N.D. Cal. 2011).

Courts of Appeals eventually take up cases involving the Wiretap Act, there is a risk of similar disagreement over the law's protections. This could lead to circuit splits and confusion over whether data sent over unencrypted Wi-Fi is protected in the various circuits. Absent congressional action to clarify the matter, the Supreme Court of the United States could be the final arbiter. This process would be lengthy and cannot be relied upon to result in greater Wi-Fi protections. As a result, judicial interpretation of the Wiretap Act is not a preferable option.

Ultimately, the best way of protecting data sent over unencrypted Wi-Fi lies with the Wi-Fi industry. WPA2 encryption is now ubiquitous on equipment certified by the Wi-Fi Alliance. Additionally, router manufacturers are already beginning to implement either simplified encryption setup features or default encryption settings. If the Wi-Fi Alliance embraces this trend and requires default or mandatory WPA2, little or no extra burden and cost will be imposed on manufacturers. Moreover, the hardware in many routers is able to support encryption without diminishing performance, minimizing costs to consumers.

Additionally, now may be the ideal time for the Wi-Fi Alliance to require default or mandatory WPA2 encryption on all certified products. As mentioned earlier, the Wi-Fi Alliance is certifying products based on a new standard, IEEE 802.11ac. The introduction of the new standard presents an optimal time to also introduce new security requirements for Wi-Fi routers.

CONCLUSION

Worldwide, approximately 200 million households use Wi-Fi networks. There are also 750,000 Wi-Fi hotspots. This adds up to 700 million users of Wi-Fi technology.[133] Unfortunately, the privacy of those users is undermined if the Wi-Fi networks are not encrypted. This is highlighted by the *Innovatio* decision.

In *Innovatio*, a U.S. District Court was called upon to answer a question about the admissibility of evidence in a patent infringement case. Its decision could have broad implications for the online privacy of Wi-Fi users. Innovatio used a combination of technologies to sniff unencrypted Wi-Fi networks, capturing extensive amounts of user data in the process. This raised the question of whether or not sniffing was prohibited by the Wiretap Act.

The court reasoned that unencrypted Wi-Fi networks were

133. *The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular*, CISCO, http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns673/white_paper_c11-649337.html (last visited Feb. 24, 2014).

configured in such a way that the communications sent over them were "readily accessible to the general public."[134] The court noted that the technology used by Innovatio in its sniffing operations consisted of a laptop, an adapter that cost as little as $200, and software that is available for free. The information sent over unencrypted Wi-Fi networks thus fell within an exception to the Wiretap Act.

The Wiretap Act is part of an evolving privacy regime in America. The origins of the right to privacy are found in the Fourth Amendment to the Constitution. The Fourth Amendment's meaning has evolved over time, with efforts made by Congress in 1986 to update protections for communications made with new kinds of technology. Unfortunately, 1986 was the last time those protections were updated.

There are several risks posed by the *Innovatio* decision and the current state of the Wiretap Act. For one, businesses can sniff unencrypted Wi-Fi networks and use the data to create user databases, monitor user activity, and craft increasingly personalized advertisements and messages. Similarly, law enforcement can monitor unencrypted Wi-Fi for signs of wrongdoing, amassing databases of user activity regardless of whether those users are suspected of criminal activity. Finally, these databases pose attractive targets for hacker groups like Anonymous, which have compromised banks and security firms in the past.

Several avenues are available for updating the Wiretap Act to protect communications sent over unencrypted Wi-Fi networks. First, Congress can revise the Wiretap Act to include protection for all communications sent over Wi-Fi, regardless of whether the network is encrypted. Second, Congress can pass encryption standards for Wi-Fi router manufacturers to follow. Additionally, states can require businesses to offer only encrypted Wi-Fi to patrons. States can also strengthen their own privacy regimes, though they must be conscious of the risk of federal preemption. Next, the Wi-Fi industry could utilize either default or mandatory WPA2 encryption settings. Finally, the courts may interpret the Wiretap Act to protect even unencrypted Wi-Fi communications.

The internet is both a useful and a dangerous tool. As people become increasingly digitized, so should the laws that protect them. Laws that were crafted decades ago are no longer sufficient to protect people from all kinds of intrusion, especially in the case of unencrypted Wi-Fi networks. Both federal and state governments should make efforts to protect users of unencrypted Wi-Fi. The courts can also be more proactive in construing the Wiretap Act to favor privacy. Most

134. *In re* Innovatio IP Ventures, 886 F.Supp.2d 888 at 892.

importantly, the Wi-Fi Alliance should set new requirements for encryption as it implements its new IEEE 802.11ac standard.

When the Wi-Fi Alliance introduced WPA encryption in 2003, it stated that one of its goals "is to ensure that consumers realize maximum benefit from their Wi-Fi products in a secure and productive environment."[135] Ten years later, stronger WPA2 encryption is now the industry norm and a new Wi-Fi standard is about to take effect. It is time for the Wi-Fi Alliance to live up to its commitment to provide a "secure and productive environment" by requiring that all Wi-Fi routers include either default or mandatory encryption settings.[136] Doing so will not only validate the Wi-Fi Alliance's commitment, but also protect users from the pitfalls of an outdated federal privacy law.

135. *White Paper*, *supra* note 20.
136. *Id.*