NEW YORK LAW SCHOOL

NYLS Law Review

Volume 58
Issue 2 *Freedom of Choice at the End of Life: Patients' Rights in a Shifting Legal and Political Landscape*

Article 13

January 2014

In re Innovatio IP Ventures, LLC Patent Litigation

ALEXANDER M. NOBLE
New York Law School, 2014

VOLUME 58 | 2013/14

ALEXANDER M. NOBLE

In re Innovatio IP Ventures, LLC Patent Litigation

58 N.Y.L. Sch. L. Rev. 473 (2013–2014)

ABOUT THE AUTHOR: Alexander M. Noble is a 2014 J.D. candidate at New York Law School.

Anyone who has accessed the Internet through a public wireless network[1] may well have been the victim of a data interception technique called "packet sniffing."[2] Packet sniffing is an increasingly common method of capturing data from personal devices that use wireless, or "Wi-Fi," networks to access the Internet.[3] Wi-Fi networks connect devices such as laptops and smartphones to the Internet by sending packets of data back and forth between Internet-capable devices and the network's router.[4] Using a machine called a "packet analyzer," third parties can capture and decode these data packets to reveal the personal information that they contain.[5]

Once decoded, packet data reveals two types of information: "header" data, which shows the addresses of the devices that transmitted the packets; and "payload" data, which consists of emails, pictures, passwords, and any other substantive information that network users are accessing, receiving, or sending online at the time of capture.[6] Packet analyzers are compact and commercially sold,[7] and they also provide third parties with a panoramic view of all user activity on a given Wi-Fi network. Considering the surging popularity of public Wi-Fi networks in the United States,[8] the legality of packet sniffing has major implications for the right to privacy in the Internet age.

---

1. In a 2012 study from Identitytheft.org, 78% of survey respondents had used public Wi-Fi at least once within the last twelve months. Press Release, Identity Theft Res. Ctr., Identity Theft and Public WiFi Linked in Consumer Minds (Oct. 19, 2012), *available at* http://archive-org.com/page/504527/2012-10-23/http://www.idtheftcenter.org/artman2/publish/lib_survey/Public-WiFi-Usage-Survey.shtml.

2. *See* Prabhaker Mateti, *Hacking Techniques in Wireless Networks*, *in* The Handbook of Information Security 83, 85–87 (Hossein Bidgoli ed., 2005), *available at* http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.doc ("*Sniffing* is eavesdropping on the network. A (packet) *sniffer* is a program that intercepts and decodes network traffic broadcast through a medium. Sniffing is the act by a machine S of making copies of a network packet sent by machine A intended to be received by machine B.").

3. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1231 (2004) (describing a packet sniffer as "a surveillance tool that sits at a point on the network and scans and then filters passing Internet traffic").

4. *See* Susan Landau, *Digital Age Communications Law Reform: National Security on the Line*, 4 J. Telecomm. & High Tech. L. 409, 424 (2006) ("[T]he Internet is a 'packet-switched' network. In such networks, fixed circuits are not dedicated for the duration of a communication. Instead, the data that is transmitted, whether files, email, Instant Messages, voice, is broken into small packets. Each packet travels its own route over the Internet. The entire set of contents is reassembled when it is received at the other end. The technology of packet routing creates some differences with circuit-switched technology.").

5. *See What Is a Network Packet Analyzer*, SolarWinds, http://www.solarwinds.com/it-management-glossary/what-is-network-packet-analyzer.aspx (last visited Dec. 21, 2013).

6. *See Payload*, TechTerms.com, http://www.techterms.com/definition/payload (last visited Dec. 21, 2013).

7. *See Riverbed Technology Product Catalog*, Riverbed, http://www.cacetech.com/products/catalog/ (last visited Dec. 21, 2013) (listing a basic packet capture device for a retail price of $198).

8. There are 245,203,319 Internet users in the United States, which amounts to roughly 78.1% of the population. *See Internet Users in North America*, Internet World Stats: Usage & Population Statistics, http://www.internetworldstats.com/stats14.htm (last updated June 30, 2012). Wigle.net, a database of user-reported Wi-Fi networks, lists over 16 million networks, and that is likely a small

In *In re Innovatio IP Ventures, LLC Patent Litigation*, the U.S. District Court for the Northern District of Illinois held that federal wiretapping laws do not prohibit third parties from intercepting packet data sent over public Wi-Fi networks.[9] Title I of the Electronic Communications Privacy Act (ECPA), also known as the Wiretap Act,[10] ordinarily imposes criminal and civil liability on any person who intentionally intercepts electronic communications without authorization.[11] However, the court in *Innovatio* determined that the interception of packet data falls within an exception to liability in section 2511(2)(g)(i) of the Wiretap Act (the "G1 exception"), which permits third parties to intercept communications that are "readily accessible to the general public."[12] The court held that because packet data sent over public Wi-Fi networks is "readily accessible to the general public," the G1 exception permits third parties to intercept it without violating the Wiretap Act.[13]

In the court's view, packet data qualified as "readily accessible to the general public" because members of the public could gain access to the data through the use of packet analyzer technology.[14] To reach this conclusion, the court focused solely on whether technology makes it possible for third parties to intercept a particular communication, while ignoring the intent of network users to keep their data private. This case comment contends that by failing to consider user intent, the court in *Innovatio* formulated an overly broad and circular definition of the phrase "readily accessible to the general public"[15] that unduly expands the G1 exception and erodes the Wiretap Act's distinction between public and private communications, thereby

fraction of the total number of Wi-Fi networks in use. *See* Predrag Klasnja et al., *"When I Am on Wi–Fi, I Am Fearless": Privacy Concerns & Practices in Everyday Wi–Fi Use*, CHI 2009, *available at* http://appanalysis.org/jjung/jaeyeon-pub/FormativeUserStudy4CHI.pdf.

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

10. Electronic Communications Privacy Act, 18 U.S.C. § 2511–22 (2012). After the statute's initial passage in 1968, Congress subsequently amended sections 2511–22, which comprise Title I, and renamed them the Electronic Communications Privacy Act. *See* Pub. L. No. 90-351, § 802, 82 Stat. 197, 213–25 (1968). This case comment follows the practice of most courts by referring to sections 2511–22 as the Wiretap Act rather than the ECPA.

11. 18 U.S.C. § 2511(1)(a) (providing that any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)").

12. *Id.* § 2511(2)(g)(i).

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

14. The court noted that "[w]ith a packet capture 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." *Id.* at 893.

15. The court reduced the G1 exception to a tautology: intercepting unsecured Wi-Fi communications should be legal because the public can use packet analyzers to access them, and packet analyzers are accessible to the public because it is not illegal to possess them. The invasive use of a surveillance technology should not be legal merely because the technology itself is legal to possess.

diminishing the privacy of individual users and undermining the integrity of public Wi-Fi networks.[16]

The plaintiff, Innovatio IP Ventures, LLC ("Innovatio") is a Delaware-based company that owns a portfolio of thirty-one patents for wireless Internet products.[17] In 2011, Innovatio filed a series of patent infringement suits against a number of hotels, restaurant chains, and businesses that use its wireless Internet products.[18] The Judicial Panel on Multidistrict Litigation then consolidated all claims and parties into a single action in the Northern District of Illinois.[19] Before the district court, Innovatio argued that the defendants committed patent infringement by using Innovatio's patented products to provide free wireless Internet access to customers of the defendants' businesses.[20]

As the case proceeded to discovery, Innovatio revealed that it had been collecting evidence of the alleged infringement by using packet analyzers to sniff the defendants' Wi-Fi networks.[21] Innovatio contended that the information it collected through packet sniffing, such as the number of users of the defendants' networks, would assist in proving its infringement claims.[22] The court, however, expressed concern that Innovatio's "sniffing protocol" involved the use of packet analyzers to capture data from the devices of users accessing the defendants' networks and may have intercepted private communications in violation of the Wiretap Act.[23] Innovatio was

16. Former Federal Communications Commission Chairman Julius Genachowski proposed creating a system of "WiFi networks across the nation, so powerful and broad in reach that consumers could use them to make calls or surf the Internet without paying a cellphone bill every month." Cecilia Kang, *Tech, Telecom Giants Take Sides as FCC Proposes Large Public WiFi Networks*, Wash. Post (Feb. 3, 2013), http://articles.washingtonpost.com/2013-02-03/business/36728627_1_wifi-networks-wireless-industry-wireless-networks; *see also* Press Release, Wi-Fi Alliance, Wi-Fi Alliance Applauds New FCC Milestone Toward the Release of Additional Spectrum for Wi-Fi (Feb. 25, 2013), *available at* http://www.wi-fi.org/media/press-releases/wi-fi-alliance%C2%AE-applauds-new-fcc-milestone-toward-release-additional-spectrum.

17. *See* Raymond P. Niro, *Setting the Record Straight on the Innovatio Patent Portfolio*, IPWatchdog (Mar. 21, 2012, 3:41 PM), http://www.ipwatchdog.com/2012/03/21/setting-the-record-straight-on-the-innovatio-patent-portfolio/id=22964/; *see also* Gregory Thomas, *Innovatio's Infringement Suit Rampage Expands to Corporate Hotels*, The Patent Examiner (Sept. 30, 2011), http://patentexaminer.org/2011/09/innovatios-infringement-suit-rampage-expands-to-corporate-hotels/.

18. *See In re Innovatio IP Ventures*, 886 F. Supp. 2d at 889; *see also* Motorola Solutions, Inc. v. Innovatio IP Ventures, LLC, 921 F. Supp. 2d 903, 907 (N.D. Ill. 2013) (noting that since February 2011, Innovatio had sent over 8,000 letters to users of its wireless products in all fifty states, alleging patent infringement and demanding payment for a license).

19. *See In re* Innovatio IP Ventures, LLC Patent Litig., 840 F. Supp. 2d 1354 (J.P.M.L. 2011) (mem.); *see also Motorola Solutions*, 921 F. Supp. 2d at 909 (addressing allegations that Innovatio had filed twenty-three "sham" lawsuits against companies who refused to buy a license).

20. *See In re Innovatio IP Ventures*, 886 F. Supp. 2d at 889.

21. *See id.* at 890.

22. *See id.*

23. *Id.*

therefore directed by the court to produce a detailed description of how its sniffing protocol operated for purposes of determining compliance with the Wiretap Act.[24]

Innovatio's sniffing protocol consisted of sending its technicians onto the defendants' premises during normal business hours to acquire packet data from their wireless networks.[25] The technicians accessed the networks with laptops and then used packet analyzers[26] to capture data from the devices of the defendants' customers and members of the public who were also accessing the networks at that time.[27] As is often the case when third parties sniff a Wi-Fi network, neither the defendants nor the individuals on the network were aware that Innovatio's technicians had intercepted their data.[28] The packet analyzers acquired packet data from all wireless devices communicating with the targeted networks, including laptops, smartphones, and tablet computers.[29]

After obtaining and storing the data packets, the technicians decoded them using a packet analyzer program called "Wireshark," which revealed both the header and payload information stored within the data.[30] The header information, which Innovatio claimed would assist in proving its patent infringement claims, showed that a number of the defendants' customers had in fact accessed the wireless networks operated with the patented products.[31] However, the decoded packets also revealed all of the payload data that the network users were accessing at the time of capture, including their "e-mails, pictures, videos, passwords, financial information, [and] private documents."[32]

Upon review, the court determined that—despite Innovatio's capture of network users' personal information without their knowledge or consent—the sniffing protocol did not violate the Wiretap Act.[33] The court therefore authorized Innovatio to continue using packet analyzers to intercept packet data from customers using the defendants' Wi-Fi networks.[34]

---

24. *See id.*

25. *See id.*

26. *See id.* at 893 (stating that Innovatio's technicians used a specific packet analyzer model called the Riverbed AirPcap Nx packet capture adapter, which is available online for public purchase); *see also Riverbed Technology Product Catalog*, *supra* note 7.

27. *See In re Innovatio IP Ventures*, 886 F. Supp. 2d at 890.

28. *See What Is a Packet Sniffer and How Does It Work?*, Spamlaws.com, http://www.spamlaws.com/how-packet-sniffers-work.html (last visited Dec. 21, 2013) ("Hackers often use packet sniffers because they are very difficult to detect and can be installed in almost any location on the network."); *What Is a Packet Sniffer?*, WiseGEEK, http://www.wisegeek.org/what-is-a-packet-sniffer.htm (last visited Dec. 21, 2013) ("This type of packet sniffer is very hard to detect because it generates no traffic of its own.").

29. *See In re Innovatio IP Ventures*, 886 F. Supp. 2d at 890.

30. *See id.*

31. *See id.*

32. *Id.*

33. *See id.* at 894.

34. *See id.* at 895 (holding that "Innovatio may collect information from the defendants' public-facing Wi-Fi networks according to its proposed protocol").

The court held that while a third party's non-consensual interception of private data ordinarily violates the Wiretap Act, Innovatio's acquisition of packet data did not because its sniffing protocol fell within the G1 exception, which makes it lawful to intercept an "electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[35] At the outset, the court determined that the phrase "readily accessible to the general public" should be interpreted according to its ordinary meaning.[36] In determining whether the packet data at issue was "readily accessible to the general public" within the ordinary meaning of the phrase, the court noted that the wireless networks from which it had been intercepted did not require users to provide a password to connect.[37] As the court accurately explained, however, whether the network is "readily accessible to the general public," is not the relevant inquiry under the G1 exception.[38] According to the precise language of the statute, the question under the G1 exception is whether the network is configured in such a way that the *electronic communications it transmits* are "readily accessible to the general public."[39]

It is exceedingly important to preserve the distinction between a network's accessibility and the accessibility of the communications it transmits in the context of public wireless networks. Public Wi-Fi networks are not password protected because their purpose is to make the Internet freely accessible to members of the public. However, when Internet users connect to public Wi-Fi networks to send emails or visit websites, they still retain a strong expectation of privacy, despite their knowledge that others are also free to communicate over the network.[40] While the network itself is intended to be freely accessed, the communications sent over it are not.

Although the *Innovatio* court initially recognized the need to analyze the accessibility of the networks and communications sent over them separately, it did not preserve that distinction in its subsequent analysis under the G1 exception. Instead, the court mistakenly relied on the network's public-facing features to decide the separate question of whether the transmitted packet data was "readily accessible to the general public." With respect to the applicability of the G1 exception to the communications at issue, the court emphasized that the defendants' Wi-Fi networks lacked password protection, "allowing any customer who so desires to access the Internet through them."[41] In explaining why this feature of the *network* was relevant to whether the communications were publicly accessible, Chief Judge Holderman observed that, once connected, any user connected to the network could use a packet

35. *Id.* at 892 (quoting 18 U.S.C. § 2511(2)(g)(i) (2012)).

36. *See id.* at 892 n.5.

37. *See id.* at 892.

38. *Id.*

39. 18 U.S.C. § 2511(2)(g)(i).

40. *See In re Innovatio IP Ventures*, 886 F. Supp. 2d at 894 (noting that users of unencrypted Wi-Fi networks have a strong expectation of privacy in their online communications).

41. *Id.* at 892.

analyzer to capture other packet data traveling over the network.[42] The court found it noteworthy that Innovatio's own technicians used a packet analyzer device "which is available to the public for purchase for $698.00."[43] Based on the lack of any security measures to block the public from initially accessing the networks in question, the court concluded that the ability to intercept packet data from the networks rendered the data "readily accessible to the general public."[44]

In support of its holding that packet data is "readily accessible to the general public," the court paradoxically noted that the vast majority of the public is unaware that packet analyzers even exist.[45] To dispatch the apparent contradiction that members of the public can have ready access to communications through a technology that they do not know exists, Chief Judge Holderman reasoned that "[t]he public's lack of awareness of the ease with which unencrypted Wi-Fi communications can be intercepted by a third party is, however, irrelevant to a determination of whether those communications are 'readily accessible to the general public.'"[46] The court pointed out that "[t]he language of the exception does not, after all, refer to 'communications that the general public knows are readily available to the general public.'"[47] Consequently, the chief judge concluded that Innovatio's interception was permissible under the G1 exception "to the extent Innovatio's proposed sniffing protocol accesses only communications sent over unencrypted Wi-Fi networks available to the general public."[48]

The *Innovatio* court's interpretation of the G1 exception is legally flawed for three reasons. First, no other court in the United States has interpreted the G1 exception to mean that a third party's ability to carry out an interception—without more—is sufficient to render a communication "readily accessible to the general public." Second, the court failed to recognize that Congress designed the G1 exception to apply to a narrow category of communications that are intentionally configured to be intercepted by the public. Third, the court's interpretation of the G1 exception contravenes the plain meaning of the statutory language by conflating communications that are "readily accessible" with those that are merely "accessible." The court's interpretation broadened the G1 exception to authorize the interception of any and all communications made over Wi-Fi networks lacking password protection—including home Wi-Fi networks that are configured exclusively for private use. Instead, the district court should have interpreted the scope of the G1

42. *See id.* at 893 ("With a packet capture 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.").

43. *Id.*

44. *See id.*

45. *See id.*

46. *Id.* at 894 ("[T]he public's expectation of privacy in a particular communication is irrelevant to the application of the Wiretap Act as currently written.").

47. *Id.*

48. *Id.*

exception to include only those communications that are intended to be publicly accessible without the use of specialized surveillance technology.

First, rulings on the G1 exception from courts in other jurisdictions demonstrate that the *Innovatio* court misinterpreted the G1 exception by applying it to the interception of packet data. Courts interpreting the Wiretap Act have consistently recognized that the G1 exception does not permit the interception of electronic communications that are intended to remain private, even when the public possesses the technological capability to intercept them. In *In re Google Inc. Street View Electronic Communications Litigation*, a district court held that packet data falls outside the G1 exception based on an extensive examination of the legislative history of the Wiretap Act.[49] In *United States v. Ahrndt*, the U.S. Court of Appeals for the Ninth Circuit held that the G1 exception did not authorize police officers to intercept files from unsecured wireless networks, reversing a lower court decision based on a broad reading of the G1 exception.[50] And in *Tapley v. Collins*, a district court held that proper application of the G1 exception must account for both the intent of the network operator and the expectations of the individuals communicating over the network.[51] Each case is discussed in turn.

In *Google Street View*, the plaintiffs brought a consolidated class action lawsuit against defendant Google for allegedly violating the Wiretap Act by intercepting packet data from their home wireless networks.[52] The action arose from Google sending its employees into residential areas to intercept packet data from the residents' non-password-protected Wi-Fi networks during data collection for the Google Street View Project.[53] The data intercepted from the plaintiffs' networks contained email addresses, usernames, passwords, and other private data.[54] Google moved to dismiss the plaintiffs' claims under the Wiretap Act, arguing that the G1 exception authorized them to intercept the plaintiffs' data because the data packets were accessible to any third party with a packet analyzer.[55] In denying Google's motion to dismiss, the court held that the plaintiffs' data was not "readily accessible to the general public" despite the possibility that members of the public were capable of intercepting it with packet analyzers.[56]

Under the *Google Street View* court's interpretation of the G1 exception, packet data does not lose its protection against wiretapping merely because members of the

49. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1078–81 (N.D. Cal. 2011).

50. *See* United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *7 (D. Or. Jan. 28, 2010), *rev'd*, 475 F. App'x 656 (9th Cir. 2012).

51. *See* Tapley v. Collins, 41 F. Supp. 2d 1366, 1373 (S.D. Ga. 1999).

52. *See In re Google Inc. St. View*, 794 F. Supp. 2d at 1070; *see also* Electronic Communications Privacy Act, 18 U.S.C. § 2511–22 (2012).

53. *See In re Google Inc. St. View*, 794 F. Supp. 2d at 1071.

54. *See id.* at 1071–72.

55. *See id.*

56. *See id.* at 1082–83.

public can intercept it with packet analyzers.[57] Chief Judge Ware explained that while the networks themselves were accessible to the public because the plaintiffs chose not to password protect them, the "networks . . . were configured such that the packets were not readable by the general public without the use of sophisticated packet sniffer technology."[58] The court further acknowledged that packet sniffers were a type of "sophisticated decoding and processing technology" and "outside the purview of the general public."[59] Based on its assessment that the packet analyzers required specialized technical knowledge to operate and members of the general public rarely use them, the court concluded that unsecured packet data could not be considered "readily accessible to the general public."[60]

In *Google Street View*, the court based its narrow construction of the G1 exception on the Wiretap Act's legislative history.[61] The court used congressional intent as a guide to decide whether the G1 exception, which Congress created in 1986—prior to the spread of wireless Internet technology—could be appropriately applied in the context of Wi-Fi communications.[62] Because Congress did not have Wi-Fi communications in mind when it drafted the G1 exception, the *Google Street View* court sought to answer the question of whether the G1 exception could be properly applied by drawing an analogy between Wi-Fi communications and a type of technology that Congress did have in mind when it created the exception. After consulting reports on the 1986 amendments to the Wiretap Act from the Senate and House of Representatives, Chief Judge Ware determined that Wi-Fi networks were analogous to early cellular phone networks, which Congress intended to protect in the Wiretap Act despite the ability of third parties to intercept them with radio scanners.[63] Despite the public's ability to eavesdrop on these calls, Congress intended to extend privacy protection to these communications because they were sent over cell phones networks "designed to send communications privately, as in solely to selected recipients."[64] In the court's view, "Wi-Fi technology shares a common design with cellular phone technology . . . in that both types of technology are architected in order to make intentional monitoring by third parties difficult."[65] Based on this analogy between Wi-Fi and early cell phone networks, Chief Judge Ware concluded

57. *See id.* at 1071.

58. *Id.* at 1082.

59. *Id.* at 1082–83.

60. *See id.* at 1082.

61. *See id.* at 1078.

62. *See id.* at 1076 ("The drafting of these provisions predated the spread of wireless internet technologies . . . .").

63. In the 1980s, the primitive state of cellular phones made it possible to intercept calls with legal, commercially sold radio-scanning equipment. *See* S. Rep. No. 99-541, at 7 (1986), *reprinted in* 1987 U.S.C.C.A.N. 3555, 3561.

64. *In re Google Inc. St. View*, 794 F. Supp. 2d at 1082–83; *see also* S. Rep. No. 99-541, at 7–8 (noting that "unlike many signals which are more commonly scanned, the design of the cellular telephone system makes the intentional monitoring of specific calls more difficult because they are handed off among cells").

65. *In re Google Inc. St. View*, 794 F. Supp. 2d at 1082–83.

that the legislative intent behind the G1 exception precluded its application in the context of Wi-Fi communications.[66]

In *Google Street View*, the court's reliance on the legislative history of the G1 exception produced a more sensible interpretation of the phrase "readily accessible to the general public" as it applies to packet data. Unlike the court's truncated analysis of packet analyzers in *Innovatio*, the *Google Street View* court did not end its analysis when it found that packet analyzers give the public the power to intercept packet data;[67] rather, the *Google Street View* court held that the G1 exception could not authorize the interception of packet data after finding that members of the public generally lack the technical knowledge and skills required to intercept it.[68] Moreover, the level of sophistication required of third parties to capture data from Wi-Fi networks reflected the intent of network designers to make third-party interception more difficult, which the *Innovatio* court failed to consider.[69] Given its acknowledgement that the vast majority of the public is unaware that packet analyzers even exist, the *Innovatio* court should have followed the approach taken by the *Google Street View* court and construed the G1 exception more narrowly to exclude packet data.

At least one other court has rejected application of the G1 exception to unsecured Wi-Fi communications, doing so in a Fourth Amendment context. In *United States v. Ahrndt*, the Ninth Circuit reversed the decision of a lower court that closely resembled the holding in *Innovatio*.[70] In *Ahrndt*, police officers accessed the defendant's unsecured wireless network, where they were able to locate child pornography files in the shared iTunes library of the defendant's computer.[71] When the defendant moved to suppress the files on the grounds that the police obtained them in violation of the Wiretap Act, the district court held that the G1 exception authorized the interception because the files were "readily accessible to the general public."[72] The court concluded that the defendant's non-password-protected Wi-Fi network was "configured so that any electronic communications emanating from his computer via his iTunes program were readily accessible to any member of the general public with a Wi-Fi enabled laptop."[73]

On appeal, the Ninth Circuit reversed in an unpublished opinion, finding that the evidence failed to establish that the defendant intentionally configured his files

66. *See id.* at 1083.

67. *See id.* at 1082–83.

68. *See id.* at 1083.

69. *See id.* at 1084.

70. *Compare* United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994 (D. Or. Jan. 28, 2010), *rev'd*, 475 F. App'x 656 (9th Cir. 2012), *with In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 892–94 (N.D. Ill. 2012).

71. *See Ahrndt*, 2010 WL 373994, at *7.

72. *See id.* at *8 ("The access, however, was not illegal under the ECPA. On the contrary, because the wireless network and iTunes software were configured so that the general public could access them, access was expressly lawful under the ECPA.").

73. *Id.*

for public access.[74] Under the district court's erroneous interpretation of the G1 exception, the defendant's computer files qualified as "readily accessible to the general public" because any member of the general public could access them with a laptop.[75] But the Ninth Circuit overruled this interpretation, holding that, in order to lose privacy protection, there would need to be proof not only that the police officers *could* access the defendant's files, but that the defendant in fact took "affirmative actions to enable open sharing in this manner."[76] The Ninth Circuit remanded the case to the district court to determine whether the evidence was sufficient to establish either that the defendant had intentionally configured his files for public access, or that a program on the defendant's computer could have automatically configured his files to be accessible by others.[77]

In *Ahrndt*, the Ninth Circuit established an intent-based standard to determine whether data sent over unsecured Wi-Fi networks is entitled to privacy protection.[78] On remand, the district court applied this standard and granted the defendant's motion to suppress evidence obtained from his Wi-Fi network.[79] The court noted that—despite the defendant's failure to password protect his wireless network—the data available on his network was nevertheless entitled to privacy protection because he intended for its contents to remain private.[80] While the default configuration of his network inadvertently rendered his data accessible to third parties, the court held that such an inadvertent result did not legally permit third parties to access it.[81]

The *Innovatio* court repeated the *Ahrndt* court's error by applying the G1 exception to Wi-Fi data without accounting for the network users' intent. If the *Innovatio* court had instead applied the Ninth Circuit's intent-based standard to determine whether Innovatio had violated the Wiretap Act,[82] it would have recognized—as the Ninth Circuit did—that the ability of third parties to acquire access to private communications does not make the capture of private data a legal interception under the Wiretap Act.

---

74. *See Ahrndt*, 475 F. App'x at 658.

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

76. *Ahrndt*, 475 F. App'x at 657–58.

77. *See id.* at 658.

78. *See id.*; *see also* United States v. Ahrndt, No. 00468-KI, 2013 WL 179326, at *7 (D. Or. Jan. 17, 2013) ("[I]n response to the Ninth Circuit's query, there is no evidence Ahrndt 'intentionally' enabled sharing of his files over his wireless network.").

79. *See Ahrndt*, 2013 WL 179326, at *12 ("Ahrndt's Motion to Suppress evidence obtained from his storage media and the statements he made to the agents is granted.").

80. *See id.* at *6.

81. *See id.* at *7 ("Here, the evidence suggests Ahrndt unknowingly, and by default of the program, shared the content stored in his LimeWire folder over his home wireless network.").

82. Given the court's acknowledgement that the intercepted data contained private information such as passwords, contents of emails, and other confidential material, accounting for intent would have weighed heavily against a finding that the G1 exception applied.

The intent-based reading of the G1 exception has further support in *Tapley v. Collins*.[83] In *Tapley*, the district court held that the G1 exception did not authorize interception of cordless phone calls despite the fact that members of the public could intercept them with radio scanners.[84] Under the court's interpretation in *Tapley*, the G1 exception authorizes the interception of radio broadcasts intended for public use, but does not extend to cordless phone calls because "cordless telephones were never designed with that intent."[85] *Tapley* thus supports the proposition that courts should not focus solely on whether the public can intercept communications "as a matter of cost and practicality" when applying the G1 exception.[86]

As these cases demonstrate, the court in *Innovatio* cast the G1 exception too broadly. By focusing solely on the public's ability to intercept the data at issue, the court disregarded important factors that other courts have found to be dispositive to the G1 analysis. Rather, courts have reached narrower interpretations of the G1 exception when they account for the intent of the person who configured the network. These interpretations are more sensible because they provide privacy protection to communications which, despite eavesdroppers' ability to access, were never intended by either the network operator or the individuals sending them to fall into public hands.

Furthermore, the legislative history of the Wiretap Act contradicts the *Innovatio* court's expansive interpretation of the G1 exception, leaving public Wi-Fi users vulnerable to the exact type of privacy invasions that Congress sought to prevent when it amended the statute to protect electronic communications.[87] The legislative history of the Wiretap Act reveals that Congress created G1 as an exception of limited scope, authorizing the interception of a narrow class of communications intended for public access.[88] Yet reference to the legislative history of the G1 exception is conspicuously absent from the court's opinion.

Congress enacted the Wiretap Act in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[89] which prohibited the interception of oral and wire communications subject to three exceptions for law enforcement and

83. *See* Tapley v. Collins, 41 F. Supp. 2d 1366, 1373 (S.D. Ga. 1999).

84. *See id.* at 1373.

85. *Id.*

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

87. *Compare* S. Rep. No. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559 (suggesting that the lack of privacy protection may discourage the public's use of Wi-Fi), *with In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012) (holding that the public's expectation of privacy is irrelevant to the application of the Wiretap Act).

88. The *Google Street View* and *Tapley* courts also grounded their narrow interpretation of the G1 exception in the legislative history of the Wiretap Act. *See In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1079 (N.D. Cal. 2011); *see also Tapley*, 41 F. Supp. 2d at 1373.

89. S. Rep. No. 99-541, at 1.

telecommunications personnel.[90] In 1986, Congress amended the Wiretap Act to add protection for electronic as well as wire and oral communications.[91] As currently written, the Act defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[92] In *Innovatio*, the court concluded that because Wi-Fi networks transmit information using radio waves, packet data qualifies as "electronic communications" under the Wiretap Act.[93]

Congressional reports accompanying the 1986 amendments to the Wiretap Act clarify that Congress intended the G1 exception to apply to a limited class of communications. The G1 exception states that "[i]t shall not be unlawful . . . for any person to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[94] According to the House Report, Congress intended the word "configure" to "establish an objective standard of design configuration to begin determining whether a system receives privacy protection."[95] Rather than casting the exception so broadly that it encompasses all communications capable of being accessed by the public, Congress deliberately worded the G1 exception to include only communications that are "designed" to be "readily accessible to the general public."[96] Although Congress did not state whether communications must be *intentionally* designed for public access, the examples that it provided suggest that the intent of the network designer is important to the G1 analysis.[97]

In discussing which types of communications qualify as "readily accessible to the general public," Congress referred exclusively to communications intentionally transmitted for public use.[98] The Senate Report states that under the G1 exception, "it would not be unlawful to intercept subcarrier and [V]BI communications that are transmitted for the use of the general public. Such 'public' communications would include the stereo subcarrier used in FM broadcasting or data carried on the VBI to provide closed-captioning of TV programming for the hearing-impaired."[99] The first

90. *See* S. Rep. No. 90-1097, at 37 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153–54.

91. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended 18 U.S.C. §§ 2510–21, 2701–10, 3121–26 (2012)).

92. 18 U.S.C. § 2510(12) (2012).

93. *In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 890 (N.D. Ill. 2012) ("Neither party disputes that the allegedly infringing Wi-Fi networks transmit information using radio waves (which are a type of electromagnetic radiation), and thus transmit electronic communications.").

94. 18 U.S.C. § 2511(2)(g)(i).

95. H.R. Rep. No. 99-647, at 41 (1986). The Senate Report contains nearly identical language. *See* S. Rep. No. 99-541, at 18 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3572.

96. S. Rep. No. 99-541, at 18.

97. *See id.* at 18–19.

98. *See id.*

99. *Id.*

example refers to stereo subcarriers, which is a type of FM radio broadcast used to transmit dual sets of audio signals to FM radios that allows listeners to play sound in "stereo" rather than merely in "mono."[100] The second refers to VBI communications, or vertical blanking interval—the portion of a television broadcast carrying "information other than video or audio, such as closed-caption text and stock market data."[101] Both examples reference communications that were created for the purpose of public use and designed to be accessible with ordinary consumer electronics. FM subcarriers are designed to be detectable with any standard FM radio and VBI communications can be detected by any standard television set.[102] The House Report also contains a third example of communications that Congress considered to be "readily accessible to the general public," stating that "[a]n example of systems which are readily accessible include[s] loud speakers hooked up to a telephone system."[103]

These are the only three examples of "readily accessible" communications that Congress provided. Through exclusive reference to communications that have been intentionally configured for public access, Congress indicated that the parameters of the G1 exception were narrowly drawn. When accessing the communication requires an electronic device, the communication is accessible with the minimum technology ordinarily used to receive communications in that medium, such as a standard FM radio or television.[104] Taken together, these examples make clear that Congress intended to limit the scope of the G1 exception to communications that are readily accessible to the public without the use of specialized surveillance hardware.

Congress would thus reject the broad interpretation of the G1 exception adopted by the court in *Innovatio*. Congress had the opportunity to include within the G1 exception all communications that the public might gain access to, but deliberately cast the exception more narrowly. By example and explanation, Congress illustrated that communications must be intentionally designed for public use to qualify as "readily accessible to the general public."[105] In light of the legislative history of the G1 exception, the *Innovatio* court should have construed the G1 exception to exclude packet data, which contains personal information intended to remain private and cannot be accessed without surveillance equipment outside the knowledge of ordinary network users.

---

100. *See Subcarriers in F.M. Broadcasting*, Dayton Indus. Corp., http://www.daytonindustrial.com/scasub.htm (last updated Oct. 16, 1998); *see also Broadcast Radio Subcarriers or Subsidiary Communications Authority (SCA)*, Fed. Commc'ns Comm'n, http://www.fcc.gov/encyclopedia/broadcast-radio-subcarriers-or-subsidiary-communications-authority-sca (last visited Dec. 21, 2013) (describing a subcarrier as a "separate audio or data channel that is transmitted along with the main audio signal over a broadcast station").

101. Margaret Rouse, *Networking and Communications: Vertical Blanking Interval (VBI)*, WhatIs.com, http://whatis.techtarget.com/definition/vertical-blanking-interval-VBI (last updated Mar. 2011).

102. *See id.*

103. H.R. Rep. No. 99-647, at 41 (1986).

104. *See id.* at 9, 21, 47; *see also Subcarriers in F.M. Broadcasting*, *supra* note 100.

105. *See* H.R. Rep. No. 99-647, at 41.

The court's interpretation of the G1 exception is also vulnerable to a textualist critique. In *Innovatio*, the court embraced an interpretation of the G1 exception that contravenes the plain language of the Wiretap Act by ignoring a key term in the statute.[106] In order to adjust the definition of "readily accessible to the general public" to include packet data, the court effectively erased the term "readily" from the statute.[107] The private information contained within packet data cannot be characterized as "readily accessible" during its transmission over a Wi-Fi network. Before third parties can access the content of another user's data packets, they must locate and connect to a wireless network, operate a packet analyzer to capture the data, execute a program to record the data, and, finally, convert the data into a readable format using additional software.[108] Under the *Innovatio* court's interpretation, any communication will qualify as "readily accessible" if, theoretically, there exists some combination of steps and technologies that would enable a third party to access it. This interpretation of the G1 exception, under which the designation of a communication as "readily accessible" is nearly automatic if the technology exists to access it, places no limits whatsoever either on the number of affirmative steps that third parties must take or on the level of specialized knowledge they must possess to successfully intercept the communication. The court therefore engineered a definition of the G1 exception that fails to distinguish between communications that are merely "accessible" from those that qualify as "readily accessible."[109]

The *Innovatio* interpretation of the G1 exception has also been subject to this criticism in legal scholarship. For example, noted scholar Orin Kerr argues that courts must account for the intent of the network designer when they apply the G1 exception because intent is implicit in the language of the statute.[110] According to Kerr, the phrase "configured so that such electronic communication is readily accessible to the general public"[111] clearly "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."[112] Under Kerr's reading, the G1 exception applies only when a network is "set up consistently with a design that reflects an intent that members of the public would be able to monitor those communications."[113]

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

107. *See* Electronic Communications Privacy Act, 18 U.S.C. § 2511(2)(g)(i) (2012) (referring to communications that are "readily accessible to the general public").

108. *See In re Innovatio IP Ventures*, 886 F. Supp. 2d at 893 ("The software necessary to analyze the data that the packet capture adapters collect is available for download for free."); *see also Packet Sniffing Part 1*, SuraSoft, http://www.surasoft.com/articles/packetsniffing.php (last visited Dec. 21, 2013).

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

110. *See* Kerr, *supra* note 86.

111. 18 U.S.C. § 2511(2)(g)(i).

112. Kerr, *supra* note 86.

113. *Id.*

Instead, the *Innovatio* court's interpretation of the G1 exception, an exception that was designed to protect the public, inflicts the greatest harm on the general public. Public Wi-Fi networks are widely recognized as a societal asset because they provide fast and free Internet services that benefit the general public.[114] The advantages of public Wi-Fi networks cannot be achieved without user confidence in the privacy of their personal data. The *Innovatio* court's ruling, however, allows third parties to intercept personal data as it travels over any network open to the public. The court endorsed an interpretation of the Wiretap Act that will ultimately "discourage potential customers from using innovative communications systems" and prevent "American businesses from developing new innovative forms of telecommunications and computer technology."[115] Applying a less expansive interpretation of the G1 exception would have protected the privacy of individual users and preserved the integrity of public Wi-Fi networks, which are quickly becoming a valuable commodity in an increasingly interconnected world.

114. The benefits of public Wi-Fi networks have been noted in the areas of innovation, business and economic development, and emergency services. *See Reasons for Open Wireless*, Open Wireless Movement, https://openwireless.org/ (last visited Dec. 21, 2013).

115. S. Rep. No. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.