From Ship-to-Shore Telegraphs to Wi-Fi Packets: Using Section 705(a) to Protect Wireless Communications

Amy McCann Roller *

TABLE OF CONTENTS

* J.D., The George Washington University Law School, May 2016. Senior Articles Editor, Federal Communications Law Journal, 2015-16. The Author would like to thank Anna Myers and Anthony Glosson for their invaluable patience with and feedback on this Note. She would also like to thank Winston C. Roller for his support throughout the writing process.

In early 2010, Google admitted that its Google Maps Street View cars had been capturing more than just street-level images of American communities.[1] For the past few years, the cars had also been collecting the contents of individuals' Internet activity from every Wi-Fi network they encountered.[2] The collected data included e-mails, text messages, Internet browsing history, and "other highly sensitive personal information."[3] The program had come about when a reportedly rogue Google engineer saw commercial opportunity in intercepting this data as it travelled through the most vulnerable link in the Internet relay: consumer Wi-Fi networks.[4]

This may sound like a modern problem—unique to our interconnected world—but the idea is not a new one. A hundred years ago, tabloid journalists had a similar idea, intercepting private telegrams as they travelled ship to shore via radio wave.[5] At the urging of the telegraph industry, Congress responded to these interceptions by enacting the first federal law to protect American wireless communications, prohibiting the unauthorized interception and disclosure of Americans' radio communications.[6]

The 1912 law remains on the books today as Section 705(a) of the Communications Act of 1934.[7] Despite the striking similarities between early interceptions and those undertaken by Google, the Federal Communications Commission (FCC) struggled with Section 705(a)'s applicability to Wi-Fi sniffing.[8] Over the years, federal courts have similarly struggled with Section 705(a)'s construction, repeatedly decrying its notorious opacity.[9] Wi-Fi sniffing, however, is exactly the type of invasion of privacy that Section 705(a) and its predecessor statutes were designed to prohibit.

This Note argues that despite recent uncertainty among courts and regulators, Section 705(a) of the Communications Act does protect unencrypted Wi-Fi traffic from unauthorized interception and divulgence. Section II of this Note looks at the development of American radio communications and their federal statutory protection. Section III of this Note

---

1. *See* Google, Inc., *Notice of Apparent Liability for Forfeiture*, DA 12-592, para. 1 (2012), https://epic.org/privacy/google/FCC%20Google%20SV%20Enforcement%20UNREDACTED.pdf [hereinafter *Unredacted Google Notice*]. This Note cites to an unredacted version of the Notice released by Google. *See, e.g.*, Peter Ha, *Google Releases Full Report on Street View Investigation, Finds that Staff Knew About Wi-Fi Sniffing*, TECHCRUNCH (Apr. 28, 2012), https://techcrunch.com/2012/04/28/543181/. The official, heavily redacted version of the document can be found in the FCC Record. *See* Google, Inc, *Notice of Apparent Liability for Forfeiture*, 27 FCC Rcd 4012 (2012), https://apps.fcc.gov/edocs_public/attachmatch/DA-12-592A1_Rcd.pdf.

2. *See Unredacted Google Notice*, *supra* note 1, at para. 1.

3. *See id.*

4. *See id.* at para 21-26, 30-31, 33-39.

5. *See Radio Communication: Hearing on S. 3620 and S. 5334 Before the S. Comm. on Commerce*, 62d Cong. 80-82 (1912) [hereinafter *1912 Hearings*].

6. *See* Farina v. Nokia Inc., 625 F.3d 97, 105 (3d Cir. 2010); *see also* Radio Act of 1912, Pub. L. No. 62-264, Regulation 19, 37 Stat. 302, 307.

7. Communications Act of 1934 § 705(a), 47 U.S.C. § 605(a) (2012).

8. *See Unredacted Google Notice*, *supra* note 1, at para. 53.

9. *See, e.g.*, Reston v. FCC, 492 F. Supp. 697, 706 (D.D.C. 1980).

looks at the conflicting interpretations of the scope of Section 705(a)'s prohibitions and how that inconsistency muddied the FCC's attempts to enforce the provision against Google when it investigated the company for Wi-Fi sniffing. Section IV lays out a novel proposal for interpreting Section 705(a) to protect unencrypted Wi-Fi and addresses some counterarguments to the proposal.

I. RADIO COMMUNICATIONS AND THEIR STATUTORY PROTECTIONS

Wireless communications, transmitted by radio wave, have been a part of American life for over a century and have been protected from unauthorized interception and disclosure for nearly as long.[10] Wireless transmission eases geographic barriers to communication by eliminating the extensive infrastructure and maintenance outlays required to lay and maintain a wired network. Unfortunately, for all their convenience, radio communications are especially easy to intercept because, unlike communications travelling over a closed wire, they travel multi-directionally through the airwaves.[11] Users and commercial operators can compensate for this special vulnerability by encrypting either the transmission or its content—i.e., the signal or the underlying communication—thereby rendering a message difficult to read, even if successfully intercepted.[12] Although sophisticated signal encryption is common for commercially transmitted wireless communications such as cell phone calls, many other wireless communications, particularly consumer Wi-Fi networks, are not.[13]

A. Radio Communications from Telegraphs to Wi-Fi

Statutorily, the Communications Act defines radio communication as "the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission."[14] In 1912, common radio communications included voiceless radiotelegraph and transmissions by amateur HAM-style radio operators, who numbered around 200,000.[15] By 1924, radio broadcasting was in full swing, with 16,590 amateur stations

10. *See infra* Sections I.A-I.B.

11. *See* Kent R. Middleton, *Radio Privacy Under Section 705(a): An Unconstitutional Oxymoron*, 9 ADMIN. L.J. AM. U. 583, 587 (1995).

12. *See* ORIN S. KERR, COMPUTER CRIME LAW 528 (3d ed. 2013).

13. *See* Bruce Schneier, *Why We Encrypt*, SCHNEIER ON SECURITY (June 23, 2015, 6:02 AM), https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html; *How to Avoid Public WiFi Security Risks*, KASPERSKY LAB, http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi-risks (last visited Sept. 24, 2016).

14. 47 U.S.C. § 153(40) (2012).

15. *See* Middleton, *supra* note 11, at 594.

transmitting programming to the general public.[16] Later, toward the end of the twentieth century, America saw the rise of cordless phones.[17] Today, radio communications' prevalence, and concomitantly their importance, has only increased as new forms of radio communication facilitate Americans' Internet access.[18]

Over the past fifteen years, consumer Wi-Fi has emerged as one of the most popular radio-based technologies in the Internet-access relay.[19] "Wi-Fi" is a proprietary term, registered to the Wi-Fi Alliance, that has been incorporated into the popular lexicon to describe wireless networks connecting consumer electronic devices to the Internet.[20] These consumer Wi-Fi networks operate using a common set of standards, established by the Institute of Electrical and Electronics Engineers, called the 802.11 protocols, which allow for interoperability of wireless devices among disparate brands of consumer electronics.[21] These end-user Wi-Fi networks connect devices such as laptops, tablets, cell phones, and game consoles[22] to a router via radio waves.[23] The router, in turn, couples with a modem that connects to the Internet via a hardwired connection.[24] A network configured in this manner negates the need for users to remain tethered to a wall while accessing the Internet.[25]

While in transmission, the Internet data that Wi-Fi ferries across the airwaves is broken down into packets.[26] Each packet contains both "header" and "payload" data.[27] The header contains addressing information, like those seen on the outside of a letter sent through the postal system, while the payload contains the substance of the communication, like the letter within

16. *See id.* at 598.

17. *See* Nat'l Acad. of Eng'g, *Telephone Timeline*, GREATEST ACHIEVEMENTS, http://www.greatachievements.org/?id=3625 (last visited Sept. 24, 2016).

18. *See* FCC, FEDERAL COMMUNICATIONS COMMISSION FREES UP AIRWAVES TO EASE WI-FI CONGESTION ACROSS THE COUNTRY (2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-326341A2.pdf [hereinafter *Part 15 Revision Fact Sheet*].

19. *See The Future of Wi-Fi*, NCTA, https://www.ncta.com/positions/unlicensed-spectrum (last visited Sept. 24, 2016).

20. *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 30:41 (2007); *see also Our Brands*, WI-FI ALLIANCE, http://www.wi-fi.org/who-we-are/our-brands (last visited Sept. 24, 2016).

21. *See* Mani Potnuru, *Limits of the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing*, 111 MICH. L. REV. 89, 93 (2012). For more technical information on the 802.11 protocols, visit the Institute's website. *See* IEEE 802.11 Wireless Local Area Networks, INST. OF ELEC. & ELEC. ENG'RS, http://www.ieee802.org/11/ (last visited Sept. 24, 2016).

22. For a look at the myriad household devices that are now connected to the Internet via Wi-Fi, see *The Future of Wi-Fi*, *supra* note 19.

23. *See* Revision of Part 15 of the Comm'ns Rules to Permit Unlicensed Nat'l Info. Infrastructure Devices in the 5 GHz Band, *First Report and Order*, 29 FCC Rcd 11599, para. 9 n.10 (2015) [hereinafter *Part 15 Revision Report and Order*].

24. *See id.*

25. *See* Potnuru, *supra* note 21.

26. *See* KERR, *supra* note 12, at 542.

27. *See id.*

the envelope.[28] This Note deals only with the law relating to the interception of payload data.

Wi-Fi, like other forms of radio communication, is particularly susceptible to interception.[29] When setting up his router, a consumer can configure his Wi-Fi network to be either encrypted or unencrypted.[30] The former prevents an interceptor from accessing the packets' content, even after he has intercepted the packets.[31] The latter, however, is the default set up for many consumer Wi-Fi routers.[32]

In the United States, Wi-Fi devices are classified as Unlicensed National Information Infrastructure Devices and governed by Part 15 of the FCC's rules.[33] So-called "Part 15 devices," including Wi-Fi routers, operate in the unlicensed portions of the 2.4 GHz and 5 GHz bands.[34] FCC regulations make this spectrum available for public use, requiring no license to operate devices in these bands.[35] However, the spectrum's unlicensed status does not mean it is unregulated—unlicensed spectrum is still subject to the full panoply of Communications Act provisions and FCC rules.[36] Although the majority of spectrum is licensed,[37] this Note only concerns itself with the law as applied to interceptions on the unlicensed bands. Additionally, there are several other forms of contemporary radio communication, including baby monitors[38] and Bluetooth,[39] that operate on unlicensed bands and can be subject to similar interceptions. For manageability, however, this Note limits its analysis to Wi-Fi communications.

Today, consumer Wi-Fi serves several important purposes. First, it helps to offload congestion from licensed spectrum bands used by mobile

---

28. *See id.*

29. *See* Middleton, *supra* note 11, at 588.

30. *See id.* at 604, 609 (indicating that originators can encrypt their messages, and that originators are capable of sending unencrypted messages).

31. *See id.* at 604 n.95; *see also* KERR, *supra* note 12, at 528.

32. *See* Eric Geier, *Lock Down Your Wi-Fi Network: 8 Tips for Small Businesses*, PCWORLD (Nov. 16, 2011, 6:03 PM), http://www.pcworld.com/article/244012/lock_down_your_wi_fi_network_8_tips_for_small_businesses.html.

33. *See* Kenneth R. Carter et al., *Unlicensed and Unshackled: A Joint OSP-OET White Paper on Unlicensed Devices and Their Regulatory Issues* 22 (FCC OSP Working Paper Series, Paper No. 39, 2003), https://apps.fcc.gov/edocs_public/attachmatch/DOC-234741A1.pdf.

34. *See* Glenn Fleishman, *Understanding Wi-Fi's Two Spectrum Bands*, MACWORLD (May 20, 2009, 7:41 AM), http://www.macworld.com/article/1140685/wifi_spectrumbands.html.

35. *See* Potnuru, *supra* note 21, at 93.

36. *See* Warning: Wi-Fi Blocking is Prohibited, *Enforcement Advisory*, 30 FCC Rcd 387, 388 n.3 (2015).

37. *See Spectrum Dashboard*, FCC, http://reboot.fcc.gov/spectrumdashboard/searchSpectrum.seam (last visited Sept. 24, 2016).

38. *See* Letter from Rep. Joseph Crowley to Julius Genachowski, Chairman, FCC, et al. 1-2, (Nov. 23, 2010), https://ecfsapi.fcc.gov/file/7021448306.pdf.

39. *See* Roman Unucheck, *How I Hacked My Smart Bracelet*, SECURELIST (Mar. 26, 2015, 11:00 AM), http://securelist.com/blog/research/69369/how-i-hacked-my-smart-bracelet/.

phone carriers.[40] In 2013, 57% of mobile data traveled over Wi-Fi rather than the mobile network.[41] By 2018, this is expected to increase to 64%.[42] Second, Wi-Fi serves as an important Internet onramp for consumers;[43] in fact, by 2017, 86% of consumers' in-home broadband traffic will traverse Wi-Fi.[44] Thus Wi-Fi is closely intertwined with both the continued efficiency of mobile networks and the continued expansion of Internet access, which both go to the core of the FCC's responsibilities.

B. Federal Law Has Prohibited Intercepting Radio Communications for over a Century

Today's Section 705(a),[45] a direct descendant of the earliest federal statute to protect the privacy of radio communications,[46] was enacted over a century ago when Congress first sought to impose order on the nation's airwaves. [47] Substantively, Section 705(a) contains of four prohibitory clauses, each banning a different permutation of intercepting and disclosing a communication.[48] Of importance to this Note is the second clause, which provides that "[n]o person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[49] Courts have generally held that this clause prohibits actually

40. *See Part 15 Revision Fact Sheet*, *supra* note 18.

41. *See Part 15 Revision Report and Order*, *supra* note 23 (statement of Comm'r O'Rielly).

42. *Id.*

43. *See* Warning, *supra* note 36.

44. *See The Future of Wi-Fi*, *supra* note 19.

45. Until the 1980s, Section 705(a) was known as Section 605. *See* Susan M. Hart, *Who Gets the Signal? Unauthorized Interception and Section 605 Now Section 705 of the Communications Act*, 6 PACE L. REV. 391, 392 n.8 (1986). The provision was renumbered in 1984, and over the years, other subsections have been added, earning it the designation as subpart (a). *Id.* The new subsections primarily relate to the protection of is wirelessly transmitted subscription television programming. *See* 47 U.S.C. § 605 (2012). Despite being renumbered as Section 705(a) in the Communications Act, the section remains codified at Section 605(a) of Title 47 in the United States Code. *Id.*

46. *See* HBO, Inc. v. Advanced Consumer Tech., Movie Antenna, Inc., 549 F. Supp. 14, 17 (S.D.N.Y. 1981) ("The language of [S]ection [705(a)] is the modern embodiment of a provision that has been a part of communications law for almost seventy years.").

47. *See* Farina v. Nokia Inc., 625 F.3d 97, 105 (3d Cir. 2010).

48. *See* FISHMAN & MCKENNA, *supra* note 20, at § 2:134; *see also* 47 U.S.C. § 605(a) (2012).

49. 47 U.S.C. § 605(a) (2012) ("Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not being authorized by the sender shall intercept any radio

intercepting and divulging the contents of a communication by members of the general public.[50] When crafting Section 705(a), Congress provided a range of enforcement mechanisms—criminal, regulatory, and civil.[51] Accordingly, a violation of Section 705(a) can be pursued by the Department of Justice in a criminal prosecution,[52] by the FCC in an enforcement action,[53] and by private litigants in the federal courts.[54] Further, the FCC has held that it has jurisdiction to resolve private Section 705(a) disputes through the agency's internal adjudicatory process.[55]

Understanding Section 705(a)'s modern meaning requires consideration of its historical development.[56] The first federal statute to protect the privacy of radio communications was Regulation 19 of the Radio Act of 1912.[57] Its language was later redrafted and recodified as Section 27

---

communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.")

50. *See* Steven A. Bookshester & Toni N. Gilbert, *Legal Minefield of Electronic Newsgathering*, 13 COMM. LAW. 11, 12 (1995) (citing Weiss v. United States, 308 U.S. 321 (1939)).

51. *See* sources cited *infra* notes 52-54.

52. *See* 47 U.S.C. § 605(e)(1)-(2). State authorities can also enforce the prohibitions on manufacturing or importing devices for intercepting radio communications in violation of Section 705(a). *See* 47 U.S.C. § 605(e)(6).

53. *See* 47 U.S.C. § 303(f), (m)(1)(A). (2012).

54. *See* 47 U.S.C. § 605(e)(3)-(4).

55. *See* Freemon v. AT&T, *Hearing Designation Order*, 9 FCC Rcd 4032, para. 8 (1994). Although the dispute in that case was between a consumer and a common carrier, the FCC held that it had jurisdiction to entertain section 705(a) disputes, independent of their common carrier authority. *See id* at para. 1 n.2.

56. *See* HBO, Inc. v. Advanced Consumer Tech., Movie Antenna, Inc., 549 F. Supp. 14, 17 (S.D.N.Y. 1981) ("Any attempt to construe [section 705(a)] requires one to examine the statute's origins, the legislative intent behind its enactment, and its regulatory history.").

57. Radio Act of 1912, Pub. L. No. 62-264, Regulation 19, 37 Stat. 302, 307 ("No person or persons engaged in or having knowledge of the operation of any station or stations, shall divulge or publish the contents of any messages transmitted or received by such station, except to the person or persons to whom the same may be directed, or their authorized agent, or to another station employed to forward such message to its destination, unless legally required so to do by the court of competent jurisdiction or other competent authority. Any person guilty of divulging or publishing any message, except as herein provided, shall, on conviction thereof, be punishable by a fine of not more than two hundred and fifty dollars or imprisonment for a period of not exceeding three months, or both fine and imprisonment, in the discretion of the court."); *see also* Reston v. FCC, 492 F. Supp. 697, 703 (D.D.C. 1980) ("Congress'[s] first legislative extension of the requirements of licensing under federal law to amateurs and its

of the Radio Act of 1927,[58] to the same effect.[59] Section 27 was, in turn, incorporated nearly verbatim into the Communications Act provision now known as Section 705(a).[60]

1. The 1968 Wiretap Act Exemptions

In 1968, Section 705(a) was amended for the last time with the passage of the Wiretap Act.[61] The Wiretap Act removed wire communications from Section 705's purview and added an introductory clause cross-referencing the Wiretap Act, excepting any interceptions that were authorized under the 1968 Wiretap Act from Section 705(a)'s prohibitions.[62]

This clause incorporated the Wiretap Act's exceptions, then codified at 18 U.S.C. § 2511(1)-(3), into Section 705(a). First, § 2511(1) included a structural exemption, permitting those interceptions specifically authorized pursuant to the Wiretap Act.[63] Next, § 2511(2) enumerated specific types of

---

initial imposition of a ban on the disclosure of radio transmissions are found in the [Radio Act of 1912].").

58. Radio Act of 1927, Pub. L. No. 69-632, § 27, 44 Stat. 1162, 1172 ("No person receiving or assisting in receiving any radio communication shall divulge or publish the contents, substance, purport, effect, or meaning thereof except through authorized channels of transmission or reception . . . no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purport, effect, or meaning of such intercepted message to any person; and no person not being entitled thereto shall receive or assists in receiving any radio communication and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto; and no person having received such intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: Provided, That this section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication broadcasted or transmitted by amateurs or others for the use of the general public or relating to ships in distress."); *see* Lauritz S. Helland, *Section 705(a) in the Modern World: A Response to Di Geronimo*, 40 FED COMM. L.J. 115, 116, 116 nn.8-9 (1988).

59. *See* S. REP. NO. 772, at 5 (1926) ("The provisions regarding the protection of . . . messages against reception and use by unauthorized persons are largely a redraft of existing law and seem necessary and proper provisions."); *see also Hearings on S. 1 and S. 1754 Before the S. Comm. on Interstate Commerce*, 69th Cong. 70-71 (1926).

60. *See* Sablowsky v. United States, 101 F.2d 183, 190 (3d Cir. 1938) ("The provisions of Section 605 seem to have been lifted almost bodily from Section 17 of the Radio Act of 1927."); *see also* Middleton, *supra* note 11, at 601, 601 n.83 (quoting Glen O. Robinson, *Title I of The Federal Communications Act: An Essay on Origins and Regulatory Purposes*, in A LEGISLATIVE HISTORY OF THE COMMUNICATIONS ACT OF 1934 3 (Max D. Paglin ed., 1989)) ("The most novel feature of the 1934 legislation [was] the merging of the telecommunications common carrier and radio regulation.").

61. *See* Wiretap Act, Pub. L. 90-351, tit. III, § 802, 82 Stat. 212 (1968) (codified at 18 U.S.C. §§ 2510-2520 (2012)) From then on, the Wiretap Act governed the interception of oral and wire communications, while Section 705(a) governed radio communications.

62. *See* 47 U.S.C. § 605(a) (2012).

63. *See* 18 U.S.C. § 2511(1) (1970) ("Except as otherwise specifically provided in this chapter any person who [commits one of the enumerated acts] shall be fined not more than $10,000 or imprisoned not more than five years, or both."). The Wiretap Act had imposed new

interceptions that "shall not be unlawful under this chapter."[64] First, it permitted interceptions by common carriers' employees that are made either in the ordinary course of business,[65] or when assisting an authorized law enforcement investigation.[66] Next, it allowed FCC employees to intercept communications while undertaking the Commission's statutorily-assigned monitoring duties.[67] Furthermore, it allowed persons acting under color of law to intercept communications with one party's consent.[68] Persons not acting under color of law were permitted to intercept their own communications or, with the consent of a party, others' communications, unless done for tortious, criminal, or other injurious purposes.[69] Finally, § 2511(3) created a national security exemption that permitted the president to authorize reasonable interceptions to protect the United States.[70]

---

and novel warrant requirements on law enforcement seeking wiretaps to gather evidence. *See id.* §§ 2515-2518. The language of Section 2511(1) clarified that those court-authorized interceptions were not otherwise unlawful under the Act.

64. *See id.* § 2511(2)(a)-(d).

65. *See id.* § 2511(2)(a)(i) ("It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in tile transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.").

66. *See id.* § 2511(2)(a)(ii) ("It shall not be unlawful under this chapter for an officer, employee, or agent of any communication common carrier to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, pursuant to this chapter, is authorized to intercept a wire or oral communication.").

67. *See id.* § 2511(2)(b) ("It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.")

68. *See id.* § 2511(2)(c) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.").

69. *See id.* § 2511(2)(d) ("It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act.").

70. *See id.* § 2511(3).

2. The 1986 Electronic Communications Privacy Act Exemptions

Later, Congress enacted the 1986 Electronic Communications Privacy Act, which was designed to help the Wiretap Act adapt to new technologies.[71] ECPA is codified alongside the Wiretap Act and is sometimes referred by courts and litigants to as part of the Wiretap Act itself.[72] ECPA contains a host of exemptions, which were codified alongside the Wiretap Act exemptions and authorizations in 18 U.S.C. §§ 2511-2519. Today, both ECPA and Section 705(a) govern the interception of radio communications.[73] The two provisions create duplicative liability and Congress intended for Section 705 to cover some circumstances not covered by ECPA.[74]

II. UNCERTAINTY HAS EMERGED AMONG COURTS AND THE FCC REGARDING SECTION 705(A)'S SCOPE AND APPLICABILITY

The authorities have not reached a consensus as to the appropriate construction of Section 705(a).[75] Discordant constructions have created substantial uncertainty, hindering enforcement and leaving Wi-Fi unprotected.[76] But the persistent uncertainty and ambiguity over Section 705(a)'s scope imperil important interests. Statutory protections for communications privacy are important to American society. Laws protecting private communications ultimately increase public trust in the means of those communications,[77] which in turn serves two important goals: the encouragement of private speech and the adoption of new communications technologies.[78] Despite these important values, Congress has been unwilling

71. *See* Bartnicki v. Vopper, 532 U.S. 514, 524 (2001) ("As enacted in 1968, Title III did not apply to the monitoring of radio transmissions. In the Electronic Communications Privacy Act of 1986, 100 Stat. 1848, however, Congress enlarged the coverage of Title III to prohibit the interception of 'electronic' as well as oral and wire communications.").

72. *See* Joffee v. Google, Inc., 746 F.3d 920, 930 (9th Cir. 2012) (referring to ECPA provisions as Wiretap Act provisions). *But see* Konop v. Hawaiian Airlines Inc., 302 F.3d 868, 874-79 (9th Cir. 2002) (referring to ECPA provisions as ECPA provisions); *In re* Pharmatrak, Inc., 329 F.3d 9 *passim* (1st Cir. 2003) (referring to ECPA provisions as ECPA provisions).

73. *See* S. REP. NO. 99-541 (1986), *as reprinted* in 1986 U.S.C.C.A.N. 3555.

74. *See id.*

75. *See, e.g.*, Reston v. FCC, 492 F. Supp. 697, 706 (D.D.C. 1980); *Unredacted Google Notice*, *supra* note 1, at para. 53.

76. *See Unredacted Google Notice*, *supra* note 1, at para. 53.

77. In fact, there has been some concern that they may increase public confidence too much. *See* Letter from John R. Bolton, Asst. Att'y Gen. of the U.S. for Legis. & Governmental Affairs, to Rep. Robert Kastenmeier, Chairman, Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. on the Judiciary (Apr. 15, 1986), *reprinted in Electronic Communications Privacy Act of 1985: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the House Comm. on the Judiciary*, 99th Cong. 290 n.1 (1986) (expressing the FCC's concern that the ECPA might "create unmerited expectations of privacy among the general public" because of the state of technology at that time).

78. *See id.* at 155.

or unable in recent years to craft new legislation, and so existing law must be repurposed, to the extent possible, to cover new forms of communication.

A. Currently, there is Substantial Uncertainty over What Protections the Law Affords to Unencrypted Wi-Fi Communications.

Wi-Fi's prevalence, paired with the current uncertainty over its legal protections, has left Americans' Internet activity vulnerable to eavesdropping.[79] The recent controversy over Google's data collection activities is a prime example of this vulnerability.[80] In a blog post on May 14, 2010, Google admitted that its "Street View" cars, which capture street-level images for its Google Maps program, had also been collecting Wi-Fi payload data from unencrypted wireless networks.[81] The resulting scandal came to be known as "Wi-Spy" in the press.[82]

Many Internet users were angered by the revelation, leading to class action lawsuits around the country.[83] While private litigation is still ongoing, investigations launched by the Federal Trade Commission, the Department of Justice, and the FCC have since concluded[84] without taking enforcement actions.[85]

On April 13, 2012, the FCC concluded its Google investigation and adopted its Notice of Apparent Liability for Forfeiture.[86] The FCC's investigation determined that a Google employee intentionally programmed equipment on board the Google Maps cars to collect payload data from all Wi-Fi networks they encountered and to store the unencrypted Wi-Fi payload data. The employee had then shown the data to at least two other Google employees.[87] The Notice officially fined Google $25,000 for obstructing the

79. *See Unredacted Google Notice*, *supra* note 1, at para. 53.

80. *See id.*

81. *Unredacted Google Notice*, *supra* note 1, at para. 9.

82. *See, e.g.*, Kashmir Hill, *"Wi-Spy" Continues to Haunt Google: Federal Court Says It May Have Violated Wiretap Act*, FORBES (Sept. 10, 2013, 3:41 PM), http://www.forbes.com/sites/kashmirhill/2013/09/10/wi-spy-continues-to-haunt-google-federal-court-says-it-may-have-violated-wiretap-act/.

83. *See In re* Google Inc. St. View Elec. Comm. Litig., 733 F. Supp. 2d 1381, 1382-83 (J.P.M.L. 2010) (consolidating various Google class actions from federal courts across the country).

84. *See* Letter from E. Ashton Johnston, Counsel, Google Inc. to P. Michele Ellison, Chief, FCC EB (Apr. 26, 2012), https://epic.org/privacy/streetview/documents/google-response-to-fcc.pdf.

85. *See Unredacted Google Notice*, *supra* note 1, at para. 15; *see also* Letter from Paul J. Fishman, U.S. Att'y, to Albert Gidari & Michael A. Sussman (May 27, 2011), http://epic.org/privacy/streetview/DOJ-Google-Street-View-Investigation-Letter-05272011.pdf; Letter from David C. Vladeck, Dir., FTC Bureau of Consumer Prot., to Albert Gidari (Oct. 27, 2010), https://www.ftc.gov/sites/default/files/documents/closing_letters/google-inquiry/101027googleletter.pdf.

86. *See Unredacted Google Notice*, *supra* note 1.

87. *See id.* at paras. 21-26, 30.

FCC's investigation and submitting non-compliant document certifications.[88] Despite the fine, the FCC declined to take any enforcement action for the underlying conduct.[89] When declining to take action under Section 705(a), the agency cited a lack of FCC precedent regarding the Section's applicability to Wi-Fi communications, legal uncertainty over the scope of the Section's prohibitions and its interaction with the Wiretap Act and ECPA, and a lack of evidence regarding whether the corporation itself made use of the information.[90]

The legal uncertainty over the scope of Section 705(a) and its interaction with the Wiretap Act and ECPA arose from Google's argument that "the Wiretap Act permits the interception of unencrypted Wi-Fi communications, and [that] some case law suggests that Section 705(a)'s prohibition on the interception or unauthorized reception of interstate radio communications excludes conduct permitted (if not expressly authorized) under the Wiretap Act." [91] In addition to the disagreement over the applicability of these exceptions, the meaning of the underlying exception is hotly disputed. Lawsuits arising from the Google interceptions were premised on the civil remedies available for violations of § 2511.[92] Examining the same "readily accessible" exception that the FCC found to be a bar to its enforcement authority, the Northern District of California found that the § 2510(16) definition of readily accessible was inapplicable, and that under its own analysis, the communications were not readily accessible to the public.[93] This view was later affirmed by the Ninth Circuit.[94] This has left the current status of the legal protection afforded to American's Wi-Fi communications unclear, despite the fact that such protections serve important economic and social objectives.

III. CORRECTLY INTERPRETED, SECTION 705(A) PROTECTS AMERICANS' UNENCRYPTED WI-FI COMMUNICATIONS

It is well established that where Section 705(a)'s prohibitions attach, it is unlawful to intercept and divulge a radio communication without authorization.[95] Although Section 705(a) has never been applied to it, Wi-Fi falls squarely within the statutory definition of "radio communications"

88. *See id.* at para. 1
89. *See id.* at paras. 53-54.
90. *See id.* at para. 53.
91. *Id.*
92. *See In re* Google Inc. Street View Elec. Communs. Litig. (*In re Street View Litig.*), 794 F. Supp. 2d 1067, 1070 (N.D. Cal. 2011)
93. *See id.* at 1082. *But see In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 893-94 (N.D. Ill. 2012) (holding that although Section 2510(16) definition was inapplicable to Wi-Fi sniffing, the communications were still "readily accessible to the general public").
94. *See* Joffe v. Google, Inc. (*Joffe I*), 729 F.3d 1262, 1264 (9th Cir. 2013), *amended on reh'g*, Joffe v. Google, Inc. (*Joffe II*), 746 F.3d 920 (9th Cir. 2013).
95. *See* 47 U.S.C. § 605(a) (2012).

subject to Section 705(a)'s protections because it transmits "writing, signs, signals, pictures, and sounds" by radio.[96] Thus, the argument that the prohibitions do not apply to Wi-Fi sniffing hinges on incorporating § 2511's "readily accessible to the general public" exception into Section 705(a).[97] To reconcile this interpretive quagmire, courts and the FCC should interpret Section 705(a) using the well-established canons of statutory construction and construe the provision in light of its statutory purpose.

A. Section 705(a) Does Not Incorporate the Readily Accessible to the General Public Exception, According to Well-Established Canons of Statutory Construction, Congressional Intent, and Early Interpretations of the Section's Meaning.

The "readily accessible" exception of § 2511 is not applicable to Section 705(a)'s prohibition on intercepting and divulging radio communications because Section 705(a) was amended to include the "except as authorized by . . . " language by the Wiretap Act of 1968.[98] At that time, the Wiretap Act did not contain the "readily accessible" exceptions;[99] they were added by the Electronic Communications Privacy Act of 1986, which was codified alongside the Wiretap Act.[100] Thus, without more indicia of congressional intent to do so, the exception should not be read into the earlier statute.

1. The Reference Statute Canon Does Not Allow for the "Readily Accessible" Exception to be Read into Section 705(a).

It is inappropriate to read the "readily accessible" exception into Section 705(a) in light of the well-established reference statute canon.[101] Because Section 705(a) refers to a specific statutory provision, it is a "specific reference" statute, which incorporates only those authorizations that existed at the time the "reference" was enacted.[102]

---

96. *See* 47 U.S.C. § 153(40) (2012); *see also supra* Section I.A (discussing technical characteristics of Wi-Fi).

97. *See Unredacted Google Notice*, *supra* note 1, at para. 53; *see also* United States v. Gass, 936 F. Supp. 810 (N.D. Okla. 1996).

98. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, § 803, 82 Stat. 197, 223.

99. *See* 47 U.S.C. § 2511 (1970); *see also supra* Section I.B.1.

100. *See* Electronic Communications Privacy Act of 1986, Pub. L. 99-508, § 101(b), 100 Stat. 1848, 1849-51 (1986); *see also supra* Section I.B.2.

101. The Supreme Court first used the reference statute canon in 1838, when construing a statute regarding jurisdiction of the Circuit Court for the District of Columbia. *See* Kendall v. United States *ex rel.* Stokes, 37 U.S. (12 Pet.) 524, 555 (1838).

102. *See* 2B NORMAN SINGER & SHAMBIE SINGER, SUTHERLAND STATUTORY CONSTRUCTION § 51:8 (7th ed.).

A reference statute is one that incorporates another law or body of law by reference.[103] There are two types of reference statutes: specific reference statutes, which refer "to a particular statute by its title or section number," and general reference statutes, which refer to an area or body of law," for example "in accord with the law of property."[104] By virtue of the clause conditioning its protections on the authorizations of Chapter 119 of Title 18,[105] Section 705(a) is a reference statute. Because it refers to a particular statutory provision, Chapter 119 of Title 18, Section 705(a) is a specific reference statute.

The distinction is important because the applicability of subsequent amendments depends upon whether Section 705(a) is a general or specific reference statute. Specific reference statutes incorporate the referee statute as it existed at the time of adoption and neither subsequent amendment nor repeal should not be read into the reference statute.[106] While it is true that there is an exception to the general principle that subsequent amendments to the reference statute should not be read into a specific reference statute when the legislature has evinced an intent that such amendments should be,[107] this is not the case here. In fact, in the case of the 1986 ECPA amendments, the opposite is true.[108]

2. Congress Did Not Intend for the "Readily Accessible" Exception to Be Carved Out of Section 705(a).

When Congress enacted ECPA, it repeatedly expressed its intent that the Act's provisions were not meant to detract from those of Section 705(a).[109] Interpreting it to the contrary, such that ECPA's exceptions would undercut Section 705(a)'s protections, violates the well-established maxim that "a construction adopted should not be such as to nullify, destroy, or defeat the intention of the legislature."[110] All other rules of statutory construction are designed to achieve that end and should not be applied so as to achieve a contrary result.[111]

---

103. *Id.* § 51:7.
104. *Id.*
105. 47 U.S.C. § 605(a) (2012).
106. *See* SINGER & SINGER, *supra* note 102, § 51:8.
107. *See id.* § 51:8 n.2.
108. *See infra* introduction.
109. *See* S. REP. NO. 99-541, *supra* note 73, at 14.
110. BARBARA J. VAN ARSDALE ET AL., 73 AM. JUR. 2D STATUTES § 59 (2016 update).
111. *See id.* § 60 (footnotes omitted) ("[T]he cardinal rule of statutory construction is to effectuate legislative intent with all rules of construction being aides to that end. The fundamental question in all cases of statutory interpretation is legislative intent, and the rules of statutory construction are designed to ascertain and enforce the intent of the legislature. The rules of grammar and canons of construction are but tools, guides to help courts determine likely legislative intent.").

ECPA's legislative history illustrates that Congress did not intend its exceptions be read into Section 705(a). The Senate Report accompanying ECPA's passage states that "[a]lthough radio communications are within the scope of the Act, the provisions of the [ECPA] directed specifically to radio do not affect the applicability of Section 705 of the Communications Act of 1934, as amended, to actions by members of the public."[112] When introducing the Act, ECPA sponsor Senator Charles Mathias took the Senate floor and remarked that some "interceptions are already covered by [S]ection 705 of the Communications Act. The provisions in this legislation are in addition to any remedies that may be available to the Government or to a private party under the Communications Act."[113] Later, in response to an inquiry by Senator John Danforth, Senator Mathias plainly stated that "conduct which is not prohibited by the [ECPA], but which is prohibited by the Communications Act, still will be subjected to the full range of remedies and penalties under the Communications Act."[114] These statements show that Congress neither intended nor expected ECPA's exceptions to be read into Section 705(a).

Furthermore, the Senate's regulatory impact statement notes that "after due consideration, the Committee [on the Judiciary] concluded that the changes in existing law contained in the bill will not increase or diminish any present regulatory responsibilities of the U.S. Department of Justice or any other department or agency affected by the legislation."[115] If Congress intended to gut Section 705(a), it would have considered that such a change would lessen the FCC's regulatory burden.

In addition, at the time it enacted Section 705(a)'s introductory clause, Congress did not intend for "readily accessible" communications to be excepted from its operation. To construe the passage in a manner that the drafters did not intend would violate the "primary," "fundamental," or "cardinal" rule of statutory construction, which is to determine and give effect to the intention of the legislature.[116] The argument that the "radio communications exception" renders Section 705(a) inapplicable to Wi-Fi rests on the introductory phrase, "[e]xcept as authorized by chapter 119, Title

112. S. REP. NO. 99-541, *supra* note 73, at 14.

113. 132 CONG. REC. 26,765 (1986) (floor speech of Sen. Mathias proposing ECPA amendments to the Wiretap Act).

114. 132 CONG. REC. 26,768 (1986) (floor debate) (response of Sen. Mathias). The full exchange went as follows:

"Mr. DANFORTH. This legislation covers some conduct that also is prohibited under section 705 of the Communications Act of 1934. Do I understand correctly that the sanctions contained in this legislation would be imposed in addition to, and not instead of, those contained in section 705 of the Communications Act?

Mr. MATHIAS. That is correct. This legislation is not intended to substitute for any liabilities for conduct that also is covered by section 705 of the Communications Act. Similarly, it is not intended to authorize any conduct which otherwise would be prohibited by section 705. The penalties provided for in the [ECPA] are in addition to those which are provided by section 705 of the Communications Act."

115. S. REP. NO. 99-541, *supra* note 73, at 52.

116. 73 AM. JUR. 2D STATUTES, *supra* note 110, § 59 ("In the interpretation of statutes, the legislative will is the all-important or controlling factor.").

18," which qualifies its prohibitions.[117] However, the exception should be interpreted as Congress understood it at the time of enactment.[118] In 1968, when Congress amended Section 705(a) to include this language, chapter 119 of Title 18 contained neither the readily accessible exception nor the subsidiary "unencrypted radio communication" exception.[119] The exception is a provision of the Electronic Privacy Communications Act of 1986.[120] Thus, Congress did not mean to exempt communications that are readily accessible to the general public from Section 705(a)'s protections.

3. Early Interpretations of Section 705(a) Support This Interpretation.

In the immediate aftermath of the ECPA's passage, it appears that courts and commentators did not consider its exceptions applicable to Section 705(a). Until the mid-1990s, a decade after ECPA's enactment, courts and commentators appear to have taken for granted that the ECPA exceptions were not incorporated into Section 705(a). For example, in the 1994 case *Snider Communication Corp. v. Cue Paging Corp.*,[121] there was a dispute over pages transmitted over the FM band.[122] The court analyzed Section 705(a)'s provisions, including the introductory clause, but never so much as mentioned that the "readily accessible" ECPA exception,[123] which would apply when transmitting on an FM band.[124] In fact, there was an entire law review article premised on the unconstitutionality of Section 705(a), as applied to the press, because it lacked an exception for police scanners, although ECPA contains just such an exception.[125] These interpretations from immediately after the act's passage are particularly important and given special consideration when constructing a statute.[126]

One could argue that despite Congress's intent, the text of Section 705(a) seems to incorporate the ECPA exceptions by referencing all of Chapter 119 of Title 18, which is in fact where the ECPA is codified.[127] Several considerations counsel against this approach. At the time the incorporation clause was written, the section did not contain the "readily

117. 47 U.S.C. § 605(a) (2012).

118. Perrin v. United States, 444 U.S. 37, 42 (1979) ("A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning . . . at the time Congress enacted the statute.").

119. *See* Wiretap Act, Pub. L. 90-351, § 802, 82 Stat. 212, 214 (1968).

120. *See* Electronic Communications Privacy Act of 1986, Pub. L. 99–508, § 101(b)(4), 100 Stat. 1848, 1850.

121. *See* Snider Comm. Corp. v. Cue Paging Corp., 840 F. Supp. 664 (E.D. Ark. 1994).

122. *See id.* at 665-67.

123. *See id.* at 667-70.

124. *See* Middleton, *supra* note 11, at 602-03, 690-91 nn.90-91.

125. *See id.* at 596, 596 n.51; Electronic Communications Privacy Act of 1986 § 101(b)(4).

126. SINGER & SINGER, *supra* note 102, § 49:7, 49:7 n.2.

127. *See* 47 U.S.C. § 605(a) (2012).

accessible to the public" provisions.[128] In addition, the text of the ECPA itself provides that nothing in Chapter 119 nor Section 705 of the Communications Act should be construed to effect the operation of interception activities authorized by the Foreign Intelligence Surveillance Act of 1978.[129] That reference to Section 705(a) would be meaningless, if its prohibitions were already circumscribed by the ECPA.

It may initially seem less than ideal to apply a law essentially drafted in 1912 to today's communications systems, but Section 705 was crafted with the flexibility to cover new forms of radio communication. First, the text of the act only refers to "radio communication," not specific technological means.[130] If Congress had intended to limit the Act to the particular technologies it had in mind at the time of enactment (i.e., telegraphs),[131] it could have. Moreover, although Wi-Fi necessarily does not come up in the legislative history of any of the acts at issue here, the Supreme Court "has never required that every permissible application of a statute be expressly referred to in its legislative history."[132]

There is, however, legislative history endorsing the idea that Section 705 is flexible in its applicability to new forms of radio communication. In 1984, when amending Section 705 to add subsection (b), Congress was careful to note that Section 705 "not only prohibits unauthorized interception of traditional radio communications, but also communications transmitted by means of new technologies."[133] Further, this admonition is especially poignant in context because, when enacting Section 705(b), Congress intended to abrogate a line of cases that had limited Section 705's application to new technology and "to preserve this broad reach of existing [Section 705] and to make clear that all communications covered under [Section 705] will continue to be protected."[134] This history confirms that in the face of courts' efforts to limit its reach to new technology, albeit of a different variety than those at issue here, Congress undertook to clarify that Section 705 should be interpreted to reach emerging technologies and that its protections should be broadly construed.

B. Seemingly Contrary Case Law Is Not Dispositive on the Issue of Incorporating the ECPA Exceptions into Section 705(a).

When resolving its investigation into Google, the FCC decided not to take enforcement action because "some case law suggests that Section 705(a)'s prohibition on the interception or unauthorized reception of

128. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, § 802, 82 Stat. 197, 214.

129. Electronic Communications Privacy Act of 1986 § 107.

130. *See* 47 U.S.C. § 605(a).

131. *See 1912 Hearings*, *supra* note 5, at 6.

132. Moskal v. United States, 498 U.S. 103, 104 (1990).

133. Int'l Cablevision, Inc. v. Sykes, 75 F.3d 123, 133 (2d Cir. 1996) (citing 130 CONG. REC. S14,285 (daily ed. Oct. 11, 1984) (statement of Sen. Packwood)).

134. *See* Cal. Satellite Sys., Inc. v. Nichols, 216 Cal. Rptr. 180, 186 (Cal. Ct. App. 1985).

interstate radio communications excludes conduct permitted (if not expressly authorized) under the Wiretap Act."[135] To support that proposition, the FCC cited *United States v. Rose*,[136] *Edwards v. State Farm Ins. Co.*,[137] and *United States v. Gass*.[138] The first two cases have no bearing on the question of the applicability of ECPA exceptions to Section 705(a) and the third is of limited precedential value.

In both *Rose* and *Edwards*, the courts did nothing more than apply exceptions from the 1968 Wiretap Act to Section 705(a). In *Rose*, the First Circuit incorporated the Wiretap Act's "reasonable expectation of privacy" exception.[139] The Fifth Circuit in *Edwards* based its reasoning on *Rose* and applied the Wiretap Act's statutory exception for "oral communications."[140] Because these cases apply only exceptions from the 1968 Act, they are consistent with the reference statute canon.

In *Gass*, the court applied the "readily accessible" exception to Section 705(a)[141] The government argued that, despite its introductory language, the Wiretap Act does not alter Section 705(a)'s prohibition on intercepting and divulging radio communications. [142] To support their argument, the government pointed to a lone journal article from 1985.[143] Accordingly, the issue of ECPA's applicability, as distinguished from that of the Wiretap Act, was not actually argued. Furthermore, the issue the court did actually consider—that the Wiretap Act exceptions apply to Section 705(a)—is consistent with the reference statute canon.

C. In the Face of Persistent Uncertainty Regarding the Scope of ECPA's Protections, Interpreting and Applying Section 705(a) to Protect Unencrypted Wi-Fi Would Serve Important Economic and Social Objectives.

The current uncertainty surrounding the protection for unencrypted Wi-Fi payload data implicates compelling economic and social policy objectives. First, studies show that privacy protections are important to consumer confidence in and concomitant with adoption of new communications technology. Second, when individuals' communications lack privacy protections, there is a chilling effect on private speech—correspondingly privacy laws can foster private speech, thereby effectuating First Amendment values. By properly construing and applying Section 705(a) to protect these private communications, courts and regulators can further these objectives.

---

135. *Unredacted Google Notice*, *supra* note 1, at para. 53.
136. United States v. Rose, 669 F.2d 23 (1st Cir. 1982).
137. Edwards v. State Farm Ins. Co., 833 F.2d 535 (5th Cir. 1987)
138. United States v. Gass, 936 F. Supp. 810 (N.D. Okla. 1996).
139. *See Rose*, 669 F.2d at 26-27.
140. *See Edwards*, 833 F.2d at 539-40.
141. *See Gass*, 936 F. Supp. at 816.
142. *See id.* at 815.
143. *See id.* at 811.

1. Protecting Private Communications Spurs Economic Growth by Fostering Public Trust in New Technologies Which in Turn Encourages Adoption.

Section 705(a), which was originally proposed by a telegraph company executive,[144] was enacted to help communications industries grow by protecting the integrity of their messages.[145] At that time, telegraph communications were unencrypted and were increasingly being intercepted by amateur radio operators and the press, who would then report on their contents.[146] These interceptions and disclosures shook consumer confidence in sending messages by telegraph, casting doubt on the technology's reliability and prudence.[147] As a result, Americans opted to continue sending important messages by first class mail, which enjoys absolute privacy protections, despite the substantial efficiencies of telegraph communication.[148] The heavy fines imposed by the new law discouraged the press's behavior and helped the telegraph industry gain consumer confidence and grow.[149]

This consumer trepidation is not a phenomenon unique to centuries past. A recent survey of Americans' response to government surveillance revelations shows a trend towards forgoing technological benefits because of privacy concerns.[150] For example, over a third of Americans who are aware of the surveillance programs taken at least one step to avoid the perceived risk of eavesdropping.[151] Some of these behavioral changes have a clear economic effect. For example, privacy concerns have lead 15% of Americans to use certain online platforms less often, 15% to avoid certain software, and 13% reported that they uninstalled software.[152] Most strikingly, in a close analogy to the telegraph example, 14% reported speaking more in person rather than online or by phone,[153] forgoing the efficiencies of online communication in favor of the assurance of privacy.

The economic import of these consumer concerns is especially compelling in the Wi-Fi context, because recent estimates put the value of the

144. *See 1912 Hearings*, *supra* note 5, at 80-82.

145. *See* United States v. Russo, 250 F. Supp. 55, 58 (E.D. Pa. 1966) ("The purpose of [S]ection 605 is to prohibit blatant public or private encroachments on the privacy of messages and the integrity of communication systems. The only way to secure this integrity is to insure that, as much as possible, only the person entitled to receive a communication learns of its contents.") (citing Nardone v. United States, 302 U.S. 379, 383 (1937)).

146. *See* Middleton, *supra* note 11, at 596, 596 nn.50-51.

147. *See 1912 Hearings*, *supra* note 5, at 81-82.

148. *See* Middleton, *supra* note 11, at 592-93, 598.

149. *See id.*

150. *See* MARTIN SHELTON ET AL., PEW RESEARCH CENTER, AMERICANS' PRIVACY STRATEGIES POST-SNOWDEN (2015), http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

151. *See id.* at 3. The survey showed that nearly ninety percent of Americans are aware of the programs. *See id.*

152. *See id.*

153. *See id.*

Wi-Fi and other open wireless technology industries at $50-100 billion annually.[154] At the same time, Internet content providers consider Wi-Fi's expansion essential to the industry's continued growth and have been pushing hard to open up more airwaves to Wi-Fi.[155]

A lack of consumer trust in Wi-Fi networks, through which we frequently send our most sensitive communications, will stifle their growth in this economically important sector. As the FCC recently acknowledged in another context, "consumers concerned about the privacy of their personal information will be more reluctant to use the Internet, stifling Internet service competition and growth," and enforcing Communications Act privacy protections "will help spur consumer demand for . . . Internet access."[156] Thus, Section 705(a) can serve important economic objectives by encouraging consumer confidence in Wi-Fi networks.

2. Protecting Private Communications Effectuates First Amendment Values by Encouraging Private Speech.

At the same time that protecting Wi-Fi serves commercial and economic interests, it also serves consumers and social interests as well. The Supreme Court has explained that laws, like Section 705(a),[157] that prohibit the disclosure of illicitly intercepted communications "encourag[e] the uninhibited exchange of ideas and information among private parties,"[158] even "encourag[ing] conversations that otherwise might not take place."[159] Conversely, in the absence of such laws, "the fear of public disclosure of private conversations might well have a chilling effect on private speech."[160] This chilling effect is not a mere abstraction—it can be empirically observed. A recent Pew study found that in response to news of government surveillance, 13% of Americans have avoided using certain words in online communications.[161] The study demonstrates that concern over prying eyes and ears leads Americans to self-censor in their private communications.[162]

---

154. *See About Us*, WE HEART WI-FI, http://weheartwifi.com/about/ (last visited Sep. 24 2016).

155. *See, e.g.*, Kate Tummarello, *Tech Industry Pushing FCC for More Wi-Fi Airwaves in 2015 Spectrum Auction*, HILL (Mar. 21, 2014 6:08 AM EDT), http://thehill.com/policy/technology/203916-tech-industry-pushing-fcc-for-more-open-airwaves.

156. *See* Protecting and Promoting the Open Internet, *Report and Order*, 30 FCC Rcd 5601, para. 54 (2015) (footnotes omitted).

157. Section 705(a) prohibits not the mere act of unauthorized interception, but only when the contents of the unauthorized interception are also disclosed. *See* 47 U.S.C. § 605(a) (2012).

158. Bartnicki v. Vopper, 532 U.S. 514, 532 (2001).

159. *Id.* at 537 (Breyer, J., concurring) (citing Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 559 (1985) (describing "freedom not to speak publicly")).

160. *Id.* at 533.

161. *See* SHELTON ET AL., *supra* note 150, at 3.

162. *See id.*

The value of uninhibited private speech does not just accrue to the unencumbered speakers individually; rather, as the Supreme Court has noted, the privacy of communications is essential to a democratic society.[163] Laws that shield private communications, like Section 705(a), serve an important societal purpose by effectuating First Amendment values.[164] As New York's high court famously explained:

> The essential thrust of the First Amendment is to prohibit improper restraints on the voluntary public expression of ideas; it shields the man who wants to speak or publish when others wish him to be quiet. There is necessarily, and within suitably defined areas, a concomitant freedom not to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect.[165]

This "freedom not to speak publicly, to speak only privately, is violated whenever an illegally intercepted conversation is revealed."[166] Like other communications privacy protections, enforcement of Section 705(a) would contribute to the vibrant national conversation protected by the First Amendment. Through enforcement of Section 705(a), benefits would accrue to individuals and society by protecting private speech and in turn encouraging it.

IV. CONCLUSION

Despite persistent interpretive confusion in recent history, courts and regulators should interpret Section 705(a) of the Communications Act to include unencrypted radio communications within the scope of the communications that the act protects from interception and divulgence. So construed, Section 705(a) prohibits intercepting unencrypted Wi-Fi communications. This prohibition would further important economic and social policies by encouraging technology adoption and fostering private speech.

163. *Bartnicki*, 532 U.S. at 533.

164. *See id.* at 533-34.

165. Hemingway's Estate v. Random House, Inc., 244 N.E.2d 250, 255 (1968) (quoted with approval in *Bartnicki*, 532 U.S. at 537 n.20; Pacific Gas & Elec. Co. v. Pub Utils. Comm'n of Cal., 475 U.S. 1, 11 (1986); *Harper & Row*, 471 U.S. at 559).

166. Boehner v. McDermott, 191 F.3d 463, 469 (D.C. Cir. 1999), *vacated*, 532 U.S. 1050 (2001) (remanding for reconsideration in light of Court's decision in *Bartnicki*).