Minnesota Journal of Law, Science & Technology

Volume 15 | Issue 2 Article 10

2014

Aligning Online Privacy Protection with Reasonable Expectations of Privacy: How Joffe Can Be Used to Modernize the Wiretap Act

Matthew Mason

Comment

Aligning Online Privacy Protection with Reasonable Expectations of Privacy: How *Joffe* Can Be Used to Modernize the Wiretap Act

*Matthew Mason**

Between May 2007 and 2010, as part of its popular Street View project, Google collected an enormous amount of Wi-Fi data transmitted from unencrypted networks throughout the United States and over thirty countries worldwide.[1] After initially denying the collection of any payload data,[2] Google publicly acknowledged that fragmented samples of payload data were collected from open Wi-Fi networks due to a code mistakenly included in its Street View software.[3] Several months later, however, Google admitted that the data collected was not just fragmentary in nature;[4] in some instances the full content of e-mails, URL searches, passwords, and financial transactions were collected.[5] In response to what has been

---

* JD Candidate, 2015, University of Minnesota Law School. The author would like to thank the entire staff of MJLST for their hard work throughout the year, and, in particular, thanks to the MJLST editors and staff who did a tremendous job revising and editing this Comment. The author also thanks Professor William McGeveran for providing guidance and feedback throughout the process.

1. Google Inc., 27 FCC Rcd. 4012, 4012 (Apr. 13, 2013) (notice of apparent liability) [hereinafter FCC Notice]; *see In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011).

2. *In re Google*, 794 F. Supp. 2d at 1071 (describing how Google claimed, on April 27, 2010, that only SSIDs and MAC addresses were collected).

3. FCC Notice, *supra* note 1, at 4012 (providing that Google acknowledged the collection of fragmented payload data on May 14, 2010). "[I]t's now clear that we have been mistakenly collecting samples of payload data . . . even though we never used that data in any Google products." *Id.* at 4015 (quoting Alan Eustace, *WiFi Data Collection: An Update*, GOOGLE OFFICIAL BLOG, http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (last updated June 9, 2010)).

4. *Id.* at 4012–13 (explaining how Google admitted for the first time that non-fragmented payload data was indeed captured).

5. *Id.*

called a "big brother-like . . . invasion of privacy,"[6] investigations have been launched in the United States[7] and abroad.[8]

In a private action against Google, the Northern District of California denied Google's motion to dismiss a claim alleging that Google's collection of payload data from unencrypted Wi-Fi networks violated the Wiretap Act.[9] The Ninth Circuit affirmed, holding that Wi-Fi communications do not constitute an "electronic communication . . . readily accessible to the general public" under the Wiretap Act, and thus are not exempt from liability.[10]

The Ninth Circuit's ruling in *Joffe v. Google, Inc.* raises a number of important issues that may have significant implications on privacy protections for Internet and other electronic communication. *Joffe* exposed our current privacy protection framework as inadequate for new technologies and advancements in communication. Such inadequacy raises the question as to what extent, and in what way, Congress must update the Wiretap Act to accommodate a changing communication landscape since the enactment of the Electronic Communications Privacy Act (ECPA) in 1986.[11] Furthermore, it becomes necessary to consider whether users of unsecured

---

6. Cecilia Kang, *Growing Anger over Google Street View Privacy Breach*, POST TECH. (May 20, 2010, 8:00 AM), http://voices.washingtonpost.com/posttech/2010/05/the_anger_is_growing_over.html (quoting Washington D.C. Council Member Jim Graham).

7. Juliana Gruenwald, *FTC Drops Probe of Google Wi-Fi Snooping*, NAT'L J., http://www.nationaljournal.com/daily/ftc-drops-probe-of-google-wi-fi-snooping-20101027 (last updated Oct. 27, 2010, 3:42 PM); Kristena Hansen, *37 States Join Probe into Google Wi-Fi Data Collection*, L.A. TIMES (July 21, 2010, 1:46 PM), http://latimesblogs.latimes.com/technology/2010/07/google-street-view.html; Amy Schatz & Amir Efrati, *FCC Investigating Google Data Collection*, WALL ST. J. (Nov. 11, 2010, 2:01 PM), http://online.wsj.com/news/articles/SB10001424052748704804504575606831614327598.

8. *See* FCC Notice, *supra* note 1, at 4019, 4023–24 (citing Canadian, French, and Dutch investigations which all concluded that Google's collection of payload data violated applicable data protection or online privacy laws).

9. *In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1084 (N.D. Cal. 2011); *see* Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), Pub. L. No. 90-351, § 802, 82 Stat. 197, 213–14 (codified as amended at 18 U.S.C. § 2511 (2012)).

10. Joffe v. Google, Inc., 729 F.3d 1262, 1265 (9th Cir. 2013) (quoting 18 U.S.C. § 2511(2)(g)(i) (2012)).

11. *See* Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848.

Wi-Fi networks have a reasonable expectation of privacy in their transmitted electronic communications. As a corollary, it is important to examine how offline Fourth Amendment principles may be applied to an increasingly online society to protect an individual's electronic and Internet communications.

This Comment seeks to examine how Congress, and the courts, might use *Joffe* as a springboard to bring privacy protections up to date with technological and communication advances. Part I will summarize how Wi-Fi communication works and the accompanying threats to privacy, examine the current statutes that protect against the interception of communications, summarize the Federal Trade Commission (FTC) investigation of the Street View incident, and assess the current protection for online communication under the Wiretap Act as well as basic principles of privacy law. Part II will comment on the reasoning and holding advanced by the *Joffe* court, and place *Joffe* in context with the current state of the law as described in Part I. Finally, Part III will argue that Congress and courts should use *Joffe* to align the reality of users' knowledge of Wi-Fi technology and reasonable expectations of privacy with the Wiretap Act. This Comment concludes that Congress should amend the ECPA to expressly protect both encrypted and unencrypted Wi-Fi transmissions, and that courts should adapt offline Fourth Amendment principles to protect online and other electronic communications.

I. UNDERSTANDING CURRENT WI-FI TECHNOLOGY, ON- AND OFFLINE PRIVACY PROTECTION, AND THE FCC GOOGLE INVESTIGATION

A. WI-FI TECHNOLOGY, PACKET SNIFFING, AND LOCATION DATA

Wi-Fi constitutes any kind of wireless local area network that uses radio waves to connect laptops and other devices to the Internet.[12] Wi-Fi networks operate on Industrial, Scientific,

12. Brief of Appellant Google Inc. at 3, Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013) (No. 11-17483) [hereinafter Brief of Appellant]; Mani Potnuru, Note, *Limits of the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing*, 111 MICH. L. REV. 89, 93 (2012).

and Medial (ISM) radio bands.[13] Wireless networks use different ISM band frequency ranges, with each range further divided into channels.[14] Wi-Fi enables point-to-point communication between specific devices, sent directly from one device to another.[15] A wireless access point (WAP) connects to a user's Internet Service Provider (ISP) through a wired connection and communicates over radio frequencies to devices equipped with a Wi-Fi adapter.[16] The WAP only allows authenticated devices to associate with, and use, the Wi-Fi network.[17]

To facilitate communication with other devices, the WAP transmits a signal providing basic information about the Wi-Fi network.[18] The transmitted information includes a device's medium access control (MAC) address,[19] and service set identifier (SSID).[20] A device's MAC address and SSID are unencrypted,[21] and can be automatically detected by most computers and smartphones.[22] Devices capable of Wi-Fi connectivity use the MAC address and SSID to connect with a WAP and communicate over the Internet.[23]

---

13. *See* Potnuru, *supra* note 12, at 93 (providing that ISM bands are unregulated frequencies which are part of the radio spectrum that may be used by anyone).

14. *See id.* at 93–94 (explaining that each wireless network is "configured to operate on one of these channels").

15. Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of Appellees and Urging Affirmance at 9, Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013) (No. 11-17483) [hereinafter EPIC Brief].

16. *See* Potnuru, *supra* note 12, at 93 (comparing a WAP to a short-range cell tower, and Wi-Fi adapters to radio receivers).

17. EPIC Brief, *supra* note 15, at 22. Authenticated devices are able to connect to the Internet and each other through the WAP. FCC Notice, *supra* note 1, at 4014–15.

18. FCC Notice, *supra* note 1, at 4014–15; Brief of Appellant, *supra* note 12, at 4.

19. FCC Notice, *supra* note 1, at 4015. A MAC address is a numeric identifier for each WAP. Brief of Appellant, *supra* note 12, at 4.

20. An SSID identifies the particular wireless local area network (LAN). FCC Notice, *supra* note 1, at 4015.

21. *Id.* (explaining that a device's MAC address and SSID are considered non-content data).

22. Brief of Appellant, *supra* note 12, at 4.

23. FCC Notice, *supra* note 1, at 4015.

Wi-Fi networks are either encrypted or unencrypted.[24] Network owners commonly forgo encryption for a variety of reasons,[25] such as to foster public access to information,[26] lack of technological expertise,[27] and the fact that users must affirmatively enable mechanisms to ensure encryption.[28] Additionally, technological limitations make it difficult to create a secured, encrypted network within a public hotspot.[29] Regardless of encryption, Wi-Fi communications are coded and sent only to specific destinations.[30] The transmitted data becomes encapsulated into frames, which are then fragmented and sent over the Wi-Fi network.[31] Wi-Fi signals travel short distances, usually only enough to cover one's home.[32]

Despite the coded nature of Wi-Fi transmissions, packet sniffing presents a significant privacy threat to electronic communications sent over a wireless network. In essence, packet sniffers are a type of wiretap applied to Wi-Fi networks in order to monitor, intercept, and read data of transmitted electronic communications.[33] Packet sniffers have the ability to collect and read e-mails, web searches, passwords, financial

---

24. Brief of Appellant, *supra* note 12, at 5. Encryption permits a user to ensure that communication made over the network remains private. Potnuru, *supra* note 12, at 94 (citing password protection as an example of encryption, making interception very difficult, if not nearly impossible).

25. Brief of Appellant, *supra* note 12, at 5.

26. *Id.*; Bruce Schneier, *Steal This Wi-Fi*, WIRED (Jan. 10, 2008), http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0110.

27. Potnuru, *supra* note 12, at 94–95.

28. *Id.* at 94 (explaining that the factory default settings of most routers and WAPs are set to operate in open mode).

29. *Id.* at 95, 107; *see also* EPIC Brief, *supra* note 15, at 29 (concluding that no practical solutions currently exist to address this problem).

30. Joffe v. Google, Inc., 729 F.3d 1262, 1278 (9th Cir. 2013); *see* EPIC Brief, *supra* note 15, at 12, 23 (stating that a device must be authenticated to send and receive communication over a Wi-Fi network).

31. EPIC Brief, *supra* note 15, at 23–24.

32. Brief of Plaintiffs-Appellees Benjamin Joffe, et al. at 16, Joffe v. Google, Inc., 729 F.3d 1262 (9th Cir. 2013) (No. 11-17483) [hereinafter Brief for Plaintiffs-Appellees]. Wi-Fi devices tend to have a range of 70 feet through 300 feet, whereas an AM radio broadcast can cover up to 100 miles. EPIC Brief, *supra* note 15, at 17.

33. EPIC Brief, *supra* note 15, at 32; *Packet Sniffing*, INTERNET SECURITY SYS., http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Packet_sniffing/default.htm (last visited Oct. 30, 2013).

transactions, and even credit card numbers.[34] With the use of advanced technology, packet sniffers can capture, decode, and re-package fragmented Wi-Fi communications.[35]

Furthermore, the increasingly popular use of geolocation technology to gather location data raises another concern.[36] Currently, MAC address mapping is the most commonly used method to gather location data, and involves a location provider (such as a Street View car) using a GPS device to detect MAC addresses of individually owned routers.[37] The GPS device then measures a router's signal strength and GPS coordinates.[38] MAC addresses for visible wireless routers are then submitted to a database, which returns the individual user's location.[39] Smartphones regularly transmit the name, location, and signal strength of nearby networks to a company like Apple or Google, enabling the phone company to pinpoint a user's location.[40] Additionally, many popular apps use and occasionally share location data absent the user's knowledge or consent.[41] A huge market for location-based services exists that is unlikely to disappear anytime soon.[42]

---

34. EPIC Brief, *supra* note 15, at 32. Packet sniffers are becoming increasingly easy to install on routers, which is troublesome because the presence of sniffers are often very difficult to detect. *Packet Sniffing*, *supra* note 33. Programs such as Firesheep are available for free online and make it easy to see what other users on an unsecured network are doing. Kate Murphy**,** *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, N.Y. TIMES, Feb. 17, 2011, http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html. However, the technical expertise required to use packet sniffing programs is relatively uncommon. Potnuru, *supra* note 12, at 110–11.

35. EPIC Brief, *supra* note 15, at 24, 30–32 (explaining that sniffing programs tend to require sophisticated software and hardware to implement).

36. Gathering of location data with geolocation technology started with Skyhook's "wardriving" program in 2003. *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://online.wsj.com/news/articles/SB10001424052748703983704576277101723453610.

37. Raymond Chow, Note, *Why-Spy? An Analysis of Privacy and Geolocation in the Wake of the 2010 Google "Wi-Spy" Controversy*, 39 RUTGERS COMPUTER & TECH. L.J. 56, 61 (2013).

38. *Id.*

39. *Id.* at 61–62.

40. Angwin & Valentino-Devries, *supra* note 36.

41. *Id.*

42. *See id.* (stating that in 2010 a $2.9 billion market existed for location-based services, with an expected increase to $8.3 billion by 2014). Furthermore, location-based features are some of the most popular features online. Peter Fleischer, *Greater Choice for Wireless Access Point Owners*,

B. STATUTORY PRIVACY PROTECTION FOR COMMUNICATIONS

Statutory protections against the interception of communications are relatively recent developments in the United States. In 1968, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act) to create a private action for the interception of communications.[43] The Wiretap Act, however, expressly limited protection to the "unauthorized aural interception" of wire or oral communications.[44]

In order to update and clarify federal privacy protections to align with changes in communication technology, Congress passed the ECPA in 1986.[45] In doing so, Congress sought to protect an individual's privacy rights in computer-to-computer transmissions of data and e-mail.[46] Another goal of Congress was to protect radio hobbyists from liability for innocently scanning frequencies of traditional radio broadcasts in order to reach public communications.[47]

A number of ECPA subsections were particularly relevant in *Joffe*. Subsection 2511(1) assigns liability to "any person

---

GOOGLE OFFICIAL BLOG (Nov. 14, 2011, 2:00 AM), http://googleblog.blogspot.com/2011/11/greater-choice-for-wireless-access.html.

43. Wiretap Act, Pub. L. No. 90-351, § 802, 82 Stat. 197, 223 (codified as amended at 18 U.S.C. § 2520 (2012)). The Department of Justice notes that the Wiretap Act generally bars third parties from installing packet sniffers capable of reading Internet traffic. DEP'T OF JUSTICE CRIMINAL DIV., COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 167 (2009).

44. *In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1077–78 (N.D. Cal. 2011).

45. Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848; S. REP. No. 99-541, at 5 (1986) ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances."); *see* H.R. REP. No. 99-647, at 16–19, 31 (1986) (expressing worry about the gradual erosion of privacy rights and attempting, through the passage of the ECPA, to keep privacy protection of electronic communication consistent with Fourth Amendment expectations of privacy); *see also In re* Pharmatrak, Inc., 329 F.3d 9, 18 (1st Cir. 2003) (stating that the objective of the ECPA was to protect against the interception of electronic communication).

46. *See* S. REP. No. 99-541, at 2, 5 (suggesting that e-mail should receive similar privacy protections as regular mail); *see also* H.R. REP. No. 99-647, at 22 (stating that individuals likely have a reasonable expectation of privacy in their e-mail communications).

47. *See, e.g.*, S. REP. No. 99-541, at 4.

who: (a) intentionally intercepts, endeavors to intercept . . . any wire, oral, or electronic communication."[48] Importantly, two exceptions from Wiretap Act liability are provided by § 2511(2)(g)(i) and (g)(ii).[49] Subsection 2510(12) defines electronic communication as "any transfer of . . . data, or intelligence of any nature transmitted in whole or in part by wire, [or] radio."[50] Subsection 2510(16) defines "'readily accessible to the general public' . . . with respect to a radio communication" as any communication that is not included in the five explicit exceptions provided by the statute.[51]

In 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA), which, under § 2510(16), added a new exception to the presumption of accessibility pertaining to electronic communications.[52] The amendment sought to extend ECPA protection to new forms of wireless data communication.[53] Despite Congress' good intentions, the § 2510(16) amendment led a rather short life.

Congress amended the ECPA once again through the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA).[54] While primarily focused on habeas corpus reform and anti-terrorism efforts, the AEDPA removed the § 2510(16) explicit exception to the presumption of accessibility for electronic communications added by the CALEA two years

---

48. 18 U.S.C. § 2511(1)(a) (2012).

49. It is not unlawful for any person: "(i) 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." 18 U.S.C. § 2511(2)(g)(i). Additionally, it is not unlawful for any person: "(ii) to intercept any radio communication which is transmitted . . . ." 18 U.S.C. § 2511(2)(g)(ii) (providing four explicit circumstances where it is lawful to intercept radio communication).

50. 18 U.S.C. § 2510(12) (2012).

51. 18 U.S.C. § 2510(16); *see In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1079–80 (N.D. Cal. 2011) (stating that § 2510(16) raises a presumption of accessibility and enumerates five specific exceptions for what is not considered readily accessible).

52. Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, § 203, 108 Stat. 4279, 4291 (1994) (codified as amended at 18 U.S.C. § 2510(16)).

53. *See* H.R. REP. No. 103-827, pt. 1, at 14 (1994) (recommending the extension of ECPA protection to cover new forms of wireless data communication); *see also* S. REP. No. 103-402, at 32 (1994) (discussing the rationale for the ECPA amendment).

54. Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), Pub. L. No. 104-132, 110 Stat. 1214, 1303.

prior.[55] Legislative history suggests Congress believed electronic communications were adequately protected prior to the passage of the CALEA; the CALEA amendment only intended to make it abundantly clear that electronic communications were protected under the ECPA.[56] Aside from the protection provided by the ECPA, CALEA, and AEDPA, federal privacy law remains relatively unchanged since the passage of the Wiretap Act over forty years ago.[57]

C. FTC AND FCC GOOGLE INVESTIGATIONS

The FTC became the first U.S. agency to conduct an investigation, albeit short lived, addressing Google's collection of payload data.[58] The FTC informed Google that it would be dropping its investigation just days after Google publicly admitted it had collected non-fragmented payload data.[59] David Vladeck, then-director of the Bureau of Consumer Protection (a division of the FTC), dropped the investigation on account of the actions Google took in the wake of the Street View incident.[60] For example, Google implemented a new "opt-out" policy through which a user may change their SSID to end with the designation "_nomap" to prevent data from being collected.[61] Encouragingly, the FTC has since called on

---

55. *Id.* It remains unclear what exactly Congress intended to accomplish by removing the § 2510(16) amendment provided by the CALEA. *See* Joffe v. Google, Inc., 729 F.3d 1262, 1276 (9th Cir. 2013).

56. *See* H.R. REP. No. 104-518, at 80, 93 (1996) (Conf. Rep.).

57. Lindsey A. Strachan, *Re-mapping Privacy Law: How the Google Maps Scandal Requires Tort Law Reform*, RICH. J.L. & TECH., 1, 10 (Spring 2011), http://jolt.richmond.edu/v17i4/article14.pdf.

58. Gruenwald, *supra* note 7.

59. *Id.* A number of privacy advocate organizations, including the EPIC and the Center for Digital Democracy, criticized the FTC's decision to drop the probe and even questioned the "influence Google has over the Obama administration." *Id.*

60. Such actions included appointing a new director of privacy management, implementing privacy training for "key employees," incorporating a privacy review process, and pledging to delete the collected payload data as soon as possible. *Id.*

61. Chow, *supra* note 37, at 73–74; Fleisher, *supra* note 42; *see also* Wayne Rash, *Google's WiFi Opt-Out Process Makes Users Navigate Technical Maze*, EWEEK.COM (Nov. 15, 2011), http://www.eweek.com/c/a/Mobile-and-Wireless/Googles-WiFi-Optout-Process-Makes-Users-Navigate-Technical-Maze-696453/ (discussing the difficulties most people would face with implementing the opt-out policy, the failure of the policy to protect users'

Congress to implement tougher consumer privacy rules—particularly legislation that would regulate data brokers who compile and sell a range of personal and financial data.[62]

On November 3, 2010, the Federal Communications Commission (FCC) sent an initial letter of inquiry requesting information on how Google collected the payload data, what Google collected, and whether any data had been examined or used.[63] Google provided minimal information, and admitted to not making a comprehensive review of the FCC request, stating it would be "time consuming" and "burdensome."[64] Overall, the investigation did not run smoothly. Google hindered and delayed the FCC's investigation by failing to respond to requests for material information and through repeated failures to provide an affidavit stating Google's responses were truthful and complete.[65]

In the end, the FCC found that not only did a Google software engineer deliberately write the code used in the Street View cars with the intention to collect payload data,[66] but evidence suggested that as early as 2007 or 2008, numerous members of Google's Street View team had access to the code.[67]

---

rights, and the benefits of implementing an opt-in policy as opposed to the selected opt-out policy).

62. *See* Tanzina Vega & Edward Wyatt, *U.S. Agency Seeks Tougher Consumer Privacy Rules*, N.Y. TIMES, Mar. 26, 2012, http://www.nytimes.com/2012/03/27/business/ftc-seeks-privacy-legislation.html?pagewanted=all (presenting the FTC's concerns about the high volume of data being collected and how little control consumers have over that data, and the FTC's position that consumers should have access to information collected about them in addition to having the ability to correct and update that information).

63. FCC Notice, *supra* note 1, at 4018–19.

64. *Id.* at 4020. Google did admit, however, that employees on the Street View team had actually reviewed the payload data on two occasions. *Id.*

65. *Id.* at 4013 (finding that Google willfully and repeatedly violated FCC orders throughout the investigation).

66. *Id.* at 4021. The engineer wrote the code with the intention to collect, store, and analyze the payload data offline for use in location-based services and potentially other Google initiatives. *Id.* at 4021–22. Ultimately, over 600 gigabytes of data (including 200 gigabytes of payload data, some of which was personally identifiable) were collected and stored on servers at Google's data center. *See* Joffe v. Google, Inc., 729 F.3d 1262, 1264 (9th Cir. 2013).

67. FCC Notice, *supra* note 1, at 4028. For example, the code design document cited privacy considerations that were never discussed. Google Inc., FCC No. DA 12-592, File No. EB-10-IH-4055, at 11 (Apr. 13, 2012). In addition, based on e-mails from 2006 collected by the FCC during the investigation, the design engineer made the Street View team (including a senior manager) aware that payload data would be collected. *Id.* at 14–15.

Additionally, the FCC investigation exposed a lack of supervision over the collected Wi-Fi data and a general disregard of privacy considerations.[68]

The FCC investigation determined that Google's code utilized a packet sniffer to capture, separate, and store the MAC address and SSID of individual WAPs.[69] The sniffer would then search for "encryption flags," and either discard data from encrypted networks or capture all wireless frame and payload data from unencrypted networks.[70] Ultimately, Google's source code discarded data sent over encrypted networks, but not the data transmitted over open networks.[71]

D. CURRENT ONLINE PRIVACY PROTECTIONS

When discussing online privacy protections it is important to note that the primary statutory framework in the United States, the ECPA, became law prior to the Internet era.[72] As a result, courts and scholars alike argue that the existing federal framework is poorly suited to address modern forms of communication.[73] Without change, privacy protection of Internet and electronic communications will likely remain "confusing and uncertain."[74] New communications technology

---

Moreover, another Street View engineer allegedly conducted a "line-by-line" review of the Wi-Fi project in 2007, and claimed he did not realize the code would collect payload data. *Id.* at 17. Despite the fact that members of the Street View team clearly should have been aware that they were collecting payload data, those who worked on the Street View project "uniformly" asserted they did not know about the data collection until April or May of 2010. *Id.* at 17.

68. *See* FCC Notice, *supra* note 1, at 4027, 4033 (finding that the privacy considerations listed in the design document were never reviewed by counsel, nor by other Street View employees, and that a Street View senior manager pre-approved the code before it was written).

69. *Id.* at 4016–17.

70. The packet sniffer would search for encryption flags; if the sniffer determined the frame was encrypted, the data was cleared, and if the frame were unencrypted the payload data would be written onto a memory disk. *See id.* at 4016–17.

71. *Id.* at 4017.

72. *E.g.*, Konop v. Hawaiian Airlines, Inc. 302 F.3d 868, 874 (9th Cir. 2002).

73. *See, e.g.*, *id.* ("[T]he existing statutory framework is ill-suited to address modern forms of communication like . . . [a] secure website.").

74. *Id.*; *see* Matthew Beirlein, Note, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 OHIO ST. L.J. 1123, 1126 (2006) (arguing that inconsistent legal responses to the treatment of open wireless networks

undoubtedly leads to new privacy problems, yet privacy protections failed to keep pace.[75] The failure of protections to keep pace with technological developments are especially disconcerting, given the fact that privacy harms might be worse now than ever before.[76]

Although the legislative history shows Congress passed the ECPA in order to protect electronic communications from interception, with a particular concern for e-mail communications,[77] courts cannot agree on how to protect online privacy. For example, some courts have found that users enjoy a reasonable expectation of privacy in e-mail communications,[78] while others have placed considerable limitations on the protection of such communication.[79] Additionally, courts

---

will create confusion among users and may ultimately hamper technological development).

75. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 483, 564 (2006) (explaining that privacy problems are much different today than yesterday, in that online privacy threats generally do not involve physical intrusion); *see also* City of Ontario v. Quon, 560 U.S. 746, 758–61 (2010) (explaining that new technology inherently means that certain modes of communication will be used more than others, which increases the need to recognize privacy rights in such forms of communication); United States v. Ahrndt, No. 10-30281, 2010 WL 373994, at *6 (D. Or. Jan. 28, 2010), *rev'd*, 475 F. App'x 656 (9th Cir. 2012) (stating that the extent to which the Fourth Amendment protects electronic communications is unresolved); Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 76–77 (2007) (discussing the gap between young peoples' expectations of privacy on the internet (selective anonymity) and those of older generations (control-centered expectation that resulted from living in an era where one had greater control over personal information)); Strachan, *supra* note 57, at 6 (describing a general disconnect between views of privacy then and now).

76. Reputational harms are more permanent and tangible than ever. *See* Sanchez Abril, *supra* note 75, at 75 (citing the permanence, searchability, replicability, and transformability of personal information data, and the "multitude of often unintended audiences" with access to such data).

77. *See* S. REP. No. 99-541, at 2, 8 (1986) (describing new technological developments at the time and defining "electronic mail").

78. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) (finding a reasonable expectation of privacy in e-mails); United States v. Szymuszkiewicz, 622 F.3d 701, 703 (7th Cir. 2010) (finding a violation of the Wiretap Act when an employee configured a supervisor's e-mail to be sent to himself); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (holding that a user has a reasonable expectation of privacy in the underlying content of e-mails).

79. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (holding that e-mail content no longer remains private once received, thus losing any reasonable expectation of privacy a user might have had); *see also* Allyson W.

disagree as to whether communication over Wi-Fi networks is exempt from Wiretap Act protection.[80] Courts also disagree about the existence of privacy protections for users of online social networks (OSNs).[81]

It is difficult to discern any particular trend in online privacy case law, but the weight of authority seems to suggest that whether a reasonable expectation of privacy in Internet communications exists depends on an individual's utilization of privacy-ensuring measures.[82] Non-content data such as a WAP, MAC address, IP address, and SSID, are not typically considered to have an accompanying reasonable expectation of privacy.[83] The distinction between individual users'

Haynes, *Virtual Blinds: Finding Online Privacy in Offline Precedents*, 14 VAND. J. ENT. & TECH. L. 603, 631–32, 638 (2012) (discussing the limited privacy protections granted to e-mail communications, and the majority view that e-mail content no longer remains private once received on account of the third-party doctrine).

80. *Compare* Joffe v. Google, Inc., 729 F.3d 1262, 1276 (9th Cir. 2013) (holding that Wi-Fi communications do not constitute an "electronic communication . . . readily accessible to the general public"), *and In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1083 (N.D. Cal. 2011) (holding that Wi-Fi communications are not radio communications, and thus not exempt under the ECPA's G1 exception), *with* United States v. Ahrndt, No. 10-30281, 2010 WL 373994, at *5–6 (D. Or. Jan. 28, 2010), *rev'd*, 475 F. App'x 656 (9th Cir. 2012) (holding that unencrypted Wi-Fi networks are readily accessible to the general public, and that a diminished expectation of privacy exists for data transferred over unsecure networks), *and In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 893–94 (N.D. Ill. 2012) (holding that communication sent over an unencrypted Wi-Fi network is considered readily accessible to the general public and excluded from Wiretap Act protection).

81. *Compare* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (holding that privacy protections for posts on social networks depend upon the use of privacy controls), *with* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 652–57 (N.Y. Sup. Ct. 2010) (holding that no expectation of privacy exists on an OSN, regardless of one's efforts to utilize privacy controls).

82. Haynes, *supra* note 79, at 638; *see*, *e.g.*, United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (holding that a user's expectation of privacy in the information contained on one's computer can be diminished by one's conduct and use of the computer); *Ahrndt*, 2010 WL 373994, at *6 (stating that society recognizes a lower expectation of privacy when using an unsecured network). *But see* United States v. Jones, 132 S. Ct. 945, 954 (2012) (concluding that the transmission of electronic signals remain subject to the *Katz* reasonable expectation of privacy test).

83. *See Forrester*, 512 F.3d at 510 (holding that no reasonable expectation of privacy exists in non-content and addressing information); Johnson v.

expectations regarding the access and use of Wi-Fi networks and their expectations that private data sent over such networks will remain private creates an additional complication.[84] Generally, users lack awareness of the privacy risks involved when communicating over Wi-Fi networks (encrypted or unencrypted),[85] and yet expect that such communications will remain private.

E. OFFLINE PRIVACY PRINCIPLES

The right to privacy developed and found its roots in the Fourth Amendment.[86] Since then, two influential articles have single-handedly shaped the development of privacy law.[87] Samuel Warren and Louis Brandeis tend to be considered the founders of privacy law.[88] Warren and Brandeis described the individual[89] right to privacy as the "right to be let alone,"[90] which built on similar rights in other legal areas.[91] Following the publication of Warren and Brandeis's article, privacy tort law experienced significant growth and experimentation.[92] During this time period, judicial analysis of privacy actions focused on whether the resulting harm fell under the principle of the right to be let alone.[93]

Over eighty years after Warren and Brandeis, Professor William Prosser wrote an article establishing the principles of

---

Microsoft Corp., No. C06-0900RAJ, 2009 WL 1794400, at *4 (W.D. Wash. June 23, 2009) ("[A]n IP address is not personally identifiable . . . .").

84. Potnuru, *supra* note 12, at 104.

85. *See id.* at 105.

86. U.S. CONST. amend. IV.

87. *See* Strachan, *supra* note 57, at 9–10.

88. *See id.* at 9.

89. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 383 (1960); Strachan, *supra* note 57, at 9 (explaining that Warren and Brandeis wanted to prevent the affairs of private individuals from being exposed to "undesirable publicity"). Warren and Brandeis believed that the resulting harm from privacy violations was primarily mental and emotional. *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1916 (2010).

90. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193, 198 (1890) (arguing that each individual has the right to determine to what extent his thoughts will be communicated to others).

91. *See* Strachan, *supra* note 57, at 9–10.

92. Richards & Solove, *supra* note 89, at 1922, 1924 (explaining that privacy tort law experienced a period of dynamism pre-Prosser).

93. *Id.* at 1915.

privacy law still in effect today.[94] In his article, Prosser delineated four privacy torts—each designed to protect a different aspect of privacy.[95] The four torts seek to protect against (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity that places an individual in false light in the public eye; and (4) the appropriation of one's name or likeness.[96] Prosser expressed concern that privacy law may expand and invade upon other distinct legal fields, and as a result, sought to steer it toward a limited and cautious path.[97] Stemming from Prosser's caution, scholars have begun to question the effectiveness of current privacy tort law.[98] Some scholars argue that Prosser made privacy tort law static and limited its ability to grow and adapt to privacy concerns relevant in today's society.[99] As a result, scholars increasingly believe that Prosser's four torts provide little guidance on how to shape future developments.[100]

The realm of privacy law is certainly more complex than Prosser's four torts.[101] The lack of changes in privacy tort law since Prosser, however, has left the tort system ill-equipped to address modern privacy claims such as those raised in *Joffe*.[102] It does not help matters that courts tend to be dismissive and skeptical of electronic communication privacy harms.[103] Moreover, the narrow and traditional judicial conception of privacy as a binary, all or nothing approach is no longer

---

94. Strachan, *supra* note 57, at 10; *see* RESTATEMENT (SECOND) OF TORTS § 652A-I (1977) (codifying Prosser's four privacy torts). Nearly every state recognizes at least one form of privacy tort by statute or common law. Richards & Solove, *supra* note 89, at 1917.

95. Prosser, *supra* note 89, at 389 (viewing the four torts as four distinct invasions of four different interests, unrelated to one another with almost nothing in common); Strachan, *supra* note 57, at 10. Prosser's methodology involved analyzing and restating the holdings of many privacy-related cases. Richards & Solove, *supra* note 89, at 1912.

96. Prosser, *supra* note 89, at 389.

97. *See* Richards & Solove, *supra* note 89, at 1887, 1906, 1915 (arguing that Prosser refused to allow privacy to mean more than his four torts).

98. *E.g.*, *id*. at 1889 (stating that most scholars believe privacy tort law has largely been ineffective).

99. *Id*. at 1887, 1922.

100. *Id*. at 1890.

101. Solove, *supra* note 75, at 483.

102. *E.g.*, Strachan, *supra* note 57, at 8.

103. *See* Richards & Solove, *supra* note 89, at 1922 (reasoning that the court's skepticism stems from the usual lack of a physical component).

sensible.[104] Regardless of the limitations faced by privacy tort law, and that private party conduct on its own fails to implicate Fourth Amendment principles,[105] this Comment argues that offline privacy principles can and should be applied to online privacy claims.[106]

II. *JOFFE V. GOOGLE, INC.*: CLASSIFYING PAYLOAD DATA TRANSMITTED OVER UNENCRYPTED WI-FI NETWORKS UNDER THE WIRETAP ACT

On November 8, 2010, Benjamin Joffe filed a class action suit against Google alleging that the interception of payload data from unencrypted Wi-Fi networks was in violation of 18 U.S.C. § 2511(1) of the Wiretap Act.[107] The district court faced a "novel question of statutory interpretation" as to the applicability of the § 2510(16) definition of "readily accessible" to the G1 exception (an express exemption to Wiretap Act protection),[108] and how to properly define "radio communication" under the Wiretap Act.[109] Ultimately, the district court denied Google's motion to dismiss.[110] Through an examination of the statute's text and legislative history, the

---

104. *See id*. at 1920 (arguing for the need to move away from the public-private dichotomy since information is rarely, if ever, completely one or the other).

105. United States v. Young, 153 F.3d 1079, 1080 (9th Cir. 1998).

106. *See* Kyllo v. United States, 533 U.S. 27 (2001); United States v. Jacobsen, 466 U.S. 109, 117, 122, 125 (1984); Katz v. United States, 389 U.S. 347, 351–54, 361 (1967) (establishing the test for what constitutes a reasonable expectation of privacy); Olmstead v. United States, 277 U.S. 438, 465–66 (1928); Byars v. United States 273 U.S. 28, 29 (1927); Ostergren v. Cuccinellie, 615 F.3d 263, 290 (4th Cir. 2010); Nat'l Cable & Telecomms. Ass'n v. FCC, 567 F.3d 659 (D.C. Cir. 2009); *Young*, 153 F.3d at 1080; Sanders v. Am. Broad. Cos., 978 P.2d 67, 71–72 (Cal. 1999); Nader v. Gen. Motors Corp., 255 N.E.2d 765 (N.Y. 1970).

107. *In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1072–74 (N.D. Cal. 2011).

108. "G1" refers to 18 U.S.C. § 2511(2)(g)(i) (2012), stating that "[i]t shall not be unlawful under this chapter . . . 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."

109. *In re Google*, 794 F. Supp. 2d at 1074, 1080 (noting that Congress failed to define "radio communication" in the Act and also declined to explain the applicability of § 2510(16) to the G1 exception).

110. *Id*. at 1084.

district court held that § 2510(16) applies to G1,[111] "radio communication" does not include data transmitted over a Wi-Fi network,[112] and that Wi-Fi data sent over an unencrypted network is not "readily accessible to the general public."[113]

Following the district court's judgment, Google sought and received an interlocutory appeal.[114] The *Joffe* court inherited the task of resolving three primary issues of statutory interpretation: (1) whether the § 2510(16) definition of "readily accessible to the general public" applies to G1; (2) whether payload data sent over an unencrypted Wi-Fi network is considered to be a radio communication; and (3) whether such Wi-Fi communications are "readily accessible to the general public" (under the ordinary meaning of the phrase).[115] The *Joffe* court became the first circuit to rule on the aforementioned issues, which gave the court an opportunity to provide much needed clarification as to the level of statutory privacy protection afforded to modern, electronic communications.[116] It remains to be seen whether *Joffe* will be used as a catalyst to provide a necessary update to privacy protections for modern forms of communication, or plunge the already muddled and outdated state of online privacy protection into further disarray.

A. "RADIO COMMUNICATION" DOES NOT INCLUDE PAYLOAD DATA SENT OVER WI-FI NETWORKS

Google once more urged the court to broadly define "radio communication" as "any information transmitted using radio waves."[117] Since the Wiretap Act does not define "radio

---

111. In addition, the court held that Congress did not intend the § 2510(16) definition of "readily accessible" to apply to electronic communication not classified as a "traditional radio service." *See id.* at 1081 (excluding the applicability of § 2510(16)'s definition to Wi-Fi communication).

112. The court defined radio communication as "traditional radio services or broadcast radio." *Id.* at 1083 (rejecting Google's proposed technical definition of "all communications transmitted over radio waves").

113. *Id.* at 1083.

114. Joffe v. Google, Inc., 729 F.3d 1262, 1265 (9th Cir. 2013).

115. *Id.* at 1267.

116. *See* Hanni Fakhoury, *What the Google Street View Decision Means for Researchers (and Cops)*, ELECTRONIC FRONTIER FOUND. (Sept. 16, 2013), http://www.eff.org/deeplinks/2013/09/what-google-street-view-decision-means-researchers-and-cops.

117. *Joffe*, 729 F.3d at 1268.

communication," the court assigned the term its ordinary meaning.[118] After determining that Google's proposed definition does not conform to the common understanding of "radio communication,"[119] the court rejected Google's definition.[120] The court reasoned that since Congress provided technical definitions for similar terms in the Wiretap Act, but did not for "radio communication," Congress intended the phrase to be given its ordinary meaning.[121]

As a result, the *Joffe* court defined "radio communication" as a "predominantly auditory broadcast," thus excluding payload data sent over unencrypted Wi-Fi networks.[122] The court concluded that defining "radio communication" as a "predominantly auditory broadcast" ensured consistency with the rest of the Wiretap Act.[123] The court reasoned that the different usage of the terms "radio communication" and "communication by radio" throughout the Wiretap Act,[124] the manner in which "radio communication" is used in G2 (an express exemption to Wiretap Act protection),[125] the avoidance

---

118. *Id.*

119. In common, everyday use, neither watching television nor sending an e-mail over a Wi-Fi network is considered to be a radio communication. *See id.* at 1268–69 (reasoning that under Google's interpretation, a TV broadcast would fall under the umbrella of "radio communication" and that one would not consider TV to be a type of "radio communication").

120. The court reasoned that the Wiretap Act does not assume that "radio communication" includes technology outside of the scope of the phrase's ordinary definition. *Id.* at 1269. For example, the Wiretap Act's damages provision provides separate penalties for intercepting satellite video communications and radio communications. *See id*. (pointing out that satellite television communications are described separately from radio communications, despite both transmitting over radio frequencies).

121. *Id.*

122. The payload data captured by Google included "emails, usernames, passwords, images, and documents," none of which can be classified as "predominantly auditory." *Id.* at 1270.

123. *Id.* at 1270.

124. The court reasoned that the phrase "communication by radio" is used more expansively throughout the Wiretap Act, encompassing all communication using radio waves. *Id.* Throughout the Wiretap Act, words that evoke traditional radio technology surround the phrase "radio communication," lending support to the ruling that "radio communication" refers narrowly to traditional broadcast radio technology. *Id.* at 1271.

125. "G2" refers to 18 U.S.C. § 2511(2)(g)(ii) (2012), which states: "It shall not be unlawful under this chapter . . . for any person . . . to intercept any radio communication which is transmitted . . . by any station for the use of the general public . . . ." While the G2 exception is not at issue in *Joffe*, the court

of absurd results inconsistent with the Wiretap Act,[126] and the inapplicability of the Communication Act's definition of "radio communication"[127] all support defining "radio communication" as a "predominantly auditory broadcast."

In arguing for a broad definition of "radio communication," Google heavily relied on two amendments that altered § 2510(16).[128] In 1994, Congress adopted § 2510(16)(F), which provided that with respect to a radio communication, electronic communications are not "readily accessible to the general public."[129] Two years later, however, Congress repealed § 2510(16)(F).[130] Google argued that by repealing § 2510(16)(F), Congress eliminated the only protection for unencrypted data sent over a Wi-Fi network.[131] The *Joffe* court rejected Google's interpretation, holding that nothing indicates what Congress intended by repealing § 2510(16)(F), and instead elected to follow the ordinary meaning of "radio communication."[132]

---

reasoned that under Google's definition it would not make sense to identify certain types of "radio communication" (that have little in common with Wi-Fi technology) to be exempt under G2 only to exempt broad, dissimilar communications (such as payload data transmitted over a Wi-Fi network) in G1. *Joffe*, 729 F.3d at 1271. Rather, it makes more sense to read the general G1 exemption in light of the specific exemptions in G2. *Id.* at 1272.

126. For example, if Google's broad definition were appropriate, protection for online communications under the Wiretap Act would turn on "whether the *recipient* of those communications" secured his or her Wi-Fi network. *Joffe*, 729 F.3d at 1272. Given that the primary purpose of the Wiretap Act is to effectively protect the privacy of communications, the court reasoned that Congress clearly did not intend to permit "such an intrusive and unwarranted invasion of privacy." *Id.*

127. The Communication Act broadly defines the phrase "radio communication." *Id.* at 1274. Congress expressly stated, however, when it wanted to apply a definition from the Communication Act to the Wiretap Act, and did not do so with respect to "radio communication." *Id.* Additionally, unlike the Wiretap Act, the phrases "radio communication" and "communication by radio" are used synonymously throughout the Communication Act. *Id.*

128. *Id.* at 1274–75; *see* AEDPA, Pub. L. No. 104-132, 110 Stat. 1214 (1996); CALEA, Pub. L. No. 103-414, § 203, 108 Stat. 4279, 4291 (1994) (codified as amended at 18 U.S.C. § 2510(16) (2012)).

129. *Joffe*, 729 F.3d at 1275.

130. *Id.*

131. Essentially, Google interpreted the amendments as standing for the notion that both before 1994 and after 1996, payload data sent over Wi-Fi networks are considered to be a "radio communication" which is "readily accessible to the general public." *See id.* at 1276.

132. *Id.* The court reasoned that the decision to add § 2510(16)(F) does not show that Congress believed data sent over a Wi-Fi network to be a "radio

B. THE § 2510(16) DEFINITION OF READILY ACCESSIBLE APPLIES TO G1

For two primary reasons, the court in *Joffe* agreed with Google and held that the definition of "readily accessible" in § 2510(16) applies to G1.[133] First, the Wiretap Act treats "radio communication" as a subset of "electronic communication."[134] Second, the Wiretap Act expressly provides that the definitions established in § 2510 apply to the entire chapter.[135] While the *Joffe* court could not disregard the statutory directive to apply § 2510(16) to G1, the court did hold that the § 2510(16) "readily accessible" definition only applies to G1 when the electronic communication at issue is also a "radio communication."[136] Therefore, because the court determined that Wi-Fi data sent over an unencrypted network is not considered a "radio communication," the § 2510(16) definition of "readily accessible" does not apply here.[137]

C. WI-FI COMMUNICATIONS ARE NOT READILY ACCESSIBLE TO THE GENERAL PUBLIC

After determining that payload data sent over an unencrypted Wi-Fi network is not a "radio communication" under the Wiretap Act, thus rendering § 2510(16) inapplicable, the *Joffe* court considered whether such transmissions are "readily accessible" under the ordinary meaning of the phrase.[138] After a short analysis, the court held that because

---

communication." *Id.* Additionally, no legislative history explains why Congress decided to repeal § 2510(16)(F). *Id.* The court then provided two plausible rationales, neither of which were consistent with Google's interpretation, to explain the decision to repeal § 2510(16)(F): (1) to eliminate redundancy; and (2) to eliminate the incoherence created by § 2510(16)(F). *Id.* (reasoning that § 2510(16)(F) made it seem as though electronic communications are a subset of radio communications, despite the fact that the Wiretap Act treats the latter as a subset of the former).

133. *Id.* at 1267.

134. *Id.*; *see* 18 U.S.C. § 2510(12) (2012) (defining electronic communication as "any transfer of data . . . transmitted in whole or in part by . . . *radio*" (emphasis added)).

135. *Joffe*, 729 F.3d at 1267; *see* 18 U.S.C. § 2510 (prefacing with the phrase "[a]s used in this chapter").

136. *Joffe*, 729 F.3d at 1266.

137. *Id.* at 1268.

138. The court determined that although the transmissions at issue fall outside of § 2510(16), such a transmission may still be considered "readily

payload data sent over Wi-Fi networks are not "readily accessible to the general public," Google may not escape liability through the use of G1.[139]

First, the court reasoned that unlike traditional radio broadcasts, Wi-Fi transmissions are significantly limited geographically.[140] Wi-Fi broadcasts are limited to a peak output of one watt, whereas other traditional radio broadcasts range from 250 to 100,000 watts.[141] Wi-Fi broadcasts often do not travel far beyond one's home or office, and tend to have a service range of less than 330 feet.[142] By contrast, an AM radio broadcast boasts a service range of up to 100 miles.[143]

Second, the court found that payload data transmitted over an unencrypted Wi-Fi network is difficult to intercept and access.[144] As opposed to traditional radio broadcasts, a wireless device must be authenticated before it may communicate with a WAP.[145] Additionally, Wi-Fi communications are encoded even if sent over an unencrypted network, and are sent only to a specific destination.[146] This method of communication makes intercepting and decoding data extremely difficult without sophisticated hardware and software.[147] Most of the general public lacks the technical expertise to intercept and decode such data.[148] As a result, the *Joffe* court affirmed the district court's decision.[149]

---

accessible to the general public" and exempt from liability under G1. *Id.* at 1277.

139. *Id. But see* United States v. Ahrndt, No. 10-30281, 2010 WL 373994, at *5 (D. Or. Jan. 28, 2010), *rev'd*, 475 F. App'x 656 (9th Cir. 2012) ("I conclude that society recognizes a lower expectation of privacy in information broadcast via an unsecured wireless network . . . .").

140. *Joffe*, 729 F.3d at 1277.

141. *Id.* at 1278.

142. *Id.*

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.* In order to intercept and decode payload data transmitted over a Wi-Fi network, a wireless device (generally a packet sniffer) must connect with the Wi-Fi network and proceed to send encapsulated and coded data to a specified destination (in Google's case, to the Street View cars and eventually their data storage facility). *Id.*

148. *Id.* Even if members of the general public commonly connect to a neighbor's unsecured Wi-Fi network, such individuals usually do not mistakenly intercept, store, and decode payload data. *Id.* at 1279.

149. *Id.* at 1278–79.

III. GETTING DOWN TO BRASS TACKS: ANALYZING THE SHORTCOMINGS OF *JOFFE*, THE RESULTING POLICY IMPLICATIONS, AND A PROPOSAL TO EFFECTIVELY PROTECT THE PRIVACY OF ONLINE COMMUNICATION

Considering that the issues presented to the *Joffe* court were primarily matters of statutory interpretation,[150] the court did a good job of resolving the issues in front of them. The court did fail, however, to take advantage of an opportunity to provide clarification and guidance as to what types of electronic communications are actually protected under the Wiretap Act. Additionally, unlike what we have seen in a number of other courts,[151] the *Joffe* court did not make use of Fourth Amendment privacy principles to address modern forms of electronic communication.[152] Perhaps the most glaring shortcoming of the *Joffe* decision, however, was the court's scant analysis of what "readily accessible to the general public" means in ordinary terms under the G1 exemption.

The *Joffe* decision failed to address a number of gaps in our current privacy protection framework relating to modern electronic communication technologies. As a result, the Wiretap Act continues to provide uncertain and inadequate privacy protection for modern electronic communications. On account of the court's failure to address the disconnect between Wi-Fi users' understanding of Wi-Fi technology and their expectations of privacy when using such technology, the gap between expectations and legal reality will likely continue to worsen. Furthermore, due to the increasing use of cell phones to collect location data[153] and the ever-growing market for

---

150. *See, e.g.*, *id.* at 1270 ("Throughout the Wiretap Act, Congress used the phrase 'radio communication' . . . . [T]he phrase 'radio communication' tends to refer more narrowly to broadcast radio technologies rather than to the radio waves by which the communication is made.").

151. *See supra* Part I.D.

152. *Joffe*, 729 F.3d at 1275–77.

153. *See* Ellen Nakashima, *Agencies Collected Data on Americans' Cellphone Use in Thousands of Tower Dumps,* WASH. POST (Dec. 8, 2013), http://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html ("Federal, state and local law enforcement agencies conducting criminal investigations collected data on cellphone activity thousands of times last year . . . . Data linked to specific cell towers can be used to track people's movements.").

location-based services,[154] electronic communication privacy protections (or, more appropriately, lack thereof) may very well be headed down a slippery slope.[155]

Recognizing the fact that the *Joffe* court's ability to effectuate change was rather limited on account of the nature of the case itself (exclusively resolving questions of statutory interpretation), the holdings that Wi-Fi communications are not considered to be a "radio communication" nor "readily accessible to the general public" were a step in the right direction.

Congress should use *Joffe* as a springboard to update the Wiretap Act to expressly protect unencrypted Wi-Fi transmissions in order to bring the reality of Wi-Fi users' knowledge and reasonable expectations of privacy in line with the law. By establishing a distinction between content and non-content data, imposing new requirements on device manufacturers, and applying offline Fourth Amendment principles to the online world, Congress would be able to provide effective privacy protections for modern electronic communications. It is time to acknowledge and address the fact that modern communication technologies have rapidly outpaced statutory and judicial privacy protections.

A. THE SHORTCOMINGS OF *JOFFE*

1. What *Joffe* Got Right

An important element of the *Joffe* decision that went relatively unnoticed was the court's willingness to view online privacy as something more than a binary, all or nothing concept.[156] Had the court adopted a binary approach, one likely result may have been that encrypted Wi-Fi networks would be considered protected under the Wiretap Act, while unencrypted

---

154. *See* SYNIVERSE, LOCATING AN OPPORTUNITY: THE RISE OF CELLULAR NETWORKS AS A METHOD FOR LOCATION-BASED SERVICES 2 (2013), *available at* http://www.syniverse.com/files/Rise_of_Cellular_Networks_as_LBS.pdf ("Although location-based services have been available for nearly ten years, their usage has only started to grow significantly in the last few years.").

155. *See supra* note 42 and accompanying text.

156. *Cf.* Richards & Solove, *supra* note 89, at 1891, 1922 (emphasizing the necessity of rethinking outdated understandings of privacy by abandoning a binary, all or nothing approach, and arguing that courts must change their approach to privacy protections in order to effectuate this change in understanding).

Wi-Fi networks would be considered "readily accessible to the general public." This type of binary approach would have led to the absurd results the *Joffe* court worked to avoid.[157] The *Joffe* court once more rejected the binary approach in holding that the applicability of G1 does not turn on whether the Wi-Fi *network* itself is accessible (unencrypted/encrypted distinction), but instead on whether the *communication* itself is readily accessible.[158] Privacy advocates point out that the *Joffe* court's rejection of the binary approach provides a strong rationale that law enforcement must now, at least in the Ninth Circuit, obtain a wiretap order or warrant to access an individual's Wi-Fi communications.[159]

It is hard to argue against the court's conclusion that the § 2510(16) "readily accessible" definition applies to G1 to the extent that such communication involved is not only electronic, but also radio.[160] After all, the statute provides specific instructions to apply the definitions found in § 2510 to the chapter's entirety.[161]

Furthermore, the *Joffe* court appropriately held that the Wi-Fi communications at issue are not a type of "radio communication" under the Wiretap Act.[162] By using the ordinary, non-technical definition of "radio communication," the court limited the reach of the § 2510(16) presumption that radio communications are "readily accessible to the general public."[163] After determining that "radio communications" are "predominantly auditory broadcasts," the court logically concluded that § 2510(16) did not apply to G1 in this instance since Wi-Fi transmissions are not considered to be "radio communications."[164] While it is quite clear that Wi-Fi differs

---

157. *See supra* note 126 and accompanying text.

158. Joffe v. Google, Inc., 729 F.3d 1262, 1275–77 (9th Cir. 2013).

159. Fakhoury, *supra* note 116.

160. *See Joffe*, 729 F.3d at 1265–66 (rejecting Joffe's interpretation that § 2510(16) applies exclusively to G2); *see also* Brief of Plaintiffs-Appellees, *supra* note 32, at 38 (arguing that since "readily accessible" is not defined with respect to electronic communications, as it is with respect to radio communications, the ordinary meaning should be used in G1).

161. *See supra* note 135 and accompanying text.

162. *See supra* Part II.A.

163. *See In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1081 (N.D. Cal. 2011) (describing the "presumption of accessibility" established by Congress in § 2510(16)).

164. *See supra* Part II.B.

from traditional radio broadcast services, the *Joffe* court failed to espouse a general principle to guide the legislature and other courts, who may now face the task of classifying a different form of modern communication technology as radio or non-radio.

2. Inadequate Analysis of the G1 Exemption

In stark contrast to the court's thorough analysis of whether payload data transmitted over an unsecured Wi-Fi network is properly classified as a "radio communication," the court glossed over what "readily accessible" means in ordinary terms under G1. The court determined that on account of the geographically limited range of Wi-Fi networks and the apparent difficulty of intercepting and decoding Wi-Fi transmissions, such transmissions are not "readily accessible to the general public" under G1.[165]

By limiting the holding to Wi-Fi transmissions, the court missed an opportunity to provide clarification and guidance as to when certain communications are considered "readily accessible" in ordinary terms, thus excluding their interception from liability under G1. Arguably, the language used in G1 suggests that what matters is the intended purpose behind the designs of certain communication technology, as opposed to whether such technology might be able to be used contrary to the designer's intention.[166] Simply put, whether something is considered "readily accessible" under G1 should depend on whether the technology itself is designed to make communications readily available to the public, and not whether an individual could engage in wiretapping "as a matter of cost and practicality."[167] If the focus lies anywhere else other than on the design of the communication technology and its intended purpose, it is difficult to see how Wi-Fi transmissions over an unencrypted network are not "readily

165. *See supra* Part II.C.

166. *See* 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/ ("The issue under 2511(2)(g)(i) is what the designers intended users to be able to do, not what someone can do contrary to the designer's intentions.").

167. *See id.*

accessible to the general public" under the phrase's ordinary meaning. By adopting such an approach, the *Joffe* court may have avoided significant criticism surrounding the holding that Wi-Fi transmissions are not "readily accessible" under the phrase's ordinary meaning.[168]

3. Failure to Incorporate Fourth Amendment Privacy Principles, Clarify Which Electronic Communications Are Protected, and Provide Guidance Moving Forward

As previously mentioned, the *Joffe* court failed to consider the applicability of Fourth Amendment privacy principles in relation to modern communication technologies.[169] Although it would have been difficult for the court to utilize a Fourth Amendment analysis given the nature of the case, numerous other courts have begun to adopt such an analysis.[170] Given the high profile nature of *Joffe* and the growing disconnect between old notions of privacy protection and modern technological issues,[171] applying Fourth Amendment privacy principles to Wi-Fi communications may have gone a long way towards updating and enhancing our current online privacy protections.[172]

Throughout the *Joffe* opinion, the court seemingly tried to jam Wi-Fi transmissions into a definition that would bring it under the Wiretap Act's protection. This approach represents more of a patch, as opposed to a long-term solution, for addressing the gaps in our current privacy protection framework as applied to new communication technologies. Such an approach simultaneously fails to provide guidance to Congress or lower courts and creates uncertainty for security

---

168. *See, e.g.*, *Wi-Fi Isn't Radio!?*, KISMET (Sept. 12, 2013), http://www.blog.kismetwireless.net/2013/09/wi-fi-isnt-radio.html ("[T]he ruling seems to think it's difficult to monitor Wi-Fi . . . . I'm not too confident about that assertion.").

169. *See supra* note 106 and accompanying text.

170. *See, e.g.*, *supra* note 106.

171. *Cf.* Strachan, *supra* note 57, at 3 (arguing that "current tort law is inadequate for such technologically advanced legal issues"); *see also* S. REP. No. 99-541, at 5 (1986) ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment.").

172. *See infra* Part III.C.3; *cf., e.g.*, Brief of Plaintiffs-Appellees, *supra* note 32, at 21 (arguing that the primary concern in passing the ECPA centered on individual privacy protection utilizing Fourth Amendment privacy protections as a touchstone to keep protections of electronic communications in line with the Fourth Amendment).

researchers and similarly situated individuals.[173] The primary purpose of the Wiretap Act is to effectively protect the privacy of communications generally, and not simply Wi-Fi communications.[174] Cabining the opinion to Wi-Fi transmissions and analyzing the case solely as a problem of statutory interpretation failed to resolve lingering uncertainty as to what types of modern electronic communications are protected by the Wiretap Act.

B. POTENTIAL POLICY RAMIFICATIONS

In addition to doing little to resolve the lingering uncertainty surrounding the applicability of the Wiretap Act to other forms of modern electronic communications, *Joffe* may encourage various detrimental policy ramifications.

A sizeable and ever-growing market currently exists for location-based services.[175] The fact that the development of geolocation technology has outpaced domestic statutory privacy protections in the United States[176] makes the billion-dollar market for location-based services particularly troubling. Of even more concern is that in the wake of Google's Wi-Fi debacle, companies such as Apple and Google have begun crowdsourcing the collection of location data to millions of smartphone users.[177] Under Android default privacy settings,

---

173. One of the primary negative technological implications of the court's decision is that individuals seeking to capture unencrypted Wi-Fi packets for legitimate research purposes may now face liability under the Wiretap Act. *Wi-Fi Isn't Radio!?*, *supra* note 168.

174. *See In re* Pharmatrak, Inc., 329 F.3d 9, 18 (1st Cir. 2003) (stating the objective of the ECPA was to protect against the interception of electronic communications); S. REP. No. 99-541, at 5 (amending the Wiretap Act to protect against electronic communication interception in light of changes in new computer technologies); *see also* Brief of Plaintiffs-Appellees, *supra* note 32, at 33 (noting that all previous amendments to the Wiretap Act were passed to keep pace with new technologies and to protect emerging forms of communication).

175. *See supra* note 42.

176. Chow, *supra* note 37, at 62.

177. Angwin & Valentino-Devries, *supra* note 36 ("Google and Apple are gathering location information as part of their race to build massive databases capable of pinpointing people's locations via their cellphones."); *see also In re* Google Android Consumer Privacy Litig., 802 F. Supp. 2d 1372, 1373 (J.P.M.L. 2011) ("These actions share factual questions arising out of the manner in which Google's Android operating system (Android OS) or apps downloaded to devices running the Android OS collect, store and/or transfer user information, including location information.").

smartphones report GPS locations and available Wi-Fi networks (among other things) to Google's collection systems.[178] A similar process occurs on Apple's iPhone.[179] Companies then use the geolocation data to create large databases of Wi-Fi hotspots.[180]

In the past, most data about people's behavior over wireless networks have been collected from PCs and generally could only be tied to a certain city or zip code.[181] The increasing popularity of Wi-Fi enabled smartphones, however, allows user data to be collected with much greater precision to specific locations.[182] Moreover, a number of popular smartphone apps use location and personal data more aggressively than Google or Apple, occasionally sharing such data with third parties without the user's knowledge or consent.[183] Such practices demonstrate the enormous potential for abuse presented by new forms of electronic communication technology in the absence of updated statutory protections.[184]

Without the express statutory protection of Wi-Fi communications sent over unencrypted networks, there exists a real possibility that we may incidentally chill the use and development of new Wi-Fi technology.[185] It is logical to expect that if one's bank account statements, e-mails, and passwords accessed over an unencrypted Wi-Fi network are held to be "readily available to the general public," that the use of such technology will decline. This may be especially true in light of the fact that reputational privacy harms created by online

178. Chow, *supra* note 37, at 71.

179. An unencrypted file on iPhones that recorded where the phone has been—and when—was discovered, with the collected data stored by default. Angwin & Valentino-Devries, *supra* note 36.

180. *Id.*

181. *Id.*

182. *Id.*

183. *Id.*

184. Although the example is a bit extreme, a man was able to obtain the social security number and work address of a female through a database company, and then proceeded to go to the female's workplace and kill her. Richards & Solove, *supra* note 89, at 1923.

185. *See* EPIC Brief, *supra* note 15, at 33 ("Holding that unsecure Wi-Fi communications are not protected from interception under the Wiretap Act would place unreasonable burdens on Wi-Fi users.").

electronic communications may very well be more tangible and permanent than ever.[186]

Along the same vein as other courts that have dealt with online privacy protections, *Joffe* did not take into consideration the importance of a typical Wi-Fi network user's understanding of how Wi-Fi works and their expectations of privacy when communicating over a Wi-Fi network.[187] A typical user who accesses a neighbor's unsecured network clearly knows that the network itself is not secure, yet because of a limited understanding of Wi-Fi technology and the accompanying security risks, such a user still expects private communications to remain secure.[188]

Although steps can be taken to secure Wi-Fi networks, typical users often find it difficult to activate or enable such features.[189] The disconnect between the general public's understanding of Wi-Fi technology and the accompanying security risks,[190] the widely held expectation of privacy in private communications transmitted over a Wi-Fi network, and our outdated statutory privacy protections can best be resolved by updating the Wiretap Act to expressly protect certain types of modern electronic communications. Congress must start taking into account the modern social contexts in which private communications are shared online, and the reasonable expectations the general public has about this shared information.[191]

C. A PROPOSAL: HOW AND WHY CONGRESS SHOULD AMEND THE WIRETAP ACT TO EXPRESSLY PROTECT WI-FI TRANSMISSIONS

Instead of relying on piecemeal, judicially imposed resolutions to effectively protect modern electronic communications, Congress should focus on amending the

---

186. Sanchez Abril, *supra* note 75, at 87.

187. *See, e.g.*, Potnuru, *supra* note 12, at 105–07 (explaining the distinction between a user's expectations regarding Wi-Fi access and use, and the expectation that data sent over Wi-Fi networks will remain private).

188. *Id.*

189. *Id.*

190. *See, e.g.*, *id.* at 105 ("Users . . . are typically unaware that data transmitted over such unsecured Wi-Fi networks can still be intercepted unless the data is somehow still encrypted.").

191. *Cf.* Richards & Solove, *supra* note 89, at 1922 (providing suggestions to reform tort law to address current privacy problems).

Wiretap Act to expressly protect Wi-Fi communications and similar electronic communications.[192] Since the inception of the Wiretap Act, last amended by the ECPA in 1986, the technological landscape has clearly undergone significant changes. Privacy problems today are much different than those of yesterday, and the paramount goal of any amendment should be to remove the current unpredictability and uncertainty surrounding privacy protections of modern electronic communications.[193] Any amendment must be carefully designed in order to account for inevitable future technological developments in addition to increasingly sophisticated packet sniffing technology. In the words of Warren and Brandeis, "the elasticity of our law . . . which has enabled it to meet the wants of an ever changing society . . . ha[s] been its greatest boast."[194]

1. The Content/Non-Content Distinction

To provide comprehensive protection for modern forms of electronic communication, including Wi-Fi transmissions, the Wiretap Act should be amended to incorporate a content/non-content distinction for liability. Essentially, any electronic communications consisting merely of non-content data would be considered "readily accessible" and thus exempt from Wiretap Act protection, whereas the interception of content data would give rise to Wiretap Act liability. For example, when looking at an e-mail, the actual text and substance of the e-mail itself would be considered content data and protected under the Wiretap Act. On the other hand, an e-mail's addressing information would be considered non-content data and therefore "readily accessible to the general public" under G1. Such an approach not only maintains the old function of offline privacy protections within a new technological environment,[195] but also conforms to the general public's

192. After all, new technology gives rise to new privacy problems. Solove, *supra* note 75, at 483.

193. *See* Solove, *supra* note 75, at 564; Warren & Brandeis, *supra* note 90, at 193.

194. Warren & Brandeis, *supra* note 90, at 193.

195. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1017–18 (2010) (replacing the inside/outside distinction applicable to offline privacy protection with a content/non-content distinction for online privacy protection).

reasonable expectations of privacy.[196] Encouragingly, recent court decisions have pointed towards adopting a content/non-content distinction.[197]

2. Imposing New Requirements on Device Manufacturers

Currently, factory default settings for the majority of Wi-Fi equipment is set to operate in an open, unsecured manner.[198] Therefore, unless a user manually enables the available security features, Wi-Fi networks continue to run as an unencrypted network. As mentioned earlier, much of the general public either lacks the technical knowledge to secure their Wi-Fi network, or simply may be unaware of the privacy risks involved with operating an unsecured network.[199] Furthermore, security standards for Wi-Fi networks often change, which places a heavy burden on even tech-savvy consumers to keep up with the current standards.[200]

A relatively easy way to address the gap between the general public's understanding of Wi-Fi technology and expectations that their Internet communications will remain private would be to statutorily require manufacturers and developers of Wi-Fi devices to provide secure default settings. Statutory requirements would go a long way towards protecting an individual's privacy online, and would address a root cause of the online privacy problem. Despite the absence of such statutory regulations, Wi-Fi device manufacturers have already begun to ship devices that provide secure default settings.[201]

3. Applying Offline Fourth Amendment Principles to the Online World

On top of imposing new statutory requirements for electronic communication device manufacturers instituting a content/non-content distinction, Congress and the judiciary

196. *See supra* Part III.B.

197. Kerr, *supra* note 195, at 1022.

198. *E.g.*, Potnuru, *supra* note 12, at 94.

199. *Id.* at 94–95. The EPIC notes that out of the users who decide to implement a password to protect their Wi-Fi networks, only fifty-nine percent of such users implement passwords meeting basic criteria for strength and privacy protection. EPIC Brief, *supra* note 15, at 26.

200. EPIC Brief, *supra* note 15, at 26.

201. *Wi-Fi Isn't Radio!?*, *supra* note 168.

should be cognizant of the benefits offline Fourth Amendment principles can bring to the online world. By applying Fourth Amendment principles in a tech-neutral fashion through the content/non-content distinction,[202] the use of such principles to provide online privacy protection becomes much easier.

The Supreme Court in *Katz v. United States* established a reasonable expectation of privacy, determining that privacy protects people and not places.[203] Later, the Court delineated a two-part test in *United States v. Jacobsen* asking whether an individual sought to preserve an area as private, and whether the individual's expectation of privacy is one that society is prepared to recognize as reasonable.[204] The principles established by the Court in *Katz* and *Jacobsen* are equally applicable to the online world, focusing on a user's reasonable expectations of privacy in their electronic communications as opposed to whether certain electronic communication devices may be manipulated (such as through a packet sniffer) to become readily accessible.[205] Recently, the Court held in *United States v. Jones* that the transmission of electronic signals remain subject to the *Katz* reasonable expectation of privacy test.[206] The holding in *Jones* certainly represents a step in the right direction, and hopefully signals the willingness of the Court to protect modern forms of electronic communication.

As this Comment has argued, the general public's reasonable expectations of privacy in Internet communications should parallel our statutory privacy protections. Additionally, one of the primary goals in passing the ECPA was to keep the

---

202. *See* Kerr, *supra* note 195, at 1007–08 ("[T]he contents of online communications ordinarily should receive Fourth Amendment protection but . . . non-content information should not be protected.").

203. Katz v. United States, 389 U.S. 347, 351–54, 361 (1967).

204. United States v. Jacobsen, 466 U.S. 109, 117, 122, 125 (1984).

205. For example, in *Kyllo*, the Court held that the use of thermal imaging devices to detect heat sources emanating from a home constituted a Fourth Amendment search requiring a warrant. Kyllo v. United States, 533 U.S. 27, 39 (2001). As opposed to focusing on the manipulation of a device (the use of thermal imaging to see what normally would not be readily accessible to the general public), the Court utilized the principles established in *Katz* and *Jacobsen* to find a breach of one's reasonable expectation of privacy. *See id.* ("We have said that the Fourth Amendment draws 'A firm line at the entrance to the house' . . . . That line, we think, must be not only firm, but also bright—which requires clear specification of those methods of surveillance that requires a warrant.").

206. United States v. Jones, 132 S. Ct. 945, 954 (2012).

protections of electronic communications in line with the Fourth Amendment.[207] Through the application of offline Fourth Amendment privacy principles, our protection for electronic communications will have the adaptability necessary to combat evolving privacy threats just as offline privacy protections have adapted to the development of post mail, cars, and telephones throughout history.[208]

CONCLUSION

There is no doubt that our society's technological and communications landscape has changed dramatically since the enactment of the ECPA in 1986. Cell phones have replaced landlines, e-mails have superseded snail mail, and pagers are now ancient technology. While one would be hard pressed to argue that technological advancements have made communication more difficult, the notion that new technologies create new privacy problems cannot be overstated.

The court's holding in *Joffe* with respect to Wi-Fi transmissions sent over an unencrypted wireless network is a step in the right direction. However, in order to bring statutory privacy protections in line with current communication technologies, much work remains to be done. Requiring manufacturers and developers to create devices with secure default settings, adapting offline Fourth Amendment privacy principles to the modern online world, and a content/non-content distinction would go a long way towards a needed modernization of the Wiretap Act.

---

207. H.R. REP. No. 99–647, at 16–19, 31 (1986). A paramount concern of the ECPA was to provide individual privacy protection using Fourth Amendment privacy protections as a touchstone. Brief of Plaintiffs-Appellees, *supra* note 32, at 21.

208. *Cf.* Kerr, *supra* note 195, at 1048 (arguing that this approach would provide much needed flexibility for the protection of modern electronic communications). If an unopened letter's contents received by snail mail is still considered private in the hands of a recipient, why do some consider an e-mail in the hands of a recipient no longer private? *Cf.* Haynes, *supra* note 79, at 625–26 (explaining that employer policy and email service agreements may severely limit privacy protection).

***