

No. 13-

---

---

IN THE  
**Supreme Court of the United States**

---

GOOGLE INC.,  
*Petitioner,*

*v.*

JOFFE, *et al.*,  
*Respondents.*

---

ON PETITION FOR A WRIT OF CERTIORARI TO THE  
UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

**PETITION FOR A WRIT OF CERTIORARI**

---

DAVID H. KRAMER  
MICHAEL H. RUBIN  
BRIAN M. WILLEN  
WILSON SONSINI  
GOODRICH & ROSATI P.C.  
650 Page Mill Road  
Palo Alto, CA 94304

SETH P. WAXMAN  
*Counsel of Record*  
RANDOLPH D. MOSS  
JONATHAN G. CEDARBAUM  
DANIEL P. KEARNEY, JR.  
WILMER CUTLER PICKERING  
HALE AND DORR LLP  
1875 Pennsylvania Ave., NW  
Washington, DC 20006  
seth.waxman@wilmerhale.com

BROOK HOPKINS  
WILMER CUTLER PICKERING  
HALE AND DORR LLP  
60 State Street  
Boston, MA 02109

---

---

## QUESTION PRESENTED

The Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, permits interception of “radio communications” that are not “scrambled or encrypted.” 18 U.S.C. § 2510(16)(A). The Act itself does not define “radio communications,” but for decades the accepted meaning of the term in the telecommunications field—and in a closely related statute, the Communications Act, 47 U.S.C. §§ 151 *et seq.*—has broadly encompassed all transmissions made using radio waves. That definition undisputedly includes the unencrypted Wi-Fi transmissions at issue in this case. The question presented is:

Whether the Ninth Circuit erred in holding that “radio communications” under the Wiretap Act are restricted to “predominantly auditory broadcasts” and do not include Wi-Fi communications even though Wi-Fi communications are transmitted using radio waves.

## **PARTIES TO THE PROCEEDINGS**

Defendant-appellant in the court of appeals, who is petitioner here, is Google Inc.

Plaintiffs-appellees in the court of appeals, who are respondents here, are: Benjamin Joffe, Lilla Marigza, Rick Benitti, Bertha Davis, Jason Taylor, Eric Myhre, John E. Redstone, Matthew Berlage, Patrick Keyes, Karl H. Schulz, James Fairbanks, Aaron Linsky, Dean M. Bastilla, Vicki Van Valin, Jeffrey Colman, Russell Carter, Stephanie Carter, and Jennifer Locsin.

## **CORPORATE DISCLOSURE STATEMENT**

Google Inc. does not have a parent corporation, and no publicly-held company owns ten percent or more of Google Inc.'s stock.

## TABLE OF CONTENTS

	Page
QUESTION PRESENTED .....	i
PARTIES TO THE PROCEEDINGS .....	ii
CORPORATE DISCLOSURE STATEMENT.....	ii
TABLE OF AUTHORITIES .....	vi
OPINIONS BELOW .....	1
JURISDICTION .....	2
STATUTORY PROVISIONS INVOLVED .....	2
INTRODUCTION AND STATEMENT .....	2
REASONS FOR GRANTING THE PETI- TION .....	9
I. THE NINTH CIRCUIT’S NOVEL GLOSS ON “RADIO COMMUNICATION” CONFLICTS WITH THE TERM’S LONG-ESTABLISHED MEANING AND WITH THE WIRETAP ACT’S TEXT AND PURPOSE.....	10
A. The Ninth Circuit’s Interpretation Is Inconsistent With The Established Meaning Of “Radio Communication” In The Telecommunications Field And Under Federal Law .....	10
B. The Ninth Circuit’s Interpretation Is Contradicted By The Text And Struc- ture Of The Wiretap Act.....	13
1. “Radio communication” in the wiretap act encompasses transmis- sions that are not “predominantly auditory” .....	13

**TABLE OF CONTENTS—Continued**

	Page
2. A central element of the ninth circuit’s reasoning—that “radio communication” does not encompass television—is plainly wrong under established telecommunications law.....	16
II. THE NINTH CIRCUIT’S DECISION FAILS TO ACCOUNT FOR MODERN TECHNOLOGICAL DEVELOPMENTS AND WILL HAVE WIDE-RANGING HARMFUL CONSEQUENCES .....	18
A. The Ninth Circuit’s Definition Draws A Line Between “Auditory” And “Non-Auditory” Transmissions That Has Become Meaningless .....	18
B. The Decision Below Creates Significant Uncertainty Regarding The Scope Of The Wiretap Act .....	19
C. The Ninth Circuit’s Holding Casts Doubt On The Legality Of Standard Security Procedures In The Information Technology Industry .....	22
D. Whether Unencrypted Wi-Fi Communications Are Covered By The Wiretap Act Presents A Significant Legal Issue .....	24
CONCLUSION .....	26
APPENDIX A: Amended Opinion of the United States Court of Appeals for the Ninth Circuit, dated December 27, 2013 .....	1a

**TABLE OF CONTENTS—Continued**

	Page
APPENDIX B: Opinion of the United States Court of Appeals for the Ninth Circuit, dated September 10, 2013 .....	31a
APPENDIX C: Order of the United States District Court for the Northern District of California, dated June 29, 2011.....	65a
APPENDIX D: Statutory Provisions .....	103a
Excerpts of 18 U.S.C. § 2510 .....	103a
Excerpts of 18 U.S.C. § 2511 .....	104a

## TABLE OF AUTHORITIES

### CASES

	Page(s)
<i>Apple Inc. v. Samsung Electronics Co.</i> , 695 F.3d 1370 (Fed. Cir. 2012) .....	19
<i>Commonwealth Scientific &amp; Industrial Research Organization v. Buffalo Technology (USA), Inc.</i> , 542 F.3d 1363 (Fed. Cir. 2008) .....	3
<i>DirectTV, Inc. v. FCC</i> , 110 F.3d 816 (D.C. Cir. 1997) .....	17
<i>Edwards v. State Farm Insurance Co.</i> , 833 F.2d 535 (5th Cir. 1987) .....	11
<i>Gozlon-Peretz v. United States</i> , 498 U.S. 395 (1991) .....	11
<i>In re Amendment of Parts 2, 73, &amp; 76</i> , 101 F.C.C.2d 973 (1985) .....	14
<i>In re Innovatio IP Ventures, LLC Patent Litigation</i> , 886 F. Supp. 2d 888 (N.D. Ill. 2012) .....	24
<i>In re Petition by Hawaiian Telephone Co.</i> , 16 F.C.C.2d 308 (1969) .....	12, 17
<i>In the Matter of Authorization of Spread Spectrum and Other Wideband Emissions Not Presently Provided for in the FCC Rules and Regulations</i> , 101 F.C.C.2d 419 (1985) .....	3
<i>In the Matter of Google Inc.</i> , 27 FCC Rcd 4012 (2012) .....	5, 13
<i>Kozoska v. Belford</i> , 417 U.S. 642 (1974) .....	12

**TABLE OF AUTHORITIES—Continued**

	Page(s)
<i>Leocal v. Aschcroft</i> , 543 U.S. 1 (2004) .....	22
<i>Northcross v. Memphis Board of Education</i> , 412 U.S. 427 (1973) .....	11
<i>United States v. Ahrndt</i> , Crim. No. 08-468, 2010 WL 373994 (D. Or. Jan. 28, 2010) .....	24, 25
<i>United States v. Rose</i> , 669 F.2d 23 (1st Cir. 1982) .....	11
<i>United States v. Shriver</i> , 989 F.2d 898 (7th Cir. 1992) .....	16, 17
<i>United States v. Szymuszkiewicz</i> , 622 F.3d 701 (7th Cir. 2010).....	18
<i>Winchester TV Cable Co. v. FCC</i> , 462 F.2d 115 (4th Cir. 1972).....	17

**STATUTES AND REGULATIONS**

7 U.S.C. § 2156 .....	17
Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.....	23
18 U.S.C.	
§ 1343.....	17
§ 2101.....	17
§ 2510.....	3, 6, 14, 20, 21
§ 2511.....	3, 6, 11, 15
§ 2520.....	25
28 U.S.C.	
§ 1254.....	2
§ 1292.....	7
Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-2 .....	23



**TABLE OF AUTHORITIES—Continued**

	Page(s)
47 U.S.C.	
§ 153.....	8
§ 605.....	11
Pub. L. No. 69-632, §31, 44 Stat. 1168, 1173 (1927).....	11
Pub. L. No. 73-416, §3(b), 48 Stat. 1064, 1065 (1934) (codified at 47 U.S.C. §153(4)).....	10
Wiretap Act, 18 U.S.C. §§ 2511 <i>et seq.</i> .....	2
45 C.F.R.	
§ 164.306.....	23
§ 164.308.....	23
§ 164.312.....	23
47 C.F.R.	
§ 2.1.....	12
§§ 25.101-25.701 .....	14, 16
§ 74.431.....	14
§ 74.432.....	14
§ 74.600.....	15
§ 74.601.....	15

**LEGISLATIVE MATERIALS**

H.R. Rep. No. 99-647 (1986).....	14, 17, 20, 21
S. Rep. No. 99-541 (1986).....	14

**OTHER AUTHORITIES**

Beyah, Raheem & Aravind Venkataraman, IEEE, <i>Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions</i> (Sept./Oct. 2011).....	23
---	----

## TABLE OF AUTHORITIES—Continued

	Page(s)
Cooke, Nelson M. & John Markus, <i>Electronics Dictionary</i> (1st ed. 1945).....	12
<i>Free Wireless Upgrades At Metro Airport Include Unlimited Minutes</i> , Detroit Free Press, Sept. 17, 2013, at A9.....	4
<i>Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness</i> , 66 Fed. Reg. 8616 (Feb. 1, 2001).....	23
Jacobson, Douglas & Joseph Idziorek, <i>Computer Security Literacy: Staying Safe in a Digital World</i> (2013) .....	4
Kerr, Dara, <i>Justice Department closes probe into Google Street View</i> , CNET (Apr. 26, 2012), available at <a href="http://news.cnet.com/8301-1023_3-57422652-93/justice-department-closes-probe-into-google-street-view/">http://news.cnet.com/8301-1023_3-57422652-93/justice-department-closes-probe-into-google-street-view/</a> .....	5
Letter to Albert Gidari, Esq., Counsel for Google, From David C. Vladeck, Director, Bureau of Consumer Protection (Oct. 27, 2010), available at <a href="http://www.ftc.gov/sites/default/files/documents/closing_letters/google-inquiry/101027googleletter.pdf">http://www.ftc.gov/sites/default/files/documents/closing_letters/google-inquiry/101027googleletter.pdf</a> .....	5
Mateti, Prabhaker, <i>Hacking Techniques in Wireless Networks</i> , in 3 <i>Handbook of Information Security</i> 83 (Hossein Bidgoli ed., 2006) .....	22, 23

**TABLE OF AUTHORITIES—Continued**

	Page(s)
McKinsey Global Institute, <i>Big Data: The Next Frontier for Innovation, Competition, and Productivity</i> (2011), available at <a href="http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation">http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation</a> .....	5
Meadows, A.J., et al., <i>Dictionary of New Information Technology</i> (1982) .....	12
Nagesh, Gautham, <i>FCC to Vote on Scrapping Telecom Landlines</i> , Wall St. J., Jan. 30, 2014, at B3.....	19
National Telecommunications & Information Administration, <i>About FirstNet</i> , available at <a href="http://www.ntia.doc.gov/page/about-firstnet">http://www.ntia.doc.gov/page/about-firstnet</a> (last visited Mar. 27, 2014).....	21
<i>Newton’s Telecom Dictionary</i> (26th ed. 2011) ....	3, 12, 13
Nisar, Kashif, et al., Information Technology (ITSim), 2010 International Symposium, <i>Enhanced Performance of Packet Transmission Using System Model Over VoIP Network</i> (June 2010).....	23
<i>Theatre Performances Available in Eight Languages</i> , BBC News, available at <a href="http://news.bbc.co.uk/2/hi/8380266.stm">http://news.bbc.co.uk/2/hi/8380266.stm</a> (last updated Nov. 26, 2014).....	4
<i>Webster’s New College Dictionary</i> (Michael Agnes ed., Wiley Publ’g, Inc. 2007) .....	3

IN THE  
**Supreme Court of the United States**

---

No. 13-

---

GOOGLE INC.,

*Petitioner,*

*v.*

JOFFE, *et al.*,

*Respondents.*

---

ON PETITION FOR A WRIT OF CERTIORARI TO THE  
UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

PETITION FOR WRIT OF CERTIORARI

---

Petitioner Google Inc. (“Google”) respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

**OPINIONS BELOW**

The opinion of the court of appeals (App. 1a-30a) is not yet published but is available at 2013 WL 6905957. That opinion amended a prior opinion (App. 31a-64a), which is reported at 729 F.3d 1262. The opinion of the district court (App. 65a-101a) is reported at 794 F. Supp. 2d 1067.

## JURISDICTION

The judgment of the court of appeals was entered on September 10, 2013. The court granted in part a petition for rehearing and filed an amended opinion on December 27, 2013. This Court has jurisdiction under 28 U.S.C. § 1254(1).

## STATUTORY PROVISIONS INVOLVED

Relevant provisions of the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, are reproduced in the Appendix.

## INTRODUCTION AND STATEMENT

This case concerns the application of the Wiretap Act, a criminal statute governing the interception of electronic and wire communications, to Wi-Fi and other technologies that involve the transmission of information using radio waves. The Ninth Circuit held that the statutory exemption for acquisition of unencrypted “radio communications” was not applicable because Wi-Fi transmissions are not “predominantly auditory broadcasts.” But that interpretation has no basis in the statutory text, is at odds with decades of understanding of the meaning of “radio communication” in telecommunications law, and is irreconcilable with modern communications technology, which does not distinguish between the transmission of auditory and other data files. Accordingly, if left uncorrected, the court of appeals’ decision will lead to confusion and uncertainty, particularly for the information technology industry and its tens of millions of customers.

1. The Wiretap Act broadly prohibits the interception of wire and electronic communications, but allows interception of “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). The Act expressly provides that “radio communications” are “readily accessible to the general public”—and thus exempt from the prohibition on interception—if they are not “scrambled or encrypted” (or transmitted in another restricted manner specified in the Act). *Id.* § 2510(16)(A). The question at issue in this case is whether unencrypted Wi-Fi communications, which are undisputedly carried over radio waves, are “radio communications” and thus not subject to the Wiretap Act’s ban on interception.

2. The term “Wi-Fi” refers to “a wireless local area network that uses radio waves to connect computers and other devices to the Internet.” *Webster’s New College Dictionary* 1636 (Michael Agnes ed., Wiley Publ’g, Inc. 2007). Wi-Fi transmissions are broadcast wirelessly to users over radio waves by devices known as routers or access points. *See Commonwealth Scientific & Indus. Research Org. v. Buffalo Tech., Inc.*, 542 F.3d 1363, 1367 (Fed. Cir. 2008) (explaining that in a Wi-Fi network, “remote devices communicate with the network access points by way of radio wave transmissions”). Wi-Fi networks operate on a specific portion of the radio spectrum allocated by the Federal Communications Commission (FCC). *See In the Matter of Authorization of Spread Spectrum and Other Wideband Emissions Not Presently Provided for in the FCC Rules and Regulations*, 101 F.C.C.2d 419, 428-430 ¶¶ 27-37 (1985). Wi-Fi is now the most common method for accessing the Internet. *Newton’s Telecom Dictionary* 1265 (26th ed. 2011). Every Wi-Fi device is assigned a unique number called a media access control (MAC) address, and routers and other access points are assigned an alpha-numeric service set identifier (SSID).

See Jacobson & Idziorek, *Computer Security Literacy: Staying Safe in a Digital World* 195, 208 (2013). Routers broadcast those SSIDs, which can be detected by computers, smartphones, and other devices with wireless capability. *Id.* at 195, 205.

The owner of a Wi-Fi network can choose to encrypt the network, often requiring users to enter a password before joining. Encryption prevents others from using the network and blocks public access to the information transmitted over the network. An unencrypted or open network is not similarly protected, and the information transmitted across the network may be acquired by the public. Indeed, Wi-Fi networks may be used to broadcast information to the public, such as subtitles translating live theater or advertisements broadcast to users of a public network. See *Theatre Performances Available in Eight Languages*, BBC News, available at <http://news.bbc.co.uk/2/hi/8380266.stm> (last updated Nov. 26, 2009); *Free Wireless Upgrades at Metro Airport Include Unlimited Minutes*, Detroit Free Press, Sept. 17, 2013, at A9.

3. Google is a company specializing in Internet-related services and products. Among its many products is an online mapping service called Street View, which provides panoramic, street-level photographs. App. 3a. Cameras mounted on cars that drive down public roads take the photographs available through Street View. *Id.* During the relevant period, the cars were also equipped with off-the-shelf radio equipment and commercially available software that allowed Google to collect identifying network information (MAC addresses and SSIDs) from Wi-Fi networks along the road. *Id.* Google collected that network identifying information to enhance its “location aware” services, which allow users to retrieve geographically relevant infor-

mation about local weather, nearby restaurants, and points of interest. *Id.* Because Wi-Fi networks have a limited range, networks can act as unique landmarks that make it possible to estimate mobile device users' locations. Many databases of network identifying information exist for this purpose. *See* McKinsey Global Inst., *Big Data: The Next Frontier for Innovation, Competition, and Productivity* 85-94 (2011), available at [http://www.mckinsey.com/insights/business\\_technology/big\\_data\\_the\\_next\\_frontier\\_for\\_innovation](http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation).

In addition to collecting identifying information about Wi-Fi networks, Google's Street View cars also collected so-called "payload data" that was sent over unencrypted Wi-Fi networks if the data was being broadcast at the moment the Street View cars passed within range of the networks. App. 4a. Google did not use any of this data in any product or service. Upon learning of the collection of payload data, Google took its Street View cars off the road and segregated the payload data the cars had collected. *Id.*

The Department of Justice, the Federal Trade Commission, and the FCC opened investigations of Google, including for possible violations of the Wiretap Act and Communications Act. All three ultimately declined to take enforcement action. *See* Kerr, *Justice Department Closes Probe Into Google Street View*, CNET, Apr. 26, 2012, available at [http://news.cnet.com/8301-1023\\_3-57422652-93/justice-department-closes-probe-into-google-street-view/](http://news.cnet.com/8301-1023_3-57422652-93/justice-department-closes-probe-into-google-street-view/); Ltr. to Gidari, Esq., Counsel for Google, from Vladeck, Director, Bureau of Consumer Protection (Oct. 27, 2010), available at [http://www.ftc.gov/sites/default/files/documents/closing\\_letters/google-inquiry/101027googleletter.pdf](http://www.ftc.gov/sites/default/files/documents/closing_letters/google-inquiry/101027googleletter.pdf); *In the Matter of Google Inc.*, 27 FCC Rcd 4012 (2012).



4. In response to Google’s public acknowledgment, more than a dozen putative class-action lawsuits were filed around the country, and eventually transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California. App. 4a. Respondents allege that payload data transmitted over their unencrypted Wi-Fi networks was collected by Google and seek to represent a class of all individuals whose Wi-Fi payload data was similarly collected. *Id.* Respondents filed a consolidated class action complaint asserting violations of the federal Wiretap Act as well as various state wiretap laws and California’s unfair competition law. *Id.*

5. The district court dismissed Respondents’ state-law claims on preemption and standing grounds, but held that Respondents’ complaint stated a claim under the Wiretap Act. App. 65a-101a.<sup>1</sup> The court recognized that 18 U.S.C. § 2510(16), which establishes that unencrypted radio communications are “readily accessible to the general public,” serves to define the scope of 18 U.S.C. § 2511(2)(g)(i), which permits the acquisition of “electronic communications” that are “readily accessible to the general public.” Because all radio communications are a form of electronic communication, the court held that the acquisition of such communications in unencrypted form is exempt from liability under the Wiretap Act. App. 86a, 89a. Thus, the court concluded, radio communications are “readily accessible to the general public” and not covered by the Wiretap Act unless the radio communications are “scrambled or encrypted” or transmitted by one of the other restricted methods specified in § 2510(16).

---

<sup>1</sup> Judge Ware issued the order under review; Judge Breyer now presides over the proceedings in the district court in this case.

But the court then defined “radio communication” narrowly so as to exclude unencrypted Wi-Fi transmissions. “Radio communication” is undefined in the Wiretap Act, but the district court declined to give the term its ordinary meaning—and the meaning it has long held in the telecommunications field—of simply all communications transmitted via radio waves. Instead, the court held that “radio communication” includes only “traditional radio services,” or “public-directed radio broadcast communication,” and not other technologies that communicate via radio waves such as unencrypted Wi-Fi networks and cellular phones. App. 87a-90a. Having concluded that unencrypted Wi-Fi transmissions are not “radio communications,” the court held that Respondents had adequately alleged that those transmissions were “electronic communications” not “readily accessible to the general public” under § 2511(2)(g)(i) and thus subject to the Wiretap Act’s interception prohibition. App. 92a-95a.

Google asked the district court to certify its Wiretap Act ruling for interlocutory appeal under 28 U.S.C. § 1292(b). The district court granted Google’s request, and the Ninth Circuit granted Google’s petition for permission to appeal.

6. The Ninth Circuit affirmed. App. 1a-30a. Like the district court, the court of appeals held that the definition of radio communications “readily accessible to the general public” in § 2510(16) applies to the § 2511(2)(g)(i) exemption to the prohibition on interception of electronic communications. App. 8a-10a. The court explained that the Act expressly provides that “radio communication” is a subset of “electronic communication,” and noted that “the statute directs us to apply § 2510(16) to the entire chapter.” App. 8a-9a. Thus, the appeals court concluded, a radio communica-

tion is deemed “readily accessible to the general public” and not covered by the Wiretap Act unless “scrambled or encrypted” or transmitted in another manner specified in § 2510(16). App. 10a-11a.

Rejecting both the district court’s definition and the one offered by Respondents, however, the court of appeals created its own unprecedented and untenably narrow definition of “radio communication.” The court acknowledged that because “radio communication” is not defined in the Wiretap Act, the court should give the term its ordinary meaning. App. 11a. Nevertheless, it rejected the conclusion that “radio communication” under the Wiretap Act, as in other related statutes, refers simply to any information transmitted using radio waves. App. 12a-14a. Instead, in the court of appeals’ view, the “ordinary meaning” of the term “radio communication” is “a predominantly auditory broadcast.” App. 15a. Thus, the court held that because the Wi-Fi transmissions Google acquired were not “predominantly auditory,” they did not constitute radio communications under the Act. App. 15a-16a.

In so holding, the court gave the phrases “radio communication” and “communication by radio”—both of which are used in the Wiretap Act—fundamentally different constructions. The court concluded that Congress intended to use the latter phrase “more expansively” to include “all communications using radio waves or a radio device.” App. 16a-17a. In reaching this conclusion, the court declined to apply the established definition in the Communications Act, which expressly defines “radio communication” and “communication by radio” to mean the same thing: “the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds.” 47 U.S.C. § 153(40); App. 13a-25a.

The court of appeals denied Google’s request for rehearing en banc on December 27, 2013.<sup>2</sup>

### REASONS FOR GRANTING THE PETITION

The term “radio communication” has for decades had an accepted meaning in the telecommunications field: a transmission of writing, signs, signals, pictures, or sounds *using radio waves*. That meaning dates back at least to the Communications Act of 1934, and is the established understanding of the term applied by courts and by the FCC. Here, however, the Ninth Circuit rejected that long-established definition. Instead, the court of appeals grafted an unprecedented limitation onto the meaning of “radio communication” under the Wiretap Act in holding that the term encompasses only “predominantly auditory broadcasts.” That interpretation defies established federal law, renders elements of the Wiretap Act incoherent, muddies the relationship between the Wiretap Act and the Communications Act, and improperly narrows the scope of the Act’s exemptive provisions.

The Ninth Circuit’s interpretation is not only wrong, it is also at odds with the reality of modern technologies, which erase any plausible line between “auditory” and “non-auditory” transmissions. A packet of data delivering voice is indistinguishable as it travels over radio waves from a packet of data delivering text. The court of appeals’ opinion staked its definition of “radio communication” on a distinction that is entirely illusory. In doing so, the Ninth Circuit’s interpretation

---

<sup>2</sup> The court of appeals initially issued an opinion on September 10, 2013. App. 31a-64a. Following Google’s petition for rehearing, the panel amended its original opinion on December 27, 2013 by deleting its discussion of an additional issue. App. 1a-30a. It is the amended opinion that is the subject of this petition.

creates significant ambiguity in an area of law where there is a need for clarity. Indeed, the court of appeals itself acknowledged that it was unsure how its novel interpretation applies to the billions of cell phone calls made in the United States each day.

The ruling creates substantial uncertainty regarding the scope of civil and criminal liability under the Wiretap Act—uncertainty that is particularly troubling given the ubiquity of modern information technologies, such as Wi-Fi, that involve the transmission of digital information by radio, and the potential for sizeable statutory damage awards under the Act. In light of all these considerations, the Court should grant the petition and resolve the important question of federal statutory construction that this case presents.

**I. THE NINTH CIRCUIT’S NOVEL GLOSS ON “RADIO COMMUNICATION” CONFLICTS WITH THE TERM’S LONG-ESTABLISHED MEANING AND WITH THE WIRE-TAP ACT’S TEXT AND PURPOSE**

**A. The Ninth Circuit’s Interpretation Is Inconsistent With The Established Meaning Of “Radio Communication” In The Telecommunications Field And Under Federal Law**

The Ninth Circuit’s interpretation of “radio communication” as limited to “predominantly auditory broadcasts” fails to give that term its established and accepted meaning under federal law. When Congress added “radio communication” to the Wiretap Act in 1986, the term had been defined for decades in related statutes. The Communications Act of 1934 expressly defined “radio communication” as “the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds.” Pub. L. No. 73-416, § 3(b), 48 Stat. 1064, 1065 (1934) (codified at 47 U.S.C. § 153(4)). And even before,

the Radio Act of 1927 had defined the term as “any intelligence, message, signal, power, pictures, or communication of any nature transferred by electrical energy from one point to another without the aid of any wire connecting the points from and at which the electrical energy is sent or received and any system by means of which such transfer of energy is effected.” Pub. L. No. 69-632, § 31, 44 Stat. 1162, 1173 (1927). Absent any indication to the contrary, the term “radio communication” should be read consistently across the Wiretap Act and these related statutes. *See, e.g., Northcross v. Memphis Board of Educ.*, 412 U.S. 427, 428 (1973) (per curiam) (“The similarity of language in [two statutes] is, of course, a strong indication that the two statutes should be interpreted *pari passu*.”); *Gozlon-Peretz v. United States*, 498 U.S. 395, 407-408 (1991) (when construing “specialized statutory terms,” courts “refer to other, related legislative enactments”).

Congress intended the Communications Act and the Wiretap Act to be construed in tandem. The two statutes expressly cross-reference each other. *See* 47 U.S.C. § 605(a) (Communications Act referencing Wiretap Act); 18 U.S.C. § 2511(2)(g)(iii) (Wiretap Act referencing Communications Act). And various provisions of the two statutes address the same subject matter, including provisions prohibiting interception that Congress intended to be read together. *See Edwards v. State Farm Ins. Co.*, 833 F.2d 535, 540 (5th Cir. 1987) (Wiretap Act limits the scope of § 605 of the Communications Act because “Congress likely intended to make the statutes consistent”); *United States v. Rose*, 669 F.2d 23, 26 (1st Cir. 1982) (“When Congress passed [the Wiretap Act] ..., it simultaneously amended § 605 to state that § 605 does not apply to communications that may be intercepted and disclosed under [the Wiretap

Act] by prefacing § 605’s prohibition against disclosure with the words ‘(e)xcept as authorized by (Title III).’” (alterations in original)). There is no plausible basis to construe the term “radio communication” differently across two statutes so closely intertwined. *See Kozoska v. Belford*, 417 U.S. 642, 650 (1974).

Yet that is precisely what the court of appeals did here. It gave the term “radio communication” in the Wiretap Act an entirely different meaning than it has in the Communications Act. That result is particularly confounding because the Ninth Circuit’s counter-textual definition diverges from the established meaning of “radio communication” in the telecommunications field. “Radio communication” is generally understood to mean “*any* communication using radio waves.” Meadows et al., *Dictionary of New Information Technology* 151 (1982) (emphasis added). “Radio communication” has long been understood to encompass transmissions of all kinds—auditory, visual, and otherwise—over radio waves. Indeed, an electronics dictionary from the 1940s defined the term (consistent with the Communications Act) as “[t]he transmission by radio of writing, signs, signals, pictures, and sounds of all kinds.” Cooke & Markus, *Electronics Dictionary* 303 (1st ed. 1945); *see also Newton’s Telecom Dictionary* 948 (26th ed. 2011) (defining “radio communication” as “[a]ny telecommunication by means of radio waves”).

The FCC’s longstanding definition of “radio communication” also clearly encompasses non-auditory radio transmissions. Under FCC rules, “radiocommunications” are all “[t]elecommunication[s] by means of radio waves.” 47 C.F.R. § 2.1; *see also In re Petition by Hawaiian Tel. Co.*, 16 F.C.C.2d 308, 310 (1969) (“A [television] broadcast signal is a radio communication.”). Not surprisingly, therefore, the FCC’s review of

Google's Street View activities never contemplated that "radio communication" under the Wiretap Act would not encompass Wi-Fi transmissions. *See In the Matter of Google, Inc.*, 27 FCC Rcd 4012, 4033-4034 ¶¶ 51-53 (2012).

The Ninth Circuit ignored all of this authority. Instead, it gave "radio communication" a new definition based on the panel's unsupported beliefs about the term's "ordinary meaning." Yet not only is the panel's definition contrary to every dictionary and supported by no other authorities, it also defies the way the term "radio" is actually used in common parlance, where it has never been limited to technologies that are predominantly auditory. For example, "packet radio" involves "the transmission of data over radio." *Newton's Telecom Dictionary* 856. And Radio Frequency Identity (RFID) technology, which uses radio waves to send data rather than sound, has everyday applications that range from identifying livestock, to paying highway tolls with E-ZPass, to tracking retail inventory. *Id.* at 979.

#### **B. The Ninth Circuit's Interpretation Is Contradicted By The Text And Structure Of The Wiretap Act**

The Ninth Circuit's definition of "radio communication" is contrary not only to the term's established meaning, but also to the text and structure of the Wiretap Act itself.

##### **1. "Radio communication" in the Wiretap Act encompasses transmissions that are not "predominantly auditory"**

The Wiretap Act identifies as "radio communications" a number of transmissions that are not "predominantly auditory broadcasts." The Ninth Circuit's re-



strictive definition, accordingly, cannot be squared with the Act's plain text.

Section 2510(16) lists several kinds of "radio communications" that contain substantial non-auditory content, such as text and pictures. For example, communications "carried on a subcarrier or other signal subsidiary to a radio transmission," 18 U.S.C. § 2510(16)(C), include "data carried on the Vertical Blanking Interval (VBI) of a television signal," S. Rep. No. 99-541, at 15 (1986). VBI communication is not predominantly auditory—it includes "textual and graphic information intended for display on viewing screens." *In re Amendment of Parts 2, 73, & 76*, 101 F.C.C.2d 973, 973-974 ¶2 (1985). Yet the Act identifies VBI communication as "radio communication." 18 U.S.C. § 2510(16)(C). Similarly, the Act forbids the interception of visual display pagers, "which involve the transmission of alphanumeric characters over the radio," S. Rep. No. 99-541, at 15, because they are a form of "radio communication" "carried by a common carrier," *id.*; 18 U.S.C. § 2510(16)(D).

Moreover, none of the "radio communications" transmitted on radio frequencies "allocated under part 25 and subparts D ... or F of part 74" of the FCC's rules, 18 U.S.C. § 2510(16)(E), are restricted to "predominantly auditory broadcasts." Those "radio communications" cover satellite broadcasts, including satellite television. 47 C.F.R. §§ 25.101-25.701. They also include Remote Pickup Broadcast Stations for "AM, FM, ... [and] TV ... station[s]," *id.* §§ 74.431, 74.432, which are used "for the transmission of material from the scene of events which occur outside the studio back to studio or production center," *id.* § 74.432(a). *See* H.R. Rep. No. 99-647, at 38 (1986) (the specified subparts of Part 74 include "video and audio transmissions from a news team in the field to the studio, and transmission from the studio to the

transmitter site”). And they include frequencies that are reserved for television broadcast auxiliary stations, and are used for the “transmission of TV program material and related communication.” 47 C.F.R. §§ 74.600, 74.601. Nor are the “radio communications” described in § 2511(2)(g)(ii) limited to “predominantly auditory broadcasts.” In particular, “radio communication which is transmitted by any station for the use of the general public,” 18 U.S.C. § 2511(2)(g)(ii)(I), includes “television broadcast signals,” H.R. Rep. No. 99-647, at 42 n.86—a type of transmission that, of course, is not “predominantly auditory.”

In short, the following non-auditory communications are clearly “radio communications” under the Wiretap Act:

- Display paging systems
- Data carried on the VBI of a television signal
- Television broadcasts
- Satellite transmissions (including satellite TV)
- Video transmissions from field reporters

These examples unmistakably demonstrate that the Wiretap Act itself does not limit the term “radio communication” to “predominantly auditory” transmissions. It is thus unsurprising that there is no support in the case law or any other authority for the Ninth Circuit’s restrictive definition.

These provisions also reveal the incongruity of construing “communication by radio” differently from “radio communication,” as the Ninth Circuit did. App. 16a-18a. For one, the two terms are just different formulations of the same words. Just as “travel by train” means the same thing as “train travel,” “radio commu-

nication” and “communication by radio” are synonymous. The Ninth Circuit’s claim that “communication by radio” is “used more expansively” to include “all communications using radio waves,” while “radio communication” “refer[s] more narrowly to broadcast radio technologies” is baseless. App. 16a-17a. The term “radio communication” as used in the Act encompasses far more than “auditory broadcasts,” as the provisions described above illustrate; the fact that “communication by radio” also encompasses non-auditory transmissions simply confirms the scope of both terms.

**2. A central element of the Ninth Circuit’s reasoning—that “radio communication” does not encompass television—is plainly wrong under established telecommunications law**

A central premise of the court of appeals’ restrictive definition was that “[o]ne would not ordinarily consider, say, television a form of “radio communication.” App. 12a. This further exposes the court’s error, however, as it is clear from the Wiretap Act’s text and legislative history that “radio communication” *does* encompass both broadcast and satellite television.

As explained above, at p. 14, subpart (E) of § 2510(16) categorizes transmissions over the radio frequencies allocated under part 25 of the FCC Rules as radio communications. Those frequencies are reserved for satellite communications, including satellite television. 47 C.F.R. §§ 25.101-25.701; *see United States v. Shriver*, 989 F.2d 898, 902 (7th Cir. 1992) (describing satellite television transmissions as “radio communications”). Moreover, it is clear that § 2511(2)(g)(ii)(I)’s reference to any “radio communication which is transmitted by any station for the use of the general public” was

intended to include broadcast television. *See* H.R. Rep. No. 99-647, at 42 n.86 (“television broadcast signals”).

Other federal courts have consistently classified television as a form of “radio communication.” *See, e.g., DirecTV, Inc. v. FCC*, 110 F.3d 816, 821 (D.C. Cir. 1997) (satellite television “is a radio communication service”); *Shriver*, 989 F.2d at 902; *Winchester TV Cable Co. v. FCC*, 462 F.2d 115, 118 n.9 (4th Cir. 1972) (“Radio communication, of course, includes television.”). The FCC has long held the same position. *See In re Petition by Hawaiian Tel. Co.*, 16 F.C.C.2d 308, 310, ¶ 9 (1969) (“A [television] broadcast signal is a radio communication[.]”).

The Ninth Circuit nevertheless based its analysis on the erroneous belief (at App. 12a) that Congress does not “assume[] that the term ‘radio’ encompasses the term ‘television.’” To support this conclusion, the court identified *other* statutes in which Congress referred to both “radio” and “television”—an observation that has no bearing on whether “radio communication” as used in the Wiretap Act encompasses television transmissions. App. 12a-13a. In any event, the other statutes cited by the Ninth Circuit use the word “radio” but do not even contain the term “radio communication,” and they are not telecommunications statutes at all. *See* 18 U.S.C. §§1343 (criminal mail fraud), 2101 (criminal incitement of a riot); 7 U.S.C. § 2156 (animal fighting). The far more apt comparison is to the Communications Act, which operates in tandem with the Wiretap Act, and unquestionably includes television in the definition of “radio communication.” *See infra* pp. 10-12.

In sum, the Ninth Circuit’s interpretation of “radio communication” is unprecedented, at odds with the statutory text and legislative history, and conflicts with

established interpretations of the term under federal law, as recognized by other courts and by the FCC. The Court should grant review to resolve the fundamental question the court of appeals' decision raises about the scope of the Wiretap Act.

## **II. THE NINTH CIRCUIT'S DECISION FAILS TO ACCOUNT FOR MODERN TECHNOLOGICAL DEVELOPMENTS AND WILL HAVE WIDE-RANGING HARMFUL CONSEQUENCES**

The Ninth Circuit's holding is not merely wrong. It is technologically unsound and creates serious practical problems in applying the Wiretap Act. Certiorari is warranted to restore coherence to this significant federal statute.

### **A. The Ninth Circuit's Definition Draws A Line Between "Auditory" And "Non-Auditory" Transmissions That Has Become Meaningless**

The Ninth Circuit's interpretation of "radio communication" rests on a distinction between "auditory" and "non-auditory" transmissions that has effectively disappeared with the evolution of modern communications technology. As a result, the court's decision threatens incoherence in the application of the Wiretap Act to the information technology industry.

While analog telephone lines or CB radios once carried "voice" or "auditory" transmissions distinct from other forms of transmission, that is no longer the case. Today, many voice calls are transmitted in packets of data using the "voice over Internet protocol" (VoIP), not only through services such as Skype and Vonage but even by primary telephone and cable providers. *See, e.g., United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010) ("Many phone calls today are made by digitizing speech and transferring the result

by packet switching.”); Nagesh, *FCC to Vote on Scraping Telecom Landlines*, Wall St. J., Jan. 30, 2014, at B3 (“VoIP is already offered by a number of phone and cable companies” and carriers such as AT&T and Verizon “want to retire their existing, circuit-switched systems and move to systems based on Internet protocol—essentially treating phone calls like other data moving over the Internet.”).

Other technologies have further blurred any “auditory”-“non-auditory” line. Text messages can be sent as voice messages that travel the Internet (and the airwaves) just like any other form of data. And technologies such as Apple’s Siri or Google’s Voice Search allow users to “speak” to a computer system over the Internet—to ask directions or to search the web—and provide for the system to “speak” back. *See Apple Inc. v. Samsung Elecs. Co.*, 695 F.3d 1370, 1375 (Fed. Cir. 2012) (“Advertised by Apple as an ‘intelligent personal assistant,’ Siri enables iPhone 4S users to speak their commands to the phone in a natural and conversational tone. ... [C]onsumers often use Siri in ways that include looking for information.”).

In the world of Internet protocol communications, a bit of data is simply a bit of data. The Ninth Circuit’s decision offers no intelligible rationale for distinguishing “auditory” bits from “non-auditory” ones.

### **B. The Decision Below Creates Significant Uncertainty Regarding The Scope Of The Wiretap Act**

Even as to more established technologies, the Ninth Circuit’s restrictive definition of “radio communication” introduces significant uncertainty in the application of the Wiretap Act. Indeed, the court of appeals’ decision calls into question how the Act applies to

basic modern technologies such as television and cell phone communications.

Consider the acquisition of television broadcast signals—watching TV—which, absent some exception, the Wiretap Act would prohibit. Television constitutes “wire communication” under 18 U.S.C. § 2510(1), (18), because it often contains “the human voice” and is generally transmitted “by the aid of wire, cable, or other like connection,” such as a cable television system. As such, it does not qualify for the exception in § 2511(2)(g)(i) for electronic communications that are “readily accessible to the general public” because wire communications are specifically excluded from the definition of electronic communications. *See* 18 U.S.C. § 2510(12)(A). Congress evidently intended § 2511(2)(g)(ii)(I)—covering any “radio communication which is transmitted by any station for the use of the general public”—to shield television from the prohibition on interception of electronic communications. H.R. Rep. No. 99-647, at 42 n.86. But under the Ninth Circuit’s interpretation, that exception would not apply because in its view “radio communication” does not encompass television. Surely Congress did not intend to criminalize watching television. The fact that the Ninth Circuit’s opinion, taken to its logical conclusion, suggests otherwise highlights the error of the court’s interpretation and the mischief it may cause.

Similarly, the Ninth Circuit’s definition creates doubt as to whether intercepting transmissions from “public safety communications systems” and “marine or aeronautical communications systems” would be protected from liability under § 2511(2)(g)(ii), as Congress intended, if such transmissions contained non-auditory information. Increasingly, such transmissions do contain non-auditory information—they contain data. *See*,

*e.g.*, National Telecommunications & Information Administration, *About FirstNet*, available at <http://www.ntia.doc.gov/page/about-firstnet> (last visited Mar. 27, 2014) (describing broadband data network for first responders).

Perhaps even more remarkably, the Ninth Circuit’s opinion calls into question whether ordinary cell phone calls are protected from interception under the Wiretap Act. The opinion itself acknowledges that, under its reading of the law, whether cell phone calls satisfy the “broadcast” portion of its “predominantly audio broadcast” test and thus qualify as radio communications is a “close question.” App. 15a. That acknowledgment leaves the tens of millions of cell phone users in the Ninth Circuit uncertain about whether their calls can lawfully be intercepted—and highlights the error of the court’s interpretation. It is clear from the Act’s legislative history that Congress viewed cell phone communications as “radio communications” and intended the “common carrier” provision in 18 U.S.C. § 2510(16)(D) to protect cell phone communications from interception. *See* H.R. Rep. No. 99-647, at 32 (“Because cellular communication is transmitted over a communication system currently regarded by the FCC as a common carrier, the Committee also intends that such communication not be considered ‘readily accessible to the general public’ at any time subsequent to the date of enactment, regardless of how a provider of cellular service is denominated by any state or how the FCC may classify any such provider in the future.” (footnote omitted)). By leaving open whether cell phone transmissions are “radio communications,” the Ninth Circuit has created ambiguity in an area where Congress intended certainty.



In short, the Ninth Circuit’s decision is out of step with modern technology and introduces significant ambiguities in the application of the Wiretap Act, creating uncertainty about how the Act applies even to everyday technological activities.<sup>3</sup>

### **C. The Ninth Circuit’s Holding Casts Doubt On The Legality Of Standard Security Procedures In The Information Technology Industry**

Review is also warranted because the Ninth Circuit’s decision potentially renders unlawful—and subjects to possible criminal liability—security procedures that are standard in the information technology (IT) industry. IT professionals routinely use the same kind of technology as Google’s Street View cars did to collect packet data in order to secure company networks. And unlike Google, which never used the payload data it collected, security professionals also parse and analyze the data collected from wired and wireless networks, including networks operated by other persons or entities, to identify vulnerabilities in and potential attacks on the networks they protect. *See generally* Mateti, *Hacking Techniques in Wireless Networks*, in 3 *Handbook of Information Security* 83, 83-93 (Hossein Bidgoli ed., 2006). For example, IT security experts use packet analysis to monitor wireless traffic in order to create a list of all access points in use. This allows them to detect unauthorized or rogue Wi-Fi access points in the

---

<sup>3</sup> Because the Wiretap Act is a criminal statute, the rule of lenity required the court to resolve any ambiguity in Petitioner’s favor and to adopt the established definition of “radio communication.” *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (“Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies.”). But far from resolving any ambiguity in the Act, the court of appeals’ decision compounded it.

network—*i.e.*, unapproved Wi-Fi networks that may be set up by employees to circumvent network security or by attackers to infiltrate the company’s network. *See, e.g.*, Beyah & Venkataraman, *Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions*, IEEE 56-57 (Sept./Oct. 2011).

These types of security measures are critical. Networks that connect company computers to each other and to the Internet are vulnerable to hacking and other security breaches, even when they are properly encrypted. *See generally* Mateti, *supra*, at 83-90. Moreover, federal statutes and regulations require certain entities, such as healthcare providers and financial institutions, to meet network security standards. *See* Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d-2 (information security for health information); 45 C.F.R. §§ 164.306, 164.308, 164.312 (associated regulations); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (information security for financial institutions); *Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness*, 66 Fed. Reg. 8616 (Feb. 1, 2001) (associated regulations).

Packet analysis can also help to enforce company policies prohibiting employees from bringing unauthorized wireless devices to worksites by tracking the addresses of all Wi-Fi devices using the network. And it can be used to optimize network performance by, for example, analyzing traffic to determine how to decrease packet loss. *See, e.g.*, Nisar et al., 2010 International Symposium, *Enhanced Performance of Packet Transmission Using System Model Over VoIP Network*, Information Technology (ITSim) 1005-1008 (June 2010).

Each of these legitimate uses of packet analysis technology could result in the acquisition of payload data from nearby unencrypted Wi-Fi networks. The technology does not distinguish between company signals and external signals—indeed doing so would defeat its security purpose. Thus, packet analysis will often collect data from any open Wi-Fi network within range. In densely populated areas, this will likely include individual home networks of the sort Respondents claim to operate. Rather than providing a clear definition that IT security professionals could rely on, the Ninth Circuit’s definition imperils an important IT security tool.

**D. Whether Unencrypted Wi-Fi Communications Are Covered By The Wiretap Act Presents A Significant Legal Issue**

Various courts in recent years have confronted the application of the Wiretap Act to unencrypted Wi-Fi transmissions, and none has adopted the Ninth Circuit’s erroneous interpretation. In *In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012), a plaintiff in a patent infringement action sought an admissibility ruling on its proposed discovery protocol to collect evidence using packet analysis (or “sniffing”) technology. The court held that the proposed protocol would not violate the Wiretap Act because “in light of the ease of ‘sniffing’ Wi-Fi networks ... the communications sent on an unencrypted Wi-Fi network are readily accessible to the general public.” *Id.* at 893.

Similarly, in *United States v. Ahrndt*, Crim No. 08-468, 2010 WL 373994 (D. Or. Jan. 28, 2010) *rev’d on other grounds and remanded*, 475 F. App’x 656 (9th Cir. 2012), the defendant filed a motion to suppress evidence collected from his shared iTunes library, which the of-

ficer accessed via defendant's unsecured Wi-Fi network. The court rejected the argument that the officer's conduct violated the Wiretap Act, holding that since defendant's Wi-Fi network was unencrypted, it was "configured so that any electronic communications emanating from his computer ... were readily accessible to any member of the general public with a Wi-Fi enabled laptop." *Arndt*, 2010 WL 373994, at \*8.

Given the ubiquity of Wi-Fi and the availability of packet-analysis technology, issues regarding the application of the Wiretap Act to Wi-Fi transmissions will continue to arise and with increasing frequency. The significance of the issue is all the greater because the Wiretap Act provides for statutory damages, in appropriate cases, in the amount of the greater of \$100 per day for each day of violation or \$10,000. 18 U.S.C. § 2520(c)(B). Defendants therefore face significant potential damages for conduct that would be innocent absent the Ninth Circuit's erroneous interpretation. This Court should intervene now and settle the uncertainty regarding the application of the Wiretap Act to Wi-Fi transmissions.

\* \* \*

The decision below manufactures a definition of "radio communication" that is at odds with established federal law and with the text, structure, and legislative history of the Wiretap Act. The Ninth Circuit's interpretation is based on a purported distinction between non-auditory and auditory radio transmissions that is illusory in modern communications technologies. The decision thus creates significant complications regarding application of the Wiretap Act to information technologies and introduces significant legal uncertainty. In light of the clear error of the court of appeals' deci-

sion, and the decision's ramifications for the information technology industry, the Court should grant review on this important question of federal statutory interpretation.

**CONCLUSION**

The petition for a writ of certiorari should be granted.

Respectfully submitted.

DAVID H. KRAMER  
MICHAEL H. RUBIN  
BRIAN M. WILLEN  
WILSON SONSINI  
GOODRICH & ROSATI P.C.  
650 Page Mill Road  
Palo Alto, CA 94304

SETH P. WAXMAN  
*Counsel of Record*  
RANDOLPH D. MOSS  
JONATHAN G. CEDARBAUM  
DANIEL P. KEARNEY, JR.  
WILMER CUTLER PICKERING  
HALE AND DORR LLP  
1875 Pennsylvania Ave., NW  
Washington, DC 20006  
seth.waxman@wilmerhale.com

BROOK HOPKINS  
WILMER CUTLER PICKERING  
HALE AND DORR LLP  
60 State Street  
Boston, MA 02109

MARCH 2014

# APPENDICES

**APPENDIX A**

UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

No. 11-17483  
D.C. No. 5:10-md-02184-JW

---

BENJAMIN JOFFE; LILLA MARIGZA; RICK BENITTI;  
BERTHA DAVIS; JASON TAYLOR; ERIC MYHRE; JOHN E.  
REDSTONE; MATTHEW BERLAGE; PATRICK KEYES;  
KARL H. SCHULZ; JAMES FAIRBANKS; AARON LINSKY;  
DEAN M. BASTILLA; VICKI VAN VALIN; JEFFREY  
COLMAN; RUSSELL CARTER; STEPHANIE CARTER;  
JENNIFER LOCSIN,  
*Plaintiffs-Appellees,*  
*v.*

GOOGLE, INC.,  
*Defendant-Appellant.*

---

Appeal from the United States District Court  
for the Northern District of California  
James Ware, District Judge, Presiding

---

Argued and Submitted  
June 10, 2013—San Francisco, California  
Filed September 10, 2013  
Amended December 27, 2013

---

**ORDER AND AMENDED OPINION**

---

Before: A. Wallace Tashima and Jay S. Bybee, Circuit Judges, and William H. Stafford, Senior District Judge.\*

Opinion by Judge Bybee

\* \* \*

### ORDER

Appellant's motion for leave to file a reply brief in support of its petition for rehearing and rehearing en banc, filed on November 6, 2013, is **GRANTED**.

Appellant's petition for rehearing, filed on September 24, 2013, is **GRANTED IN PART**. The court's opinion, filed on September 10, 2013, and appearing at 729 F.3d 1362 (9th Cir. 2013), is hereby **AMENDED**. An amended opinion is filed concurrently with this order.

Judge Bybee votes to deny Appellant's petition for rehearing en banc, filed on September 24, 2013, and Judge Tashima and Judge Stafford so recommend. The full court has been advised of Appellant's petition for rehearing en banc, and no request to vote on whether to rehear the case en banc has been made. Appellant's petition for rehearing en banc is **DENIED**.

No subsequent petitions for rehearing or rehearing en banc shall be filed by either party.

### OPINION

BYBEE, Circuit Judge:

In the course of capturing its Street View photographs, Google collected data from unencrypted

---

\* The Honorable William H. Stafford, Jr., Senior District Judge for the U.S. District Court for the Northern District of Florida, sitting by designation.



Wi-Fi networks. Google publicly apologized, but plaintiffs brought suit under federal and state law, including the Wiretap Act, 18 U.S.C. § 2511. Google argues that its data collection did not violate the Act because data transmitted over a Wi-Fi network is an “electronic communication” that is “readily accessible to the general public” and exempt under the Act. 18 U.S.C. § 2511(2)(g)(i). The district court rejected Google’s argument. *In re Google Inc. St. View Elec. Comm’n Litig.*, 794 F. Supp. 2d 1067, 1073–84 (N.D. Cal. 2011). We affirm.

## I. BACKGROUND

### A. *Facts and History*

Google launched its Street View feature in the United States in 2007 to complement its Google Maps service by providing users with panoramic, street-level photographs. Street View photographs are captured by cameras mounted on vehicles owned by Google that drive on public roads and photograph their surroundings. Between 2007 and 2010, Google also equipped its Street View cars with Wi-Fi antennas and software that collected data transmitted by Wi-Fi networks in nearby homes and businesses. The equipment attached to Google’s Street View cars recorded basic information about these Wi-Fi networks, including the network’s name (SSID), the unique number assigned to the router transmitting the wireless signal (MAC address), the signal strength, and whether the network was encrypted. Gathering this basic data about the Wi-Fi networks used in homes and businesses enables companies such as Google to provide enhanced “location-based” services, such as those that allow mobile phone users to find nearby restaurants and attractions or receive driving directions.

But the antennas and software installed in Google's Street View cars collected more than just the basic identifying information transmitted by Wi-Fi networks. They also gathered and stored "payload data" that was sent and received over unencrypted Wi-Fi connections at the moment that a Street View car was driving by.<sup>1</sup> Payload data includes everything transmitted by a device connected to a Wi-Fi network, such as personal emails, usernames, passwords, videos, and documents.

Google acknowledged in May 2010 that its Street View vehicles had been collecting fragments of payload data from unencrypted Wi-Fi networks. The company publicly apologized, grounded its vehicles, and rendered inaccessible the personal data that had been acquired. In total, Google's Street View cars collected about 600 gigabytes of data transmitted over Wi-Fi networks in more than 30 countries.

Several putative class-action lawsuits were filed shortly after Google's announcement, and, in August 2010, the cases were transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California. In November, 2010, Plaintiffs-Appellees (collectively "Joffe") filed a consolidated complaint, asserting claims against Google under the federal Wiretap Act, 18 U.S.C. § 2511; California Business and Professional Code § 17200; and various state wiretap statutes. Joffe seeks to represent a class comprised of all persons whose electronic communications were intercepted by Google Street View vehicles since May 25, 2007.

---

<sup>1</sup> Google may have also used its software to capture encrypted data, but the plaintiffs have conceded that their wireless networks were unencrypted.

Google moved to dismiss Joffe’s consolidated complaint. The district court declined to grant Google’s motion to dismiss Joffe’s federal Wiretap Act claims.<sup>2</sup> *In re Google Inc. St. View Elec. Commc’n Litig.*, 794 F. Supp. 2d at 1084. On Google’s request, the court certified its ruling for interlocutory appeal under 28 U.S.C. § 1292(b) because the district court resolved a novel question of statutory interpretation. We granted Google’s petition, and we have jurisdiction under 28 U.S.C. § 1292(b).

### B. *District Court’s Decision*

Google maintained before the district court that it should have dismissed Joffe’s Wiretap Act claims because data transmitted over unencrypted Wi-Fi networks falls under the statutory exemption that makes it lawful to intercept “electronic communications” that are “readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i). The question was whether payload data transmitted on an unencrypted Wi-Fi network is “readily accessible to the general public,” such that the § 2511(2)(g)(i) exemption applies to Google’s conduct.

To answer this question, the district court first looked to the definitions supplied by the Act. *In re Google Inc. St. View Elec. Commc’n Litig.*, 794 F. Supp. 2d at 1075–76. The statute provides in relevant part that “‘readily accessible to the general public’ means, with respect to a radio communication, that such communication is not ... (A) scrambled or encrypted.”

---

<sup>2</sup> The district court granted Google’s motion to dismiss Joffe’s claims under California law and other state wiretap statutes. *In re Google Inc. St. View Elec. Commc’n Litig.*, 794 F. Supp. 2d at 1085–86. These claims are not at issue here.

18 U.S.C. § 2510(16). An unencrypted *radio communication* is, therefore, “readily accessible to the general public.” In short, intercepting an unencrypted *radio communication* does not give rise to liability under the Wiretap Act because of the combination of the § 2511(2)(g)(i) exemption and the § 2510(16) definition.

The district court then considered whether data transmitted over a Wi-Fi network is a “radio communication” because the phrase is not defined by the Act. *In re Google Inc. St. View Elec. Commc’n Litig.*, 794 F. Supp. 2d at 1076–81. The court reasoned that “radio communication” encompasses only “traditional radio services,” and not other technologies that also transmit data using radio waves, such as cellular phones and Wi-Fi networks.<sup>3</sup> *Id.* at 1079–83. Since Wi-Fi networks are not a “radio communication,” the definition of “readily accessible to the general public” provided by § 2510(16) does not apply because the definition is expressly limited to electronic communications that are radio communications.

Finally, the court addressed whether data transmitted over unencrypted Wi-Fi networks is nevertheless an “electronic communication” that is “readily accessible to the general public” under § 2511(2)(g)(i). *Id.* at 1082–84. Although the court determined that Wi-Fi networks do not involve a “radio communication” under § 2510(16) and are therefore not “readily accessible to the general public” by virtue of the definition of the phrase, it still had to resolve whether they are “readily accessible to the general

---

<sup>3</sup> It is less clear whether the district court’s definition also excludes television broadcasts. Joffe argued at oral argument that television broadcasts are “traditional radio services.”

public” as the phrase is ordinarily understood because the statute does not define the phrase as it applies to an “electronic communication” that is not a “radio communication.” The court reasoned that “without more, merely pleading that a network is unencrypted does not render that network readily accessible to the general public and serve to remove the intentional interception of electronic communications from that network from liability under the [Electronic Communications Privacy Act].” *Id.* at 1084. The court accordingly declined to grant Google’s motion to dismiss Joffe’s Wiretap Act claims. *Id.*

## II. OVERVIEW OF THE WIRETAP ACT

The Wiretap Act imposes liability on a person who “intentionally intercepts ... any wire, oral, or electronic communication,” 18 U.S.C. § 2511(1)(a), subject to a number of exemptions. *See* 18 U.S.C. § 2511(2)(a)–(h). There are two exemptions that are relevant to our purposes. First, the Wiretap Act exempts intercepting “an electronic communication made through an electronic communication system” if the system is configured so that it is “readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i). “Electronic communication” includes communication by radio, 18 U.S.C. § 2510(12), and “readily accessible to the general public” means, with respect to a radio communication that the communication is “not ... scrambled or encrypted,” 18 U.S.C. § 2510(16)(A). Second, the Act exempts intercepting “radio communication” by “any station for the use of the general public;” by certain governmental communication systems “readily accessible to the general public,” including police, fire, and civil defense agencies; by a station operating on an authorized

frequency for “amateur, citizens band, or general mobile radio services;” or by a marine or aeronautical communications system. 18 U.S.C. § 2511(2)(g)(ii)(I)–(IV).

Google only argues, as it did before the district court, that it is exempt from liability under the Act because data transmitted over a Wi-Fi network is an “electronic communication ... readily accessible to the general public” under § 2511(2)(g)(i). It concedes that it does not qualify for any of the exemptions for specific types of “radio communication” under § 2511(2)(g)(ii). Joffe, however, argues that if data transmitted over a Wi-Fi network is not exempt as a “radio communication” under § 2511(2)(g)(ii), it cannot be exempt as a radio communication under the broader exemption for “electronic communication” in § 2511(2)(g)(i). This argument has some force, and we wish to address it before we consider Google’s claims.

Joffe contends that the definition of “readily accessible to the general public” in § 2510(16) does not apply to the § 2511(2)(g)(i) exemption. Instead, Joffe argues, the § 2510(16) definition applies exclusively to § 2511(2)(g)(ii)(II), which exempts specifically enumerated types of “radio communication” when they are “readily accessible to the general public.” We ultimately reject Joffe’s alternative reading of the statute, although—as we will explain—we find § 2511(2)(g)(ii) useful as a lexicographical aid to understanding the phrase “radio communication.”

As noted, § 2510(16) defines “readily accessible to the general public” solely with respect to a “radio communication,” and not with respect to other types of “electronic communication.” Although § 2511(2)(g)(i) does not use the words “radio communication,” the

statute nevertheless directs us to apply the § 2510(16) definition to the § 2511(2)(g)(i) exemption. First, “radio communication” is a subset of “electronic communication.” See 18 U.S.C. § 2510(12) (providing that, subject to certain exceptions, “‘electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, *radio*, electromagnetic, photoelectronic or photooptical system”) (emphasis added). Second, the statute directs us to apply § 2510(16) to the entire chapter. The definitions in 18 U.S.C. § 2510 are prefaced with the phrase, “As used in this chapter.” We cannot disregard this command by holding that the definition of “‘readily accessible to the general public’ [ ] with respect to a radio communication” applies to § 2511(2)(g)(ii), but not § 2511(2)(g)(i).

Admittedly, following the plain language of the statute creates some tension with § 2511(2)(g)(ii)(II), which provides an exemption for intercepting “any radio communication which is transmitted ... by any governmental, law enforcement, civil defense, private land mobile, or public communications system, including police and fire, readily accessible to the general public.” Under our reading of the statute—which is the same reading adopted by the district court, Google, and Joffe in his lead argument—§ 2511(2)(g)(i) exempts all electronic communications (including radio communications) that are “readily accessible to the general public” as the phrase is defined in § 2510(16). This reading likely renders § 2511(2)(g)(ii)(II) superfluous. As discussed, that section exempts specific kinds of radio communications that are “readily accessible to the general public,” such as those transmitted by a law enforcement communications

system. But this exemption is unnecessary when § 2511(2)(g)(i) already exempts all radio communications that are “readily accessible to the general public.”

Although our reading may render § 2511(2)(g)(ii)(II) superfluous or at least redundant, we understand that Congress “sometimes drafts provisions that appear duplicative of others—simply in Macbeth’s words, ‘to make assurance double sure.’ That is, Congress means to clarify what might be doubtful—that the mentioned item is covered.” *Shook v. D.C. Fin. Responsibility & Mgmt. Assistance Auth.*, 132 F.3d 775, 782 (D.C. Cir. 1998). This interpretation is especially plausible given that Congress was concerned that radio hobbyists not face liability for intercepting readily accessible broadcasts, such as those covered by § 2511(2)(g)(ii)(II), which can be picked up by a police scanner. *See* 132 Cong. Rec. S7987-04 (1986) (“In order to address radio hobbyists’ concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful.”).

In short, we agree with Google that the definition of “readily accessible to the general public” in § 2510(16) applies to the § 2511(2)(g)(i) exemption when the communication in question is a “radio communication.” With that understanding, we now turn to whether data transmitted over a Wi-Fi network is a “radio communication” exempt from the Wiretap Act as an “electronic communication” under § 2511(2)(g)(i).

### III. ANALYSIS

Google contends that data transmitted over a Wi-Fi network is a “radio communication” and that the Act exempts such communications by defining them as



“readily accessible to the general public,” 18 U.S.C. § 2511(2)(g)(i), so long as “such communication is not ... scrambled or encrypted,” 18 U.S.C. § 2510(16)(A). We reject this claim.<sup>4</sup> We hold that the phrase “radio communication” in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi-Fi network. As a consequence, the definition of “readily accessible to the general public [ ] with respect to a radio communication” set forth in § 2510(16) does not apply to the exemption for an “electronic communication” that is “readily accessible to the general public” under 18 U.S.C. § 2511(2)(g)(i).

A. *The Ordinary Meaning of “Radio Communication” Does Not Include Data Transmitted over a Wi-Fi Network*

The Wiretap Act does not define the phrase “radio communication” so we must give the term its ordinary meaning. See *Hamilton v. Lanning*, 130 S. Ct. 2464, 2471 (2010) (“When terms used in a statute are undefined, we give them their ordinary meaning.”); *United States v. Daas*, 198 F.3d 1167, 1174 (9th Cir. 1999) (“If the statute uses a term which it does not define, the court gives that term its ordinary meaning.”).

---

<sup>4</sup>This case raises a question of statutory interpretation, which we review de novo. *Phoenix Mem’l Hosp. v. Sebelius*, 622 F.3d 1219, 1224 (9th Cir. 2010). We begin by “determin[ing] whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case.” *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 450 (2002). We must assume that “the ordinary meaning of that language accurately expresses the legislative purpose [of Congress].” *Park ’N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985).

According to Google, radio communication “refers to any information transmitted using radio waves, *i.e.*, the radio frequency portion of the electromagnetic spectrum.” Appellant’s Br. at 28. The radio frequency portion of the spectrum is “the part of the spectrum where electromagnetic waves have frequencies in the range of about 3 kilohertz to 300 gigahertz.” *Id.* at 27.

Google’s technical definition does not conform with the common understanding held contemporaneous with the enacting Congress. *See United States v. Iverson*, 162 F.3d 1015, 1022 (9th Cir. 1998) (“When a statute does not define a term, we generally interpret that term by employing the *ordinary, contemporary, and common* meaning of the words that Congress used”) (emphasis added). The radio frequency portion of the electromagnetic spectrum covers not only Wi-Fi transmissions, but also television broadcasts, Bluetooth devices, cordless and cellular phones, garage door openers, avalanche beacons, and wildlife tracking collars. *See* Fed. Comm’n Comm’n, *Encyclopedia – FM Broadcast Station Classes and Service Countours*, available at <http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf> (last visited Aug. 13, 2013). One would not ordinarily consider, say, television a form of “radio communication.” Not surprisingly, Congress has not typically assumed that the term “radio” encompasses the term “television.” *See, e.g.*, 18 U.S.C. § 1343 (imposing liability for “[f]raud by wire, radio, or television”) (emphasis added); 18 U.S.C. § 2101 (imposing liability for inciting a riot by means of “mail, telegraph, radio, or television”) (emphasis added); 7 U.S.C. § 2156 (defining an “instrumentality of interstate commerce” as “any written, wire, radio, television or other form of communication); *see also FCC v. Nat’l Citizens Comm. for Broad.*, 436 U.S. 775,

815 (1978) (noting that “radio and television stations are given different weight,” under the regulations at issue, and describing regulations governing “a radio *or* television broadcast station”) (emphasis added).

The Wiretap Act itself does not assume that the phrase “radio communication” encompasses technologies like satellite television that are outside the scope of the phrase as it is ordinarily defined. For example, the statute’s damages provision sets out specified penalties when the “violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted *or* if the communication is a radio communication that is transmitted on [frequencies specified by regulation].” 18 U.S.C. § 2520(c)(1) (emphasis added). Congress described separately the act of “viewing [ ] a private satellite video communication” even though such communication is transmitted on a radio frequency and would fall within Google’s proposed definition of “radio communication.” Taken together, these disparate provisions offer evidence that Congress does not use “radio” or “radio communication” to reference all of the myriad forms of communication that use the radio spectrum. Rather, it uses “radio” to refer to traditional radio technologies, and then separately describes other modes of communication that are not ordinarily thought of as radio, but that nevertheless use the radio spectrum.

Google’s proposed definition is in tension with how Congress—and virtually everyone else—uses the phrase. In common parlance, watching a television show does not entail “radio communication.” Nor does sending an email or viewing a bank statement while connected to a Wi-Fi network. There is no indication that the Wiretap Act carries a buried implication that

the phrase ought to be given a broader definition than the one that is commonly understood. *See Mohamad v. Palestinian Auth.*, 132 S. Ct. 1702, 1707 (2012) (favoring a definition that matches “how we use the word in everyday parlance” and observing that “Congress remains free, as always, to give the word a broader or different meaning. But before we will assume it has done so, there must be *some* indication Congress intended such a result”).

Importantly, Congress provided definitions for many other similar terms in the Wiretap Act, but refrained from providing a technical definition of “radio communication” that would have altered the notion that it should carry its common, ordinary meaning. *See, e.g.*, 18 U.S.C. § 2510(1) (defining “wire communication”); 18 U.S.C. § 2510(12) (defining “electronic communication”); 18 U.S.C. § 2510(15) (defining “electronic communication service”); 18 U.S.C. § 2510(17) (defining “electronic storage”). As Google writes in its brief, “[t]he fact that the Wiretap Act provides specialized definitions for certain compound terms—but not for ‘radio communication’—is powerful evidence that the undefined term was not similarly intended [to] be defined in a specialized or narrow way” but rather “according to its ordinary meaning.” Appellant’s Br. at 29. We agree and, accordingly, we reject Google’s proposed definition of “radio communication” in favor of one that better reflects the phrase’s ordinary meaning.

B. *A “Radio Communication” is a Predominantly Auditory Broadcast, Which Excludes Payload Data Transmitted over Wi-Fi Networks*

There are two telltale indicia of a “radio communication.” A radio communication is commonly

understood to be (1) predominantly auditory, and (2) broadcast. Therefore, television—whether connected via an indoor antenna or a satellite dish—is not radio, by virtue of its visual component. A land line phone does not broadcast, and, for that reason, is not radio. On the other hand, AM/FM, Citizens Band (CB), ‘walkie-talkie,’ and shortwave transmissions are predominantly auditory, are broadcast, and are, not coincidentally, typically referred to as “radio” in everyday parlance. Thus, we conclude that “radio communication” should carry its ordinary meaning: a predominantly auditory broadcast.<sup>5</sup>

The payload data transmitted over unencrypted Wi-Fi networks that was captured by Google included emails, usernames, passwords, images, and documents that cannot be classified as predominantly auditory. They therefore fall outside of the definition of a “radio

---

<sup>5</sup> We need not reach the question of what exactly constitutes a “broadcast” because the Wi-Fi transmissions in question were not predominantly auditory. Whether cell phone calls—which are projected wirelessly over great distances—are broadcast would similarly be a close question.

We also need not fully consider the extent to which non-auditory transmissions may be included in a broadcast before that broadcast is no longer a radio broadcast. Modern FM radio stations, for example, commonly transmit small amounts of data denoting the artist and title of the song. But because such data is ancillary to the audio transmission, they likely do not remove the transmissions from the domain of a “radio communication” under the Act.

And, finally, we do not address how to classify a traditional radio broadcast delivered to a web-enabled device connected to a Wi-Fi network, such as a radio station streamed over the internet. Here, Google’s collection efforts were not limited to auditory transmissions.

communication” as the phrase is used in 18 U.S.C. § 2510(16).

C. *Defining “Radio Communication” to Include Only Predominantly Auditory Broadcasts is Consistent with the Rest of the Wiretap Act*

Crucially, defining “radio communication” as a predominantly auditory broadcast yields a coherent and consistent Wiretap Act. Google’s overly broad definition does not. *See K Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988) (“In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole.”)

Throughout the Wiretap Act, Congress used the phrase “radio communication”—which is at issue here—and the similar phrase “communication by radio.” Even within the very provision that we are construing—18 U.S.C. § 2510(16)—Congress used both phrases. We must ascribe to each phrase its own meaning. *See SEC v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003) (“It is a well-established canon of statutory interpretation that the use of different words or terms within a statute demonstrates that Congress intended to convey a different meaning for those words.”). The phrase “communication by radio” is used more expansively: it conjures an image of all communications using radio *waves* or a radio *device*. *See, e.g.*, 18 U.S.C. § 2510(16)(E) (describing radio communication that “is a two-way voice communication by radio transmitted on a frequency “not exclusively allocated to broadcast auxiliary services.”).

When read in context, the phrase “radio communication” tends to refer more narrowly to

broadcast radio technologies rather than to the radio waves by which the communication is made. “Radio communication” is typically surrounded by words that evoke traditional radio technologies whenever it is used in the Act. *See Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995) (“[A] word is known by the company it keeps (the doctrine of *noscitur a sociis*). This rule we rely upon to avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving ‘unintended breadth to the Acts of Congress.’”). For example, 18 U.S.C. § 2511(2)(g)(ii), *inter alia*, exempts from liability the interception of “any radio communication which is transmitted ... by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services.” These are traditional audio broadcasts that fit squarely within the ordinary meaning of “radio communication.” The phrase “radio communication” is used five times in the Wiretap Act. *See* 18 U.S.C. § 2510(16), 18 U.S.C. § 2511(2)(g)(ii), 18 U.S.C. § 2511(2)(g)(v), 18 U.S.C. § 2511(5)(a)(i)(B), 18 U.S.C. § 2520(c)(1). Defining the term as a predominantly auditory broadcast would not distort the meaning of any of these provisions or otherwise lead to incoherence or inconsistency.

On the other hand, the Wiretap Act uses “communication by radio” to refer more broadly to any communication transmitted by radio wave. *See* 18 U.S.C. § 2510(12) (defining “electronic communication” to include any communication “transmitted in whole or in part by ... radio”); 18 U.S.C. § 2511(1)(b)(ii) (prohibiting the use of a “device to intercept any oral communication” if the “device transmits communications by radio”); 18 U.S.C. § 2511(2)(b) (authorizing FCC employees, in carrying out their

official duties, “to intercept ... [an] oral communication transmitted by radio”). Congress’s decision to use both of these phrases implies that it intended to distinguish “radio communication” from “communications by radio.” See *McCarthy*, 322 F.3d at 656. Ideally, Congress would have supplied definitions to make the distinction between these terms more apparent. Nevertheless, by relying on their ordinary meaning and evaluating how they are used in context, we conclude that the former refers more narrowly to a predominantly auditory broadcast while only the latter encompasses other communications made using radio waves.

The way the phrase “radio communication” is used in 18 U.S.C. § 2511(2)(g)(ii) is particularly relevant in defining the term because that provision specifically exempts from liability the interception of certain kinds of radio communication. The provision is not directly at issue here because—as Google acknowledges—Google’s conduct is not encompassed by any of the § 2511(2)(g)(ii) exemptions, hence its reliance on § 2511(2)(g)(i). But it is instructive to understand the types of communication exempted by § 2511(2)(g)(ii) since the phrase “radio communication” is “known by the company it keeps,” *Gustafson*, 513 U.S. at 575. The exemptions include, *inter alia*, radio communications transmitted “by any station for the use of the general public,” 18 U.S.C. § 2511(2)(g)(ii)(I), “by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services,” 18 U.S.C. § 2511(2)(g)(ii)(III), and “by any marine or aeronautical communications system,” 18 U.S.C. § 2511(2)(g)(ii)(IV). Other than the fact that they all use the radio spectrum, these radio communications have little in common with a home Wi-



Fi network. Of course § 2511(2)(g)(i) exempts radio communications that are “readily accessible to the general public” even if they are not specifically set out in § 2511(2)(g)(ii). But it would be odd for Congress to take pains to identify particular kinds of radio communications that should be exempt in § 2511(2)(g)(ii) only to exempt broad swaths of dissimilar communications, such as data transmitted over a Wi-Fi network, under the auspices of § 2511(2)(g)(i). It is more sensible to read the general exemption in § 2511(2)(g)(i)—insofar as it applies to “radio communication” rather than other kinds of “electronic communication”—in light of the specific exemptions in § 2511(2)(g)(ii).

Relatedly, giving “radio communication” its ordinary meaning as a predominantly auditory broadcast also avoids producing absurd results that are inconsistent with the statutory scheme. *See Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982) (“[I]nterpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available.”); *Ariz. State Bd. for Charter Schools v. U.S. Dep’t of Educ.*, 464 F.3d 1003, 1008 (9th Cir. 2006) (“[W]ell-accepted rules of statutory construction caution us that ‘statutory interpretations which would produce absurd results are to be avoided.’ When a natural reading of the statutes leads to a rational, common-sense result, an alteration of meaning is not only unnecessary, but also extrajudicial.”). Under the expansive definition of “radio communication” proposed by Google, the protections afforded by the Wiretap Act to many online communications would turn on whether the *recipient* of those communications decided to secure her wireless network. A “radio communication” is

“readily accessible to the general public” and, therefore, exempt from Wiretap Act liability if it is not scrambled or encrypted. 18 U.S.C. § 2510(16). Consider an email attachment containing sensitive personal information sent from a secure Wi-Fi network to a doctor, lawyer, accountant, priest, or spouse. A company like Google that intercepts the contents of that email from the encrypted home network has, quite understandably, violated the Wiretap Act. But the sender of the email is in no position to ensure that the recipient—be it a doctor, lawyer, accountant, priest, or spouse—has taken care to encrypt her own Wi-Fi network. Google, or anyone else, could park outside of the recipient’s home or office with a packet sniffer while she downloaded the attachment and intercept its contents because the sender’s “radio communication” is “readily accessible to the general public” solely by virtue of the fact that the *recipient’s* Wi-Fi network is not encrypted. Surely Congress did not intend to condone such an intrusive and unwarranted invasion of privacy when it enacted the Wiretap Act “to protect against the unauthorized interception of electronic communications.” S. Rep. No. 99-541 (1986), at 1; *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) (“The legislative history of the [Wiretap Act] suggests that Congress wanted to protect electronic communications that are configured to be private, such as email.”); *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003) (“The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.”).

The definition of “readily accessible to the general public” in § 2510(16) is limited to “radio communication,” and does not encompass all “electronic communication.” Congress’s decision to carve out

“radio communication” for less protection than some other types of “electronic communication” makes sense if “radio communication” is given its ordinary meaning. Traditional radio services can be easily and mistakenly intercepted by hobbyists. *See* 132 Cong. Rec. S7987-04 (1986) (“In order to address radio hobbyists’ concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful.”). But “radio hobbyists” do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks. Lending “radio communication” a broad definition that encompasses data transmitted on Wi-Fi networks would obliterate Congress’s compromise and create absurd applications of the exemption for intercepting unencrypted radio communications. For example, § 2511(2)(g)(ii)(II) exempts from liability, *inter alia*, the act of intercepting “any radio communication which is transmitted ... by any governmental, law enforcement ... or public safety communications system, including police and fire, readily accessible to the general public.” This provision reinforces the work performed by § 2511(2)(g)(i), which already exempts a “radio communication” that is “readily accessible to the general public.” Congress’s decision to ensure that these communications were exempt makes sense if “radio communication” encompasses only predominantly auditory broadcasts since these transmissions can be picked up by widely available police scanners. But if “radio communication” includes data transmitted over Wi-Fi networks, then § 2511(2)(g)(ii)(II) also underscores that liability should not attach to intercepting data from an unencrypted Wi-Fi network operated by, say, a police department or government agency. It seems doubtful that Congress

wanted to emphasize that Google or anyone else could park outside of a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity.

Next, Google strenuously argues that the rest of the Wiretap Act supports its position that “radio communication” in 18 U.S.C. § 2510(16) means “any information transmitted using radio waves.” Google leans heavily on § 2510(16)(D) and the accompanying legislative history, which together suggest that cellular telephone and paging systems are a form of “radio communication.” If cell phone and paging systems are a type of “radio communication,” Google argues, it must be the case that Congress intended that the phrase include Wi-Fi networks and the rest of the radio spectrum because these technologies differ from paradigmatic radio communications like AM/FM, CB, and shortwave transmissions. But cell phone communications were not dissimilar from CB, shortwave, or other two-way forms of traditional radio broadcasts when § 2510(16)(D) was added to the Wiretap Act in 1986 as part of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848. When Congress enacted § 2510(16)(D), cell phones were still called “cellular radiotelephones.” *See* H.R. Rep. No. 99-647, at 20 (1986). As with other audio broadcasts, cellular conversations were often inadvertently picked up by radio hobbyists “scanning radio frequencies in order to receive public communications.” S. Rep. No. 99-541, at 3560 (1986); *see also* H.R. Rep. No. 99-647, at 20 (“Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls”). The fact that technology has evolved and

cellular communications are no longer as similar to CB broadcasts as they once were does not require us to read “radio communication” to include all communications made using radio waves. Rather, the historical context surrounding Congress’s protection of cellular conversations as a form of a “radio communication” is consistent with the commonsense definition of the term because, at the time of the enactment of the definition in 1986, cellular conversations could have reasonably been construed as analogous to a form of two-way radio.<sup>6</sup> Assuming, *arguendo*, that the phrase “radio communication” covers cell phone transmissions as they existed in 1986 does not inevitably lead to the conclusion that it also encompasses transmissions that are plainly not predominantly auditory broadcasts, such as payload data transmitted over a Wi-Fi network.

Google also looks beyond the Wiretap Act in an effort to fit its expansive definition of “radio communication” into the statutory scheme. It points

---

<sup>6</sup> With modern advances in cellular technology, it is less clear how cell phones would fit within the statutory scheme today. We need not resolve this question here. Whether cell phone transmissions are an example of a “radio communication” is relevant to defining the phrase, but it is not a precursor to observing that a “radio communication” is ordinarily a predominantly auditory broadcast or to holding that payload data transmitted over a Wi-Fi network is not a “radio communication.” We previously held that cell phone communications are “wire communications” for purposes of the Wiretap Act, but we did not address whether they are an example of a “radio communication.” See *In re U.S. for an Order Authorizing Roving Interception of Oral Commc’ns*, 349 F.3d 1132, 1138 n.12 (9th Cir. 2003) (“Despite the apparent wireless nature of cellular phones, communications using cellular phones are considered wire communications under the statute, because cellular telephones use wire and cable connections when connecting calls.”).

out that the Communications Act expressly defines the phrases “radio communication” and “communication by radio” broadly to include “the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds.” 47 U.S.C. § 153(40). But when Congress wanted to borrow a definition from the Communications Act to apply to the Wiretap Act, it expressly said so. *See* 18 U.S.C. § 2510(1) (giving the phrase “communication common carrier” the meaning that it has “in section 3 of the Communications Act”). Here, Congress refrained from incorporating the definition of “radio communication” used in the Communications Act. And, as previously discussed, the Wiretap Act uses the phrases “radio communication” and “communication by radio” differently, indicating that Congress did not intend to import the Communications Act’s definition, which treats them as synonyms. *See* 47 U.S.C. § 153(40). Furthermore, the Communication Act’s definition of “radio communication” encompasses technologies like television by including “the transmission by radio of ... pictures ... of all kinds,” 47 U.S.C. § 153(40), while the Wiretap Act sometimes distinguishes them. *See, e.g.*, 18 U.S.C. § 2520(c)(1) (providing specified penalties when the “violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on [frequencies specified by regulation]”). Separate references to television-related communications would be redundant when paired with the phrase “radio communication” if we were to assume that the Communication Act’s definition applied to the Wiretap Act. Importantly, the presumption that a definition set out in one part of the code is intended to govern

another is hardly unyielding in the face of such contradictory evidence. *See, e.g., General Dynamics Land Sys., Inc. v. Cline*, 540 U.S. 581, 595 (2004) (holding that the word “age” carries a different meaning in different sections of the ADEA); *Robinson v. Shell Oil*, 519 U.S. 337, 343 (1997) (holding that the term “employees” carries a different meaning in different sections of Title VII).

Google also leans heavily on a series of amendments to 18 U.S.C. § 2510(16) to argue that Congress impliedly gave the phrase “radio communication” a meaning other than the ordinary one that we adopt here. In 1990, Senator Patrick Leahy commissioned a task force to study the effect of new technologies, including the precursors to wireless networking, on the statutory scheme created in 1986 by the Electronic Communications Privacy Act. *See* S. Hrg. 103-1022, at 179 (1994). In its report, the task force indicated it was concerned that communications by “wireless modems’ which can transmit data between computers ... will not be protected unless the user goes to the expense of full data encryption.” *Id.* at 183. The section of the report on “Wireless Data Communications” concluded that “[t]he task force recommends appropriate amendments to legally protect digital communications of this type from unauthorized interception.” *Id.* In short, the task force was of the opinion that the version of 18 U.S.C. § 2510(16) enacted in 1986 did not adequately protect unencrypted “wireless data communications.” The task force must have implicitly decided that “wireless data communications” were a “radio communication” because otherwise it would not have been concerned with § 2510(16), which only applies to “radio communication.” *See id.*

In 1994, Congress amended § 2510(16) to add a new category of communication—which it called an “electronic communication”—that it deemed to be a “radio communication” that was not “readily accessible to the general public.” In relevant part, the statute provided that “‘readily accessible to the general public’ means, with respect to a radio communication, that such communication is not ... (F) an electronic communication.” 18 U.S.C. § 2510(16) (1994). Google claims that Congress added § 2510(16)(F) in 1994 in order to protect from interception new technologies that transmitted data using radio frequencies, including the contemporary versions of wireless networks. There is some support for this proposition in the congressional record. *See* H.R. Rep. No. 103-827, at 18 (1994) (explaining that the bill “[e]xtends privacy protections of the Electronic Communications Privacy Act to cordless phones and certain data communications transmitted by radio”).

The significance of all of this is that Congress repealed 18 U.S.C. § 2510(16)(F) in 1996. Google attempts to draw a series of inferences from the 1994 and 1996 amendments: The 1994 Congress thought that data transmissions across the wireless networks of the day were a type of “radio communication.” Otherwise, Congress would not have needed to amend § 2510(16) in order to shield them from interception given that the provision only applies to “radio communication.” By deleting § 2510(16)(F), the 1996 Congress removed the sole protection for unencrypted data transmissions over wireless networks by returning § 2510(16) to its pre-amendment form. From Google’s perspective, the upshot of this historical narrative is that payload data transmitted over an unencrypted Wi-Fi network is a “radio communication”



that is “readily accessible to the general public” before the 1994 amendment and, crucially, after the 1996 repeal.

This evidence of congressional action and inaction is far more equivocal than Google acknowledges. First, the task force’s report does not control what the phrase “radio communication” meant to Congress when it enacted § 2510(16) in 1986. The task force’s report suggests that it thought that the “wireless data communication” technology that existed in 1991 entailed “radio communication” as the phrase is used in § 2510(16). But the task force’s opinion on questions of statutory interpretation has no independent authority; it is not charged with divining congressional intent. The task force’s recommendation informs us that in 1991 a group of fifteen individuals thought that early versions of wireless networks involved “radio communication” under the statute. Their opinion is not indicative of what Congress intended when it included the phrase in the Wiretap Act. It may be considered evidence of the phrase’s ordinary meaning. But it does not outweigh the more substantial evidence, discussed at length above, indicating that the ordinary meaning of “radio communication” excludes data transmitted over a Wi-Fi network.

Second, Congress’s decision to add § 2510(16)(F) in 1994 does not prove that it thought data transmitted over a Wi-Fi network constituted a “radio communication.” The 1994 Congress was certainly concerned about ensuring that “certain data communications transmitted by radio” were protected from interception. But that does not necessarily mean that it was of the view that such communications were a “radio communication” under § 2510(16). Congress might have been forestalling the possibility that

evolving technologies would be construed as radio communications, contrary to the ordinary meaning of the phrase.

Third, and perhaps most importantly, there is no reliable indication of what the 1996 Congress intended to accomplish by repealing § 2510(16)(F). Google mines the 1991 task force report and the 1994 congressional record, but it cannot close the loop on its argument because the 1996 Congress did not leave behind the snippets of enactment history that are essential to Google’s narrative. Consider two possible rationales for the 1996 repeal of § 2510(16)(F): first, Congress might have deleted the provision because it found it redundant. That is, Congress might have thought that data transmitted over a radio frequency was not a “radio communication,” which would render the additional protection for such communications offered by § 2510(16)(F) unnecessary.

Alternatively, Congress might have (correctly) determined that § 2510(16)(F) made the statute incoherent. Recall that the short-lived provision provided that “‘readily accessible to the general public’ means, with respect to a radio communication, that such communication is not ... (F) an electronic communication.” 18 U.S.C. § 2510(16)(F) (1994). The phrase “electronic communication” has been broadly defined since the Electronic Communications Privacy Act of 1986. In 1994, when § 2510(16)(F) was added, the Wiretap Act provided—as it still does today—that “‘electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce.” 18 U.S.C. § 2510(12). As Google stresses

in its briefs, and the statute plainly states, “radio communication” is a subset of “electronic communication.” Yet § 2510(16)(F) conveyed that a “radio communication” was not “readily accessible to the general public” if it was an “electronic communication,” which incoherently implies that the latter was a subset of the former. The repeal of § 2510(16)(F) could, therefore, have been a housekeeping matter designed to resolve this internal tension without affecting the protection afforded “electronic communications, including data” that the 1994 Congress sought to protect.

Neither of these entirely plausible explanations for the amendment and repeal are consistent with Google’s assumption that the pre-1994 conception of “radio communication” included data transmitted over a Wi-Fi network and the 1996 repeal of § 2510(16)(F) sought to restore that conception. The point is that we do not know why the 1996 Congress deleted § 2510(16)(F). We choose to rely on the ordinary meaning of the phrase “radio communication” rather than follow a trail of enactment history that culminates in silence and then speculate as to Congress’s unexpressed intent.

Finally, Google’s fall back position is that the rule of lenity dictates that we accept its proposed definition of “radio communication.” Although this is a civil suit, the Wiretap Act also carries criminal penalties so Google’s reliance on the rule of lenity is not unfounded. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (“Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies.”). But we do not resort to the rule of lenity every time a difficult question of statutory interpretation arises. Rather, “the rule of lenity only applies if, after

considering text, structure, history, and purpose, there remains a ‘grievous ambiguity or uncertainty in the statute.’” *Barber v. Thomas*, 130 S. Ct. 2499, 2508 (2010) (citations omitted); *see also Smith v. United States*, 508 U.S. 223, 239 (1993) (“The mere possibility of articulating a narrower construction [ ] does not make the rule of lenity applicable. Instead, that venerable rule is reserved for cases where, ‘[a]fter “seizing every thing from which aid can be derived,” the Court is ‘left with an ambiguous statute.’”) (citations omitted). Here, the traditional tools of statutory interpretation are sufficient. The ordinary meaning of “radio communication” is consistent with the structure of the Act and avoids absurd results without running afoul of any clearly expressed congressional intent. We need not resort to the rule of lenity where, as here, the ambiguity can be fairly resolved.

#### IV. CONCLUSION

For the foregoing reasons, we agree with the district court that data transmitted over a Wi-Fi network is not a “radio communication” under 18 U.S.C. § 2510(16).

**AFFIRMED.**

**APPENDIX B**

UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

---

No. 11-17483  
D.C. No. 5:10-md-02184-JW

---

BENJAMIN JOFFE; LILLA MARIGZA; RICK BENITTI;  
BERTHA DAVIS; JASON TAYLOR; ERIC MYHRE; JOHN E.  
REDSTONE; MATTHEW BERLAGE; PATRICK KEYES;  
KARL H. SCHULZ; JAMES FAIRBANKS; AARON LINSKY;  
DEAN M. BASTILLA; VICKI VAN VALIN; JEFFREY  
COLMAN; RUSSELL CARTER; STEPHANIE CARTER;  
JENNIFER LOCSIN,  
*Plaintiffs-Appellees,*

*v.*

GOOGLE, INC.,  
*Defendant-Appellant.*

---

Appeal from the United States District Court  
for the Northern District of California  
James Ware, District Judge, Presiding

---

Argued and Submitted  
June 10, 2013—San Francisco, California  
Filed September 10, 2013

---

**OPINION**

---

Before: A. Wallace Tashima and Jay S. Bybee, Circuit Judges, and William H. Stafford, Senior District Judge.\*

Opinion by Judge Bybee

\* \* \*

## OPINION

BYBEE, Circuit Judge:

In the course of capturing its Street View photographs, Google collected data from unencrypted Wi-Fi networks. Google publicly apologized, but plaintiffs brought suit under federal and state law, including the Wiretap Act, 18 U.S.C. § 2511. Google argues that its data collection did not violate the Act because data transmitted over a Wi-Fi network is an “electronic communication” that is “readily accessible to the general public” and exempt under the Act. 18 U.S.C. § 2511(2)(g)(i). The district court rejected Google’s argument. *In re Google Inc. St. View Elec. Comm’n Litig.*, 794 F. Supp. 2d 1067, 1073–84 (N.D. Cal. 2011). We affirm.

### I. BACKGROUND

#### A. *Facts and History*

Google launched its Street View feature in the United States in 2007 to complement its Google Maps service by providing users with panoramic, street-level photographs. Street View photographs are captured by cameras mounted on vehicles owned by Google that drive on public roads and photograph their surroundings. Between 2007 and 2010, Google also

---

\* The Honorable William H. Stafford, Jr., Senior District Judge for the U.S. District Court for the Northern District of Florida, sitting by designation.

equipped its Street View cars with Wi-Fi antennas and software that collected data transmitted by Wi-Fi networks in nearby homes and businesses. The equipment attached to Google's Street View cars recorded basic information about these Wi-Fi networks, including the network's name (SSID), the unique number assigned to the router transmitting the wireless signal (MAC address), the signal strength, and whether the network was encrypted. Gathering this basic data about the Wi-Fi networks used in homes and businesses enables companies such as Google to provide enhanced "location-based" services, such as those that allow mobile phone users to find nearby restaurants and attractions or receive driving directions.

But the antennas and software installed in Google's Street View cars collected more than just the basic identifying information transmitted by Wi-Fi networks. They also gathered and stored "payload data" that was sent and received over unencrypted Wi-Fi connections at the moment that a Street View car was driving by.<sup>1</sup> Payload data includes everything transmitted by a device connected to a Wi-Fi network, such as personal emails, usernames, passwords, videos, and documents.

Google acknowledged in May 2010 that its Street View vehicles had been collecting fragments of payload data from unencrypted Wi-Fi networks. The company publicly apologized, grounded its vehicles, and rendered inaccessible the personal data that had been acquired. In total, Google's Street View cars collected about 600 gigabytes of data transmitted over Wi-Fi networks in more than 30 countries.

---

<sup>1</sup> Google may have also used its software to capture encrypted data, but the plaintiffs have conceded that their wireless networks were unencrypted.

Several putative class-action lawsuits were filed shortly after Google's announcement, and, in August 2010, the cases were transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California. In November, 2010, Plaintiffs-Appellees (collectively "Joffe") filed a consolidated complaint, asserting claims against Google under the federal Wiretap Act, 18 U.S.C. § 2511; California Business and Professional Code § 17200; and various state wiretap statutes. Joffe seeks to represent a class comprised of all persons whose electronic communications were intercepted by Google Street View vehicles since May 25, 2007.

Google moved to dismiss Joffe's consolidated complaint. The district court declined to grant Google's motion to dismiss Joffe's federal Wiretap Act claims.<sup>2</sup> *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d at 1084. On Google's request, the court certified its ruling for interlocutory appeal under 28 U.S.C. § 1292(b) because the district court resolved a novel question of statutory interpretation. We granted Google's petition, and we have jurisdiction under 28 U.S.C. § 1292(b).

#### B. *District Court's Decision*

Google maintained before the district court that it should have dismissed Joffe's Wiretap Act claims because data transmitted over unencrypted Wi-Fi networks falls under the statutory exemption that makes it lawful to intercept "electronic communications" that are "readily accessible to the

---

<sup>2</sup> The district court granted Google's motion to dismiss Joffe's claims under California law and other state wiretap statutes. *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d at 1085-86. These claims are not at issue here.



general public.” 18 U.S.C. § 2511(2)(g)(i). The question was whether payload data transmitted on an unencrypted Wi-Fi network is “readily accessible to the general public,” such that the § 2511(2)(g)(i) exemption applies to Google’s conduct.

To answer this question, the district court first looked to the definitions supplied by the Act. *In re Google Inc. St. View Elec. Commc’n Litig.*, 794 F. Supp. 2d at 1075–76. The statute provides in relevant part that “‘readily accessible to the general public’ means, with respect to a radio communication, that such communication is not ... (A) scrambled or encrypted.” 18 U.S.C. § 2510(16). An unencrypted *radio communication* is, therefore, “readily accessible to the general public.” In short, intercepting an unencrypted *radio communication* does not give rise to liability under the Wiretap Act because of the combination of the § 2511(2)(g)(i) exemption and the § 2510(16) definition.

The district court then considered whether data transmitted over a Wi-Fi network is a “radio communication” because the phrase is not defined by the Act. *In re Google Inc. St. View Elec. Commc’n Litig.*, 794 F. Supp. 2d at 1076–81. The court reasoned that “radio communication” encompasses only “traditional radio services,” and not other technologies that also transmit data using radio waves, such as cellular phones and Wi-Fi networks.<sup>3</sup> *Id.* at 1079–83. Since Wi-Fi networks are not a “radio communication,” the definition of “readily accessible to the general public” provided by § 2510(16) does not apply because

---

<sup>3</sup> It is less clear whether the district court’s definition also excludes television broadcasts. Joffe argued at oral argument that television broadcasts are “traditional radio services.”

the definition is expressly limited to electronic communications that are radio communications.

Finally, the court addressed whether data transmitted over unencrypted Wi-Fi networks is nevertheless an “electronic communication” that is “readily accessible to the general public” under § 2511(2)(g)(i). *Id.* at 1082–84. Although the court determined that Wi-Fi networks do not involve a “radio communication” under § 2510(16) and are therefore not “readily accessible to the general public” by virtue of the definition of the phrase, it still had to resolve whether they are “readily accessible to the general public” as the phrase is ordinarily understood because the statute does not define the phrase as it applies to an “electronic communication” that is not a “radio communication.” The court determined that data transmitted over an unencrypted Wi-Fi network is not “readily accessible to the general public.” *Id.* at 1082–83. As a result, the § 2511(2)(g)(i) exemption does not apply to Google’s conduct. The court accordingly declined to grant Google’s motion to dismiss Joffe’s Wiretap Act claims. *Id.* at 1084.

## II. OVERVIEW OF THE WIRETAP ACT

The Wiretap Act imposes liability on a person who “intentionally intercepts ... any wire, oral, or electronic communication,” 18 U.S.C. § 2511(1)(a), subject to a number of exemptions. *See* 18 U.S.C. § 2511(2)(a)–(h). There are two exemptions that are relevant to our purposes. First, the Wiretap Act exempts intercepting “an electronic communication made through an electronic communication system” if the system is configured so that it is “readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i). “Electronic communication” includes communication by radio, 18

U.S.C. § 2510(12), and “readily accessible to the general public” means, with respect to a radio communication” that the communication is “not ... scrambled or encrypted,” 18 U.S.C. § 2510(16)(A). Second, the Act exempts intercepting “radio communication” by “any station for the use of the general public;” by certain governmental communication systems “readily accessible to the general public,” including police, fire, and civil defense agencies; by a station operating on an authorized frequency for “amateur, citizens band, or general mobile radio services;” or by a marine or aeronautical communications system. 18 U.S.C. § 2511(2)(g)(ii)(I)–(IV).

Google only argues, as it did before the district court, that it is exempt from liability under the Act because data transmitted over a Wi-Fi network is an “electronic communication ... readily accessible to the general public” under § 2511(2)(g)(i). It concedes that it does not qualify for any of the exemptions for specific types of “radio communication” under § 2511(2)(g)(ii). Joffe, however, argues that if data transmitted over a Wi-Fi network is not exempt as a “radio communication” under § 2511(2)(g)(ii), it cannot be exempt as a radio communication under the broader exemption for “electronic communication” in § 2511(2)(g)(i). This argument has some force, and we wish to address it before we consider Google’s claims.

Joffe contends that the definition of “readily accessible to the general public” in § 2510(16) does not apply to the § 2511(2)(g)(i) exemption. Instead, Joffe argues, the § 2510(16) definition applies exclusively to § 2511(2)(g)(ii)(II), which exempts specifically enumerated types of “radio communication” when they are “readily accessible to the general public.” We

ultimately reject Joffe’s alternative reading of the statute, although—as we will explain—we find § 2511(2)(g)(ii) useful as a lexicographical aid to understanding the phrase “radio communication.”

As noted, § 2510(16) defines “readily accessible to the general public” solely with respect to a “radio communication,” and not with respect to other types of “electronic communication.” Although § 2511(2)(g)(i) does not use the words “radio communication,” the statute nevertheless directs us to apply the § 2510(16) definition to the § 2511(2)(g)(i) exemption. First, “radio communication” is a subset of “electronic communication.” See 18 U.S.C. § 2510(12) (providing that, subject to certain exceptions, “‘electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, *radio*, electromagnetic, photoelectronic or photooptical system”) (emphasis added). Second, the statute directs us to apply § 2510(16) to the entire chapter. The definitions in 18 U.S.C. § 2510 are prefaced with the phrase, “As used in this chapter.” We cannot disregard this command by holding that the definition of “‘readily accessible to the general public’ [ ] with respect to a radio communication” applies to § 2511(2)(g)(ii), but not § 2511(2)(g)(i).

Admittedly, following the plain language of the statute creates some tension with § 2511(2)(g)(ii)(II), which provides an exemption for intercepting “any radio communication which is transmitted ... by any governmental, law enforcement, civil defense, private land mobile, or public communications system, including police and fire, readily accessible to the general public.” Under our reading of the statute—which is the same reading adopted by the district court,

Google, and Joffe in his lead argument—§ 2511(2)(g)(i) exempts all electronic communications (including radio communications) that are “readily accessible to the general public” as the phrase is defined in § 2510(16). This reading likely renders § 2511(2)(g)(ii)(II) superfluous. As discussed, that section exempts specific kinds of radio communications that are “readily accessible to the general public,” such as those transmitted by a law enforcement communications system. But this exemption is unnecessary when § 2511(2)(g)(i) already exempts all radio communications that are “readily accessible to the general public.”

Although our reading may render § 2511(2)(g)(ii)(II) superfluous or at least redundant, we understand that Congress “sometimes drafts provisions that appear duplicative of others—simply in Macbeth’s words, ‘to make assurance double sure.’ That is, Congress means to clarify what might be doubtful—that the mentioned item is covered.” *Shook v. D.C. Fin. Responsibility & Mgmt. Assistance Auth.*, 132 F.3d 775, 782 (D.C. Cir. 1998). This interpretation is especially plausible given that Congress was concerned that radio hobbyists not face liability for intercepting readily accessible broadcasts, such as those covered by § 2511(2)(g)(ii)(II), which can be picked up by a police scanner. *See* 132 Cong. Rec. S7987-04 (1986) (“In order to address radio hobbyists’ concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful.”).

In short, we agree with Google that the definition of “readily accessible to the general public” in § 2510(16) applies to the § 2511(2)(g)(i) exemption when the communication in question is a “radio communication.” With that understanding, we now

turn to whether data transmitted over a Wi-Fi network is a “radio communication” exempt from the Wiretap Act as an “electronic communication” under § 2511(2)(g)(i).

### III. ANALYSIS

In support of its position that it is exempt under § 2511(2)(g)(i), Google offers two arguments. First, it contends that data transmitted over a Wi-Fi network is an electronic “radio communication” and that the Act exempts such communications by defining them as “readily accessible to the general public,” 18 U.S.C. § 2511(2)(g)(i), so long as “such communication is not ... scrambled or encrypted,” 18 U.S.C. § 2510(16)(A). Second, Google contends that even if data transmitted over an unencrypted Wi-Fi network is not a “radio communication,” it is still an “electronic communication ... readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i).

We reject both claims.<sup>4</sup> We hold that the phrase “radio communication” in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi-Fi network. As a consequence, the definition of “readily accessible to the general public [ ] with respect to a radio communication” set forth in § 2510(16) does not apply to the exemption for an “electronic communication” that is

---

<sup>4</sup>This case raises a question of statutory interpretation, which we review de novo. *Phoenix Mem'l Hosp. v. Sebelius*, 622 F.3d 1219, 1224 (9th Cir. 2010). We begin by “determin[ing] whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case.” *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 450 (2002). We must assume that “the ordinary meaning of that language accurately expresses the legislative purpose [of Congress].” *Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985).

“readily accessible to the general public” under 18 U.S.C. § 2511(2)(g)(i). We further hold that payload data transmitted over an unencrypted Wi-Fi network is not “readily accessible to the general public” under the ordinary meaning of the phrase as it is used in § 2511(2)(g)(i).

A. *Data Transmitted over a Wi-Fi Network Is Not a “Radio Communication” under the Wiretap Act.*

We turn first to the question of whether data transmitted over a Wi-Fi network is a “radio communication” as that term is used in 18 U.S.C. § 2510(16). If data transmitted over a Wi-Fi network is a radio communication, then any radio communication that is not scrambled or encrypted is considered “readily accessible to the general public,” and is exempt from liability under the Wiretap Act. 18 U.S.C. § 2511(2)(g)(i).

1. The ordinary meaning of “radio communication” does not include data transmitted over a Wi-Fi network

The Wiretap Act does not define the phrase “radio communication” so we must give the term its ordinary meaning. *See Hamilton v. Lanning*, 130 S. Ct. 2464, 2471 (2010) (“When terms used in a statute are undefined, we give them their ordinary meaning.”); *United States v. Daas*, 198 F.3d 1167, 1174 (9th Cir. 1999) (“If the statute uses a term which it does not define, the court gives that term its ordinary meaning.”).

According to Google, radio communication “refers to any information transmitted using radio waves, *i.e.*, the radio frequency portion of the electromagnetic spectrum.” Appellant’s Br. at 28. The radio frequency

portion of the spectrum is “the part of the spectrum where electromagnetic waves have frequencies in the range of about 3 kilohertz to 300 gigahertz.” *Id.* at 27.

Google’s technical definition does not conform with the common understanding held contemporaneous with the enacting Congress. *See United States v. Iverson*, 162 F.3d 1015, 1022 (9th Cir. 1998) (“When a statute does not define a term, we generally interpret that term by employing the *ordinary, contemporary, and common* meaning of the words that Congress used”) (emphasis added). The radio frequency portion of the electromagnetic spectrum covers not only Wi-Fi transmissions, but also television broadcasts, Bluetooth devices, cordless and cellular phones, garage door openers, avalanche beacons, and wildlife tracking collars. *See* Fed. Comm’n Comm’n, *Encyclopedia – FM Broadcast Station Classes and Service Contours*, available at <http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf> (last visited Aug. 13, 2013). One would not ordinarily consider, say, television a form of “radio communication.” Not surprisingly, Congress has not typically assumed that the term “radio” encompasses the term “television.” *See, e.g.*, 18 U.S.C. § 1343 (imposing liability for “[f]raud by wire, radio, or television”) (emphasis added); 18 U.S.C. § 2101 (imposing liability for inciting a riot by means of “mail, telegraph, radio, or television”) (emphasis added); 7 U.S.C. § 2156 (defining an “instrumentality of interstate commerce” as “any written, wire, radio, television or other form of communication); *see also FCC v. Nat’l Citizens Comm. for Broad.*, 436 U.S. 775, 815 (1978) (noting that “radio and television stations are given different weight,” under the regulations at issue, and describing



regulations governing “a radio *or* television broadcast station”) (emphasis added).

The Wiretap Act itself does not assume that the phrase “radio communication” encompasses technologies like satellite television that are outside the scope of the phrase as it is ordinarily defined. For example, the statute’s damages provision sets out specified penalties when the “violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted *or* if the communication is a radio communication that is transmitted on [frequencies specified by regulation].” 18 U.S.C. § 2520(c)(1) (emphasis added). Congress described separately the act of “viewing [ ] a private satellite video communication” even though such communication is transmitted on a radio frequency and would fall within Google’s proposed definition of “radio communication.” Taken together, these disparate provisions offer evidence that Congress does not use “radio” or “radio communication” to reference all of the myriad forms of communication that use the radio spectrum. Rather, it uses “radio” to refer to traditional radio technologies, and then separately describes other modes of communication that are not ordinarily thought of as radio, but that nevertheless use the radio spectrum.

Google’s proposed definition is in tension with how Congress—and virtually everyone else—uses the phrase. In common parlance, watching a television show does not entail “radio communication.” Nor does sending an email or viewing a bank statement while connected to a Wi-Fi network. There is no indication that the Wiretap Act carries a buried implication that the phrase ought to be given a broader definition than the one that is commonly understood. *See Mohamad v.*

*Palestinian Auth.*, 132 S. Ct. 1702, 1707 (2012) (favoring a definition that matches “how we use the word in everyday parlance” and observing that “Congress remains free, as always, to give the word a broader or different meaning. But before we will assume it has done so, there must be *some* indication Congress intended such a result”).

Importantly, Congress provided definitions for many other similar terms in the Wiretap Act, but refrained from providing a technical definition of “radio communication” that would have altered the notion that it should carry its common, ordinary meaning. *See, e.g.*, 18 U.S.C. § 2510(1) (defining “wire communication”); 18 U.S.C. § 2510(12) (defining “electronic communication”); 18 U.S.C. § 2510(15) (defining “electronic communication service”); 18 U.S.C. § 2510(17) (defining “electronic storage”). As Google writes in its brief, “[t]he fact that the Wiretap Act provides specialized definitions for certain compound terms—but not for ‘radio communication’—is powerful evidence that the undefined term was not similarly intended [to] be defined in a specialized or narrow way” but rather “according to its ordinary meaning.” Appellant’s Br. at 29. We agree and, accordingly, we reject Google’s proposed definition of “radio communication” in favor of one that better reflects the phrase’s ordinary meaning.

2. A “radio communication” is a predominantly auditory broadcast, which excludes payload data transmitted over Wi-Fi networks

There are two telltale indicia of a “radio communication.” A radio communication is commonly understood to be (1) predominantly auditory, and (2) broadcast. Therefore, television—whether connected

via an indoor antenna or a satellite dish—is not radio, by virtue of its visual component. A land line phone does not broadcast, and, for that reason, is not radio. On the other hand, AM/FM, Citizens Band (CB), ‘walkie-talkie,’ and shortwave transmissions are predominantly auditory, are broadcast, and are, not coincidentally, typically referred to as “radio” in everyday parlance. Thus, we conclude that “radio communication” should carry its ordinary meaning: a predominantly auditory broadcast.<sup>5</sup>

The payload data transmitted over unencrypted Wi-Fi networks that was captured by Google included emails, usernames, passwords, images, and documents that cannot be classified as predominantly auditory. They therefore fall outside of the definition of a “radio communication” as the phrase is used in 18 U.S.C. § 2510(16).

---

<sup>5</sup> We need not reach the question of what exactly constitutes a “broadcast” because the Wi-Fi transmissions in question were not predominantly auditory. Whether cell phone calls—which are projected wirelessly over great distances—are broadcast would similarly be a close question.

We also need not fully consider the extent to which non-auditory transmissions may be included in a broadcast before that broadcast is no longer a radio broadcast. Modern FM radio stations, for example, commonly transmit small amounts of data denoting the artist and title of the song. But because such data is ancillary to the audio transmission, they likely do not remove the transmissions from the domain of a “radio communication” under the Act.

And, finally, we do not address how to classify a traditional radio broadcast delivered to a web-enabled device connected to a Wi-Fi network, such as a radio station streamed over the internet. Here, Google’s collection efforts were not limited to auditory transmissions.

3. Defining “radio communication” to include only predominantly auditory broadcasts is consistent with the rest of the Wiretap Act

Crucially, defining “radio communication” as a predominantly auditory broadcast yields a coherent and consistent Wiretap Act. Google’s overly broad definition does not. *See K Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988) (“In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole.”)

Throughout the Wiretap Act, Congress used the phrase “radio communication”—which is at issue here—and the similar phrase “communication by radio.” Even within the very provision that we are construing—18 U.S.C. § 2510(16)—Congress used both phrases. We must ascribe to each phrase its own meaning. *See SEC v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003) (“It is a well-established canon of statutory interpretation that the use of different words or terms within a statute demonstrates that Congress intended to convey a different meaning for those words.”). The phrase “communication by radio” is used more expansively: it conjures an image of all communications using radio *waves* or a radio *device*. *See, e.g.*, 18 U.S.C. § 2510(16)(E) (describing radio communication that “is a two-way voice communication by radio transmitted on a frequency “not exclusively allocated to broadcast auxiliary services.”).

When read in context, the phrase “radio communication” tends to refer more narrowly to broadcast radio technologies rather than to the radio waves by which the communication is made. “Radio communication” is typically surrounded by words that

evoke traditional radio technologies whenever it is used in the Act. *See Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995) (“[A] word is known by the company it keeps (the doctrine of *noscitur a sociis*). This rule we rely upon to avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving ‘unintended breadth to the Acts of Congress.’”). For example, 18 U.S.C. § 2511(2)(g)(ii), *inter alia*, exempts from liability the interception of “any radio communication which is transmitted ... by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services.” These are traditional audio broadcasts that fit squarely within the ordinary meaning of “radio communication.” The phrase “radio communication” is used five times in the Wiretap Act. *See* 18 U.S.C. § 2510(16), 18 U.S.C. § 2511(2)(g)(ii), 18 U.S.C. § 2511(2)(g)(v), 18 U.S.C. § 2511(5)(a)(i)(B), 18 U.S.C. § 2520(c)(1). Defining the term as a predominantly auditory broadcast would not distort the meaning of any of these provisions or otherwise lead to incoherence or inconsistency.

On the other hand, the Wiretap Act uses “communication by radio” to refer more broadly to any communication transmitted by radio wave. *See* 18 U.S.C. § 2510(12) (defining “electronic communication” to include any communication “transmitted in whole or in part by ... radio”); 18 U.S.C. § 2511(1)(b)(ii) (prohibiting the use of a “device to intercept any oral communication” if the “device transmits communications by radio”); 18 U.S.C. § 2511(2)(b) (authorizing FCC employees, in carrying out their official duties, “to intercept ... [an] oral communication transmitted by radio”). Congress’s decision to use both of these phrases implies that it intended to distinguish

“radio communication” from “communications by radio.” See *McCarthy*, 322 F.3d at 656. Ideally, Congress would have supplied definitions to make the distinction between these terms more apparent. Nevertheless, by relying on their ordinary meaning and evaluating how they are used in context, we conclude that the former refers more narrowly to a predominantly auditory broadcast while only the latter encompasses other communications made using radio waves.

The way the phrase “radio communication” is used in 18 U.S.C. § 2511(2)(g)(ii) is particularly relevant in defining the term because that provision specifically exempts from liability the interception of certain kinds of radio communication. The provision is not directly at issue here because—as Google acknowledges—Google’s conduct is not encompassed by any of the § 2511(2)(g)(ii) exemptions, hence its reliance on § 2511(2)(g)(i). But it is instructive to understand the types of communication exempted by § 2511(2)(g)(ii) since the phrase “radio communication” is “known by the company it keeps,” *Gustafson*, 513 U.S. at 575. The exemptions include, *inter alia*, radio communications transmitted “by any station for the use of the general public,” 18 U.S.C. § 2511(2)(g)(ii)(I), “by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services,” 18 U.S.C. § 2511(2)(g)(ii)(III), and “by any marine or aeronautical communications system,” 18 U.S.C. § 2511(2)(g)(ii)(IV). Other than the fact that they all use the radio spectrum, these radio communications have little in common with a home Wi-Fi network. Of course § 2511(2)(g)(i) exempts radio communications that are “readily accessible to the general public” even if they are not specifically set out in § 2511(2)(g)(ii). But it would be odd for Congress to

take pains to identify particular kinds of radio communications that should be exempt in § 2511(2)(g)(ii) only to exempt broad swaths of dissimilar communications, such as data transmitted over a Wi-Fi network, under the auspices of § 2511(2)(g)(i). It is more sensible to read the general exemption in § 2511(2)(g)(i)—insofar as it applies to “radio communication” rather than other kinds of “electronic communication”—in light of the specific exemptions in § 2511(2)(g)(ii).

Relatedly, giving “radio communication” its ordinary meaning as a predominantly auditory broadcast also avoids producing absurd results that are inconsistent with the statutory scheme. *See Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982) (“[I]nterpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available.”); *Ariz. State Bd. for Charter Schools v. U.S. Dep’t of Educ.*, 464 F.3d 1003, 1008 (9th Cir. 2006) (“[W]ell-accepted rules of statutory construction caution us that ‘statutory interpretations which would produce absurd results are to be avoided.’ When a natural reading of the statutes leads to a rational, common-sense result, an alteration of meaning is not only unnecessary, but also extrajudicial.”). Under the expansive definition of “radio communication” proposed by Google, the protections afforded by the Wiretap Act to many online communications would turn on whether the *recipient* of those communications decided to secure her wireless network. A “radio communication” is “readily accessible to the general public” and, therefore, exempt from Wiretap Act liability if it is not scrambled or encrypted. 18 U.S.C. § 2510(16). Consider an email attachment containing sensitive

personal information sent from a secure Wi-Fi network to a doctor, lawyer, accountant, priest, or spouse. A company like Google that intercepts the contents of that email from the encrypted home network has, quite understandably, violated the Wiretap Act. But the sender of the email is in no position to ensure that the recipient—be it a doctor, lawyer, accountant, priest, or spouse—has taken care to encrypt her own Wi-Fi network. Google, or anyone else, could park outside of the recipient’s home or office with a packet sniffer while she downloaded the attachment and intercept its contents because the sender’s “radio communication” is “readily accessible to the general public” solely by virtue of the fact that the *recipient’s* Wi-Fi network is not encrypted. Surely Congress did not intend to condone such an intrusive and unwarranted invasion of privacy when it enacted the Wiretap Act “to protect against the unauthorized interception of electronic communications.” S. Rep. No. 99-541 (1986), at 1; *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) (“The legislative history of the [Wiretap Act] suggests that Congress wanted to protect electronic communications that are configured to be private, such as email.”); *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003) (“The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.”).

The definition of “readily accessible to the general public” in § 2510(16) is limited to “radio communication,” and does not encompass all “electronic communication.” Congress’s decision to carve out “radio communication” for less protection than some other types of “electronic communication” makes sense if “radio communication” is given its ordinary meaning. Traditional radio services can be easily and mistakenly



intercepted by hobbyists. *See* 132 Cong. Rec. S7987-04 (1986) (“In order to address radio hobbyists’ concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful.”). But “radio hobbyists” do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks. Lending “radio communication” a broad definition that encompasses data transmitted on Wi-Fi networks would obliterate Congress’s compromise and create absurd applications of the exemption for intercepting unencrypted radio communications. For example, § 2511(2)(g)(ii)(II) exempts from liability, *inter alia*, the act of intercepting “any radio communication which is transmitted ... by any governmental, law enforcement ... or public safety communications system, including police and fire, readily accessible to the general public.” This provision reinforces the work performed by § 2511(2)(g)(i), which already exempts a “radio communication” that is “readily accessible to the general public.” Congress’s decision to ensure that these communications were exempt makes sense if “radio communication” encompasses only predominantly auditory broadcasts since these transmissions can be picked up by widely available police scanners. But if “radio communication” includes data transmitted over Wi-Fi networks, then § 2511(2)(g)(ii)(II) also underscores that liability should not attach to intercepting data from an unencrypted Wi-Fi network operated by, say, a police department or government agency. It seems doubtful that Congress wanted to emphasize that Google or anyone else could park outside of a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity.

Next, Google strenuously argues that the rest of the Wiretap Act supports its position that “radio communication” in 18 U.S.C. § 2510(16) means “any information transmitted using radio waves.” Google leans heavily on § 2510(16)(D) and the accompanying legislative history, which together suggest that cellular telephone and paging systems are a form of “radio communication.” If cell phone and paging systems are a type of “radio communication,” Google argues, it must be the case that Congress intended that the phrase include Wi-Fi networks and the rest of the radio spectrum because these technologies differ from paradigmatic radio communications like AM/FM, CB, and shortwave transmissions. But cell phone communications were not dissimilar from CB, shortwave, or other two-way forms of traditional radio broadcasts when § 2510(16)(D) was added to the Wiretap Act in 1986 as part of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848. When Congress enacted § 2510(16)(D), cell phones were still called “cellular radiotelephones.” *See* H.R. Rep. No. 99-647, at 20 (1986). As with other audio broadcasts, cellular conversations were often inadvertently picked up by radio hobbyists “scanning radio frequencies in order to receive public communications.” S. Rep. No. 99-541, at 3560 (1986); *see also* H.R. Rep. No. 99-647, at 20 (“Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls”). The fact that technology has evolved and cellular communications are no longer as similar to CB broadcasts as they once were does not require us to read “radio communication” to include all communications made using radio waves. Rather, the

historical context surrounding Congress's protection of cellular conversations as a form of a "radio communication" is consistent with the commonsense definition of the term because, at the time of the enactment of the definition in 1986, cellular conversations could have reasonably been construed as analogous to a form of two-way radio.<sup>6</sup> Assuming, *arguendo*, that the phrase "radio communication" covers cell phone transmissions as they existed in 1986 does not inevitably lead to the conclusion that it also encompasses transmissions that are plainly not predominantly auditory broadcasts, such as payload data transmitted over a Wi-Fi network.

Google also looks beyond the Wiretap Act in an effort to fit its expansive definition of "radio communication" into the statutory scheme. It points out that the Communications Act expressly defines the phrases "radio communication" and "communication by radio" broadly to include "the transmission by radio of writing, signs, signals, pictures, and sounds of all

---

<sup>6</sup> With modern advances in cellular technology, it is less clear how cell phones would fit within the statutory scheme today. We need not resolve this question here. Whether cell phone transmissions are an example of a "radio communication" is relevant to defining the phrase, but it is not a precursor to observing that a "radio communication" is ordinarily a predominantly auditory broadcast or to holding that payload data transmitted over a Wi-Fi network is not a "radio communication." We previously held that cell phone communications are "wire communications" for purposes of the Wiretap Act, but we did not address whether they are an example of a "radio communication." See *In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns*, 349 F.3d 1132, 1138 n.12 (9th Cir. 2003) ("Despite the apparent wireless nature of cellular phones, communications using cellular phones are considered wire communications under the statute, because cellular telephones use wire and cable connections when connecting calls.").

kinds.” 47 U.S.C. § 153(40). But when Congress wanted to borrow a definition from the Communications Act to apply to the Wiretap Act, it expressly said so. *See* 18 U.S.C. § 2510(1) (giving the phrase “communication common carrier” the meaning that it has “in section 3 of the Communications Act”). Here, Congress refrained from incorporating the definition of “radio communication” used in the Communications Act. And, as previously discussed, the Wiretap Act uses the phrases “radio communication” and “communication by radio” differently, indicating that Congress did not intend to import the Communications Act’s definition, which treats them as synonyms. *See* 47 U.S.C. § 153(40). Furthermore, the Communication Act’s definition of “radio communication” encompasses technologies like television by including “the transmission by radio of ... pictures ... of all kinds,” 47 U.S.C. § 153(40), while the Wiretap Act sometimes distinguishes them. *See, e.g.*, 18 U.S.C. § 2520(c)(1) (providing specified penalties when the “violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on [frequencies specified by regulation]”). Separate references to television-related communications would be redundant when paired with the phrase “radio communication” if we were to assume that the Communication Act’s definition applied to the Wiretap Act. Importantly, the presumption that a definition set out in one part of the code is intended to govern another is hardly unyielding in the face of such contradictory evidence. *See, e.g., General Dynamics Land Sys., Inc. v. Cline*, 540 U.S. 581, 595 (2004) (holding that the word “age” carries a different

meaning in different sections of the ADEA); *Robinson v. Shell Oil*, 519 U.S. 337, 343 (1997) (holding that the term “employees” carries a different meaning in different sections of Title VII).

Google also leans heavily on a series of amendments to 18 U.S.C. § 2510(16) to argue that Congress impliedly gave the phrase “radio communication” a meaning other than the ordinary one that we adopt here. In 1990, Senator Patrick Leahy commissioned a task force to study the effect of new technologies, including the precursors to wireless networking, on the statutory scheme created in 1986 by the Electronic Communications Privacy Act. *See* S. Hrg. 103-1022, at 179 (1994). In its report, the task force indicated it was concerned that communications by “wireless modems’ which can transmit data between computers ... will not be protected unless the user goes to the expense of full data encryption.” *Id.* at 183. The section of the report on “Wireless Data Communications” concluded that “[t]he task force recommends appropriate amendments to legally protect digital communications of this type from unauthorized interception.” *Id.* In short, the task force was of the opinion that the version of 18 U.S.C. § 2510(16) enacted in 1986 did not adequately protect unencrypted “wireless data communications.” The task force must have implicitly decided that “wireless data communications” were a “radio communication” because otherwise it would not have been concerned with § 2510(16), which only applies to “radio communication.” *See id.*

In 1994, Congress amended § 2510(16) to add a new category of communication—which it called an “electronic communication”—that it deemed to be a “radio communication” that was not “readily accessible

to the general public.” In relevant part, the statute provided that “‘readily accessible to the general public’ means, with respect to a radio communication, that such communication is not ... (F) an electronic communication.” 18 U.S.C. § 2510(16) (1994). Google claims that Congress added § 2510(16)(F) in 1994 in order to protect from interception new technologies that transmitted data using radio frequencies, including the contemporary versions of wireless networks. There is some support for this proposition in the congressional record. *See* H.R. Rep. No. 103-827, at 18 (1994) (explaining that the bill “[e]xtends privacy protections of the Electronic Communications Privacy Act to cordless phones and certain data communications transmitted by radio”).

The significance of all of this is that Congress repealed 18 U.S.C. § 2510(16)(F) in 1996. Google attempts to draw a series of inferences from the 1994 and 1996 amendments: The 1994 Congress thought that data transmissions across the wireless networks of the day were a type of “radio communication.” Otherwise, Congress would not have needed to amend § 2510(16) in order to shield them from interception given that the provision only applies to “radio communication.” By deleting § 2510(16)(F), the 1996 Congress removed the sole protection for unencrypted data transmissions over wireless networks by returning § 2510(16) to its pre-amendment form. From Google’s perspective, the upshot of this historical narrative is that payload data transmitted over an unencrypted Wi-Fi network is a “radio communication” that is “readily accessible to the general public” before the 1994 amendment and, crucially, after the 1996 repeal.

This evidence of congressional action and inaction is far more equivocal than Google acknowledges. First, the task force's report does not control what the phrase "radio communication" meant to Congress when it enacted § 2510(16) in 1986. The task force's report suggests that it thought that the "wireless data communication" technology that existed in 1991 entailed "radio communication" as the phrase is used in § 2510(16). But the task force's opinion on questions of statutory interpretation has no independent authority; it is not charged with divining congressional intent. The task force's recommendation informs us that in 1991 a group of fifteen individuals thought that early versions of wireless networks involved "radio communication" under the statute. Their opinion is not indicative of what Congress intended when it included the phrase in the Wiretap Act. It may be considered evidence of the phrase's ordinary meaning. But it does not outweigh the more substantial evidence, discussed at length above, indicating that the ordinary meaning of "radio communication" excludes data transmitted over a Wi-Fi network.

Second, Congress's decision to add § 2510(16)(F) in 1994 does not prove that it thought data transmitted over a Wi-Fi network constituted a "radio communication." The 1994 Congress was certainly concerned about ensuring that "certain data communications transmitted by radio" were protected from interception. But that does not necessarily mean that it was of the view that such communications were a "radio communication" under § 2510(16). Congress might have been forestalling the possibility that evolving technologies would be construed as radio communications, contrary to the ordinary meaning of the phrase.

Third, and perhaps most importantly, there is no reliable indication of what the 1996 Congress intended to accomplish by repealing § 2510(16)(F). Google mines the 1991 task force report and the 1994 congressional record, but it cannot close the loop on its argument because the 1996 Congress did not leave behind the snippets of enactment history that are essential to Google’s narrative. Consider two possible rationales for the 1996 repeal of § 2510(16)(F): first, Congress might have deleted the provision because it found it redundant. That is, Congress might have thought that data transmitted over a radio frequency was not a “radio communication,” which would render the additional protection for such communications offered by § 2510(16)(F) unnecessary.

Alternatively, Congress might have (correctly) determined that § 2510(16)(F) made the statute incoherent. Recall that the short-lived provision provided that “‘readily accessible to the general public’ means, with respect to a radio communication, that such communication is not ... (F) an electronic communication.” 18 U.S.C. § 2510(16)(F) (1994). The phrase “electronic communication” has been broadly defined since the Electronic Communications Privacy Act of 1986. In 1994, when § 2510(16)(F) was added, the Wiretap Act provided—as it still does today—that “‘electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce.” 18 U.S.C. § 2510(12). As Google stresses in its briefs, and the statute plainly states, “radio communication” is a subset of “electronic communication.” Yet § 2510(16)(F) conveyed that a



“radio communication” was not “readily accessible to the general public” if it was an “electronic communication,” which incoherently implies that the latter was a subset of the former. The repeal of § 2510(16)(F) could, therefore, have been a housekeeping matter designed to resolve this internal tension without affecting the protection afforded “electronic communications, including data” that the 1994 Congress sought to protect.

Neither of these entirely plausible explanations for the amendment and repeal are consistent with Google’s assumption that the pre-1994 conception of “radio communication” included data transmitted over a Wi-Fi network and the 1996 repeal of § 2510(16)(F) sought to restore that conception. The point is that we do not know why the 1996 Congress deleted § 2510(16)(F). We choose to rely on the ordinary meaning of the phrase “radio communication” rather than follow a trail of enactment history that culminates in silence and then speculate as to Congress’s unexpressed intent.

Finally, Google’s fall back position is that the rule of lenity dictates that we accept its proposed definition of “radio communication.” Although this is a civil suit, the Wiretap Act also carries criminal penalties so Google’s reliance on the rule of lenity is not unfounded. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (“Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies.”). But we do not resort to the rule of lenity every time a difficult question of statutory interpretation arises. Rather, “the rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a ‘grievous ambiguity or uncertainty in the statute.’” *Barber v. Thomas*, 130 S. Ct. 2499, 2508

(2010) (citations omitted); *see also Smith v. United States*, 508 U.S. 223, 239 (1993) (“The mere possibility of articulating a narrower construction [ ] does not make the rule of lenity applicable. Instead, that venerable rule is reserved for cases where, “[a]fter “seizing every thing from which aid can be derived,” the Court is ‘left with an ambiguous statute.’”) (citations omitted). Here, the traditional tools of statutory interpretation are sufficient. The ordinary meaning of “radio communication” is consistent with the structure of the Act and avoids absurd results without running afoul of any clearly expressed congressional intent. We need not resort to the rule of lenity where, as here, the ambiguity can be fairly resolved.

B. *Wi-Fi Transmissions Are Not “Readily Accessible to the General Public” under 18 U.S.C. § 2511(2)(g)(i)*

In the previous section, we concluded that payload data transmitted over a Wi-Fi network is not a “radio communication” under 18 U.S.C. § 2510(16). As a result, the definition of “readily accessible to the general public” in § 2510(16) does not apply to the exemption for intercepting an “electronic communication” that is “readily accessible to the general public” in § 2511(2)(g)(i). But that does not end the inquiry. Although payload data transmitted over an unencrypted Wi-Fi network is not “readily accessible to the general public” *by definition* solely because it is an unencrypted “radio communication,” it is still possible for a transmission that falls outside of the purview of the § 2510(16) definition to be considered “readily accessible to the general public”

under the ordinary meaning of that phrase.<sup>7</sup> We now hold, in agreement with the district court, that payload data transmitted over an unencrypted Wi-Fi network is not “readily accessible to the general public” and, consequently, that Google cannot avail itself of the § 2511(2)(g)(i) exemption.

First, Wi-Fi transmissions are not “readily” available because they are geographically limited and fail to travel far beyond the walls of the home or office where the access point is located. Google was only able to intercept the plaintiffs’ communications because its Street View vehicles passed by the street outside of each plaintiff’s house. The FCC generally limits the peak output of Wi-Fi broadcasts to 1 watt. *See* 47 C.F.R. § 15.247(b). Meanwhile, AM, FM, and other traditional radio broadcasts typically range from 250 to 100,000 watts. *See* Fed. Commc’n Comm’n, *Encyclopedia – FM Broadcast Station Classes and Service Countours*, available at <http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf> (last visited Aug. 13, 2013); *see also* Fed. Commc’n Comm’n,

---

<sup>7</sup> The phrase “readily accessible to the general public” is only defined insofar as the communication at issue is a “radio communication.” *See* 18 U.S.C. § 2510(16) (“‘readily accessible to the general public’ means, with respect to a radio communication ...”). The phrase is undefined where, as here, the transmission is an “electronic communication” that is not a “radio communication.” Since the term at issue is undefined, we look to its ordinary meaning. *See Hamilton*, 130 S. Ct. at 2471 (“When terms used in a statute are undefined, we give them their ordinary meaning.”). Joffe does not dispute that payload data transmitted over a Wi-Fi network is an “electronic communication,” which the Act defines as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce” subject to specific exceptions that do not apply here. 18 U.S.C. § 2510(12).

*Encyclopedia – AM Broadcast Station Classes; Clear, Regional, and Local*, available at <http://www.fcc.gov/encyclopedia/am-broadcast-stationclasses-clear-regional-and-local-channels> (last visited Aug. 13, 2013). As a result, AM radio stations have a service range of up to 100 miles, while individual Wi-Fi access points usually have a range of less than 330 feet. See Fed. Comm’n Comm’n, *Encyclopedia – Why AM Radio Stations Must Reduce Power, Change Operations, or Cease Broadcasting at Night*, <http://www.fcc.gov/encyclopedia/why-am-radio-stations-must-reduce-power-changeoperations-or-cease-broadcasting-night> (last visited Aug. 13, 2013); Encyclopedia Britannica Online, *Wi-Fi*, <http://www.britannica.com/EBchecked/topic/1473553/Wi-Fi> (last visited Aug. 13, 2013).

Second, the payload data transmitted over unencrypted Wi-Fi networks is only “accessible” with some difficulty. Unlike traditional radio broadcasts, a Wi-Fi access point cannot associate or communicate with a wireless device until it has been authenticated. See IEEE Computer Soc’y, *IEEE Standard for Information Technology — Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks — Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* 473, Fig. 11-6 (2007). Devices on Wi-Fi networks—even unencrypted networks—communicate via encoded messages sent to a specific destination over the wireless channel. *Id.* Therefore, intercepting and decoding payload data communicated on a Wi-Fi network requires sophisticated hardware and software. To capture this information, a wireless device must initiate a connection with the network and send encapsulated and coded data over the network to a

specific destination. If the communications were intercepted by a traditional analog radio device they would sound indistinguishable from random noise. Wi-Fi transmissions are not “readily accessible” to the “general public” because most of the general public lacks the expertise to intercept and decode payload data transmitted over a Wi-Fi network.<sup>8</sup> Even if it is commonplace for members of the general public to connect to a neighbor’s unencrypted Wi-Fi network, members of the general public do not typically mistakenly intercept, store, and decode data transmitted by other devices on the network. Consequently, we conclude that Wi-Fi communications are sufficiently inaccessible that they do not constitute an “electronic communication ... readily accessible to the general public” under 18 U.S.C. § 2511(2)(g)(i) as the phrase is ordinarily understood.

---

<sup>8</sup> Google argues that unencrypted data transmitted over a Wi-Fi network is “readily accessible to the general public” because the hardware used to intercept the data can be purchased by anyone and the software used to decode the data can be downloaded from the internet. A district court also reached this conclusion in a patent case. *See In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 893 (N.D. Ill. 2012) (“In light of the ease of sniffing Wi-Fi networks, the court concludes that the communications sent on an unencrypted Wi-Fi network are readily accessible to the general public.”). The availability of the technology necessary to intercept the communication cannot be the sole determinant of whether it is “readily accessible to the general public” as the phrase is ordinarily understood. A device that surreptitiously logs a computer user’s keystrokes can be purchased online and easily installed, but that hardly means that every keystroke—whether over a wired or a wireless connection—is “readily accessible to the general public.”

64a

IV. CONCLUSION

For the foregoing reasons, we affirm the judgment of the district court.

**AFFIRMED.**

**APPENDIX C**

UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

---

IN RE GOOGLE INC. STREET VIEW ELECTRONIC  
COMMUNICATIONS LITIGATION

---

No. C 10-MD-02184 JW  
Filed: June 29, 2011

---

**ORDER GRANTING IN PART AND DENYING IN  
PART DEFENDANT’S MOTION TO DISMISS WITH  
LEAVE TO AMEND**

---

**I. INTRODUCTION**

Plaintiffs<sup>1</sup> bring this putative class action against Google, Inc. (“Defendant”), alleging three causes of action for violation of the federal Wiretap Act, 18 U.S.C. §§ 2511, *et seq.*, violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, and violation of various state wiretap statutes. Plaintiffs allege that Defendant intentionally intercepted data packets, including payload data, from Plaintiffs’ Wi-Fi networks utilizing specially designed packet sniffer software installed on Defendant’s Google Street View vehicles.

---

<sup>1</sup> Plaintiffs are Patrick Keyes, Matthew Berlage, Aaron Linsky, James Fairbanks, Jeffrey Colman, John Redstone, Karl Schulz, Dean Bastilla, Vicki Van Valin, Stephanie and Russell Carter, Danielle Reyas, Bertha Davis, Jason Taylor, Jennifer Locsin, James Blackwell, Rich Benitti, Benjamin Joffe, Lilla Marigza, Wesley Hartline, David Binkley and Eric Myhre.

Presently before the Court is Defendant's Motion to Dismiss.<sup>2</sup> The Court conducted a hearing on March 21, 2011. Based on the papers submitted to date and oral argument, the Court GRANTS in part and DENIES in part Defendant's Motion to Dismiss.

## II. BACKGROUND

### A. Factual Allegations

In a Consolidated Class Action Complaint filed on November 8, 2011,<sup>3</sup> Plaintiffs allege as follows:

Plaintiffs are individuals who reside in various states,<sup>4</sup> and who maintained a Wi-Fi network in their homes that was not readily accessible to the general public and used the Wi-Fi connection to send and receive various types of payload data, including usernames, passwords and personal emails. (CCAC ¶¶ 18-38.) Each of Plaintiffs' homes can be seen depicted on Google Maps and Google Street View. (*Id.*) Defendant Google develops and hosts a broad range of Internet-based services and is incorporated under the laws of Delaware with its principal place of business in Mountain View, California. (*Id.* ¶ 39.)

Defendant launched Google Street View on May 25, 2007 in several select cities across the United States. (CCAC ¶ 55.) In the last three

---

<sup>2</sup> (Defendant Google Inc.'s Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint, hereafter, "Motion," Docket Item No. 60.)

<sup>3</sup> (Consolidated Class Action Complaint, hereafter, "CCAC," Docket Item No. 54.)

<sup>4</sup> Plaintiffs are citizens and residents of Washington, D.C.; Ohio; Pennsylvania; Nevada; Tennessee; Washington; California; Illinois; and Oregon. (CCAC ¶¶ 18-38.)



years, Google Street View has expanded broadly and now includes more cities and rural areas in the United States, and has expanded worldwide into more than 30 countries. (Id.) Google Street View is a feature embedded within Defendant's Google Maps program that offers panoramic views of various positions along streets using photos taken from a fleet of specially adapted vehicles commonly known as Google Street View vehicles. (Id. ¶¶ 54, 55.) Each Google Street View vehicle is equipped with nine directional cameras to capture 360 degree views of the streets and 3G/GSM/Wi-Fi antennas with custom-designed software for the capture and storage of wireless signals and data. (Id. ¶ 55.) Additionally, Defendant used smaller vehicles, commonly known as Google Trikes, also outfitted with the cameras and Wi-Fi equipment, to capture photo and Wi-Fi data from areas inaccessible to cars. (Id. ¶ 58.) While Defendant issued press releases to the public to disclose its intent to utilize the vehicles in order to capture photo data, Defendant failed to disclose its intent to also capture Wi-Fi data. (Id. ¶ 56.)

In 2006, prior to the launch of the Google Street View vehicles, Defendant's employee engineers intentionally created a data collection system that included code that sampled, collected, decoded and analyzed all types of data broadcast through Wi-Fi connections. (CCAC ¶¶ 60-61.) This data collection system is commonly known as a packet analyzer, wireless sniffer, network analyzer, packet sniffer or protocol analyzer. (Id. ¶ 61.) Defendant authorized inclusion of this wireless sniffer technology into its Google Street View vehicles and even sought to patent the process. (Id. ¶ 65.) The wireless sniffer

secretly captures data packets as they stream across Wi-Fi connections and then decodes or decrypts the data packet and analyzes the contents. (Id. ¶ 62.) In order to view the contents of the data packets captured by the wireless sniffer in a readable form, the packets must be stored on digital media and then decoded using cryptanalysis or a similarly complicated technology. (Id. ¶ 63.) As such, the data packets are not readable by the general public absent this sophisticated decoding and processing technology. (Id. ¶ 64.) Defendant has admitted to storing this data on their servers. (Id. ¶ 6.) The content of the data packets collected by Defendant included Plaintiffs' SSID information (the Wi-Fi network name), MAC address (the ID number of the Wi-Fi network's hardware), usernames, passwords and personal emails. (Id. ¶¶ 66, 69.)

On April 27, 2010, in response to an inquiry from a European privacy authority, Defendant posted an entry explaining that it had collected SSIDs and MAC addresses. (CCAC ¶ 69.) However, at that time, Defendant claimed to have not collected any payload, or content data from the packets. (Id. ¶ 70.) On May 14, 2010, following a request by the privacy authority to audit packet data collected by Defendant, Defendant admitted to collecting "fragmentary" samples of "publicly broadcast" payload data from open (i.e., nonpassword-protected) Wi-Fi networks and that, through this conduct, it had collected about 600 gigabytes of data from more than 30 countries. (Id. ¶¶ 71-72, 110.) Prior to May 14, 2010, Plaintiffs were unaware of and could not have discovered the existence of Defendant's unlawful conduct. (Id.

¶¶ 100-10.) On June 9, 2010, Defendant admitted that it had been collecting Wi-Fi data in the United States via Google Street View vehicles since 2007. (Id. ¶ 80.) On July 9, 2010, Defendant issued an apology on its Official Google Australia Blog where it admitted to intercepting the data in an attempt to improve Defendant's location-based services, e.g., search and maps. (Id. ¶ 100.) In October 2010, Defendant was forced to admit, following continuing investigations, that it had intercepted whole emails, usernames, passwords and other private data. (Id. ¶ 77.)

On the basis of the allegations outlined above, Plaintiffs allege three causes of action: (1) violation of the federal Wiretap Act, 18 U.S.C. §§ 2511, *et seq.*; (2) violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*; and (3) violation of various state wiretap statutes. (CCAC at 28-31.)

## **B. Procedural History**

On August 17, 2010, the United States Judicial Panel on Multidistrict Litigation transferred eight pending actions to this Court pursuant to 28 U.S.C. § 1407. (See Docket Item No. 1.) On October 18, 2010, the Court appointed Jeffrey Kodoff of Spector Roseman Kodroff & Willis, P.C. and Daniel Small of Cohen Milstein Sellers & Toll, PLLC as Interim Class and Co-Lead Counsel and Elizabeth Cabraser of Lieff Cabraser Heimann & Bernstein, LLP as Interim Class and Liaison Counsel. (See Docket Item No. 47.) On November 8, 2010, Plaintiffs filed their Consolidated Class Action Complaint. (See CCAC.)

On March 21, 2011, the Court conducted a hearing on Defendant's Motion to Dismiss. That same day, the

Court issued an Order directing the parties to submit supplemental briefs addressing three questions: (1) what “radio communication” means within the purview of the Wiretap Act; (2) whether wireless home internet networks are “radio communications” within the purview of the Wiretap Act’s usage of that term; and (3) whether cellular telephone calls constitute “radio communications” as intended by Congress when drafting the Wiretap Act and, if so, whether such technology properly fits within any of the five enumerated exceptions to the definition of “readily accessible to the general public” as outlined in Section 2510(16). (See Docket Item No. 73.) On April 11, 2011, the parties timely filed their Supplemental Briefs. (See Docket Item Nos. 79, 80.) Also on April 11, 2011, the Electronic Privacy Information Center filed a Brief for Amicus Curiae in support of Plaintiffs. (See Docket Item No. 80.)

Presently before the Court is Defendant’s Motion to Dismiss.

### **III. STANDARDS**

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a complaint may be dismissed against a defendant for failure to state a claim upon which relief may be granted against that defendant. Dismissal may be based on either the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory. Balistreri v. Pacifica Police Dep’t, 901 F.2d 696, 699 (9th Cir. 1990); Robertson v. Dean Witter Reynolds, Inc., 749 F.2d 530, 533-34 (9th Cir. 1984). For purposes of evaluating a motion to dismiss, the court “must presume all factual allegations of the complaint to be true and draw all reasonable inferences in favor of the nonmoving party.” Usher v.

City of Los Angeles, 828 F.2d 556, 561 (9th Cir. 1987). Any existing ambiguities must be resolved in favor of the pleading. Walling v. Beverly Enters., 476 F.2d 393, 396 (9th Cir. 1973).

However, mere conclusions couched in factual allegations are not sufficient to state a cause of action. Papasan v. Allain, 478 U.S. 265, 286 (1986); see also McGlinchy v. Shell Chem. Co., 845 F.2d 802, 810 (9th Cir. 1988). The complaint must plead “enough facts to state a claim for relief that is plausible on its face.” Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A claim is plausible on its face “when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009). Thus, “for a complaint to survive a motion to dismiss, the non-conclusory ‘factual content,’ and reasonable inferences from that content, must be plausibly suggestive of a claim entitling the plaintiff to relief.” Moss v. U.S. Secret Serv., 572 F.3d 962, 969 (9th Cir. 2009). Courts may dismiss a case without leave to amend if the plaintiff is unable to cure the defect by amendment. Lopez v. Smith, 203 F.3d 1122, 1129 (9th Cir. 2000).

#### **IV. DISCUSSION**

Defendant moves to dismiss Plaintiffs’ Complaint on the grounds that: (1) Plaintiffs have failed to plead that their Wi-Fi broadcasts were not “readily accessible” and thus, Defendant is entitled to exemption from liability under 18 U.S.C. § 2511(2)(g)(i), one of the Wiretap Act’s exemptions (“exemption G1”); (2) Plaintiffs’ claims based on state law wiretap statutes are preempted by the Wiretap Act and, alternatively, fail to state a claim; and (3) Plaintiffs’ “unlawful” and

“unfair” Cal. Bus. & Prof. Code §§ 17200 claims are also preempted by the Wiretap Act and, alternatively, fail to state a claim or plead standing under Proposition 64. (Motion at 5-19.) Plaintiffs respond that dismissal is improper as: (1) the Wiretap Act’s statutory definition of “readily accessible” relied on by Defendant solely applies to “radio communications” under § 2511(2)(g)(ii) (“exemption G2”) and is, thus, inapplicable to “electronic communications” under exemption G1 and the ordinary meaning of “readily accessible” should be used; (2) additionally, exemption G1 only applies to unlawful interception and access, and Plaintiffs allege that Defendant further used and disclosed the intercepted communications; (3) the state wiretap statutes are not preempted by the Wiretap Act either expressly, by field preemption, or by conflict; and (4) claims under Cal. Bus. & Prof. Code §§ 17200, *et seq.*, are not preempted by the Wiretap Act as they are qualitatively different and are properly pleaded. (Opp’n at 3-25.) The Court addresses each ground in turn.

#### **A. Wiretap Act**

Defendant contends that Plaintiffs’ Wi-Fi broadcasts were “readily accessible to the general public,” per the statutory definition provided in Section 2510(16) of the Wiretap Act, such that exemption G1 obviates Defendant’s liability for any alleged interceptions. (Motion at 5-12.) Plaintiffs respond that the Section 2510(16) definition of “readily accessible to the general public” applies solely to “radio communications,” as specified, and thus would only apply to exemption G2 (“radio communications”) and not exemption G1 (“electronic communications”). (Opp’n at 2-10.)

73a

The Wiretap Act, 18 U.S.C. § 2511(1) provides a private right of action against:

- (1) Except as otherwise specifically provided in this chapter any person who—
  - (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; ...
  - (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
  - (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; ... .

However, Section 2511(2) provides exemptions to Section 2511(1)'s private right of action:

- (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—
  - (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

- (ii) to intercept any radio communication which is transmitted—
  - (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles or persons in distress;
  - (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
  - (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
  - (IV) by any marine or aeronautical communications system; . . . .

Section 2510(16) provides the sole definition in the Wiretap Act for “readily accessible to the general public”:

- (16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not—
  - (A) scrambled or encrypted;
  - (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
  - (C) carried on a subcarrier or other signal subsidiary to a radio transmission;



- (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
- (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way communication by radio; ... .

18 U.S.C. § 2510.

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

In establishing the standard principles of statutory construction, the Supreme Court has held that the starting point at which courts should discern congressional intent is always the existing statutory text. Lamie v. U.S. Trustee, 540 U.S. 526, 534 (2004). Unless a court finds the existing statutory text such that a plain meaning interpretation would lead to absurd results, the court is bound to enforce the existing text according to its terms. Id. (citing Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A., 530 U.S. 1, 6 (2000)). “In ascertaining the plain meaning of the statute, the court must look to the particular

statutory language at issue, as well as the language and design of the statute as a whole.” K-Mart Corp. v. Cartier, Inc., 486 U.S. 281, 291 (1988). One measure of ambiguity is that the statutory text at issue is fairly capable of more than one interpretation. Chickasaw Nation v. United States, 534 U.S. 84, 90 (2001). Should a court find the statutory text ambiguous or should a plain text reading fail to yield a definitive interpretation, a court may then turn to the legislative history in order to add context to the statute. SEC v. McCarthy, 322 F.3d 650, 655 (9th Cir. 2003).

### **1. Plain Text Reading**

In this case, Congress has not expressly declared its intent as to how Section 2510(16) should apply to exemption G1 in the plain text of the statute, nor has Congress defined “radio communication” anywhere within the Act. As Congress has not provided a definition for “radio communication” within the confines of the Act, the Court first attempts to discern the ordinary and plain meaning of the term from the context of its use, from dictionary references and from Congress’ use of similar terms within the Act.

#### **a. Statutory Text**

Section 2510(16) defines “readily accessible to the general public” as it pertains specifically to “radio communication” by first establishing a presumption of ready accessibility and then defining five types of radio communications which would be expressly excluded from that presumption. Notably, none of the five express exemptions from ready accessibility under Section 2510(16) specifically address wireless internet technologies, as the list predominantly addresses radio broadcast technologies. See 18 U.S.C. §§ 2510(16)(A)-

(E). In addition to Section 2510(16), the Act uses the term “radio communication” on three other occasions. First, Section 2511(2)(g), which provides five exceptions to liability for intentional interception of wire, oral or electronic communications, makes it lawful to intentionally intercept:

[A]ny radio communication which is transmitted—

- (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or person in distress;
- (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
- (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
- (IV) by any marine or aeronautical communications system; . . . .

18 U.S.C. § 2511(2)(g)(ii). Second, Section 2511(2)(g) also makes it lawful “for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.” 18 U.S.C. § 2511(2)(g)(v). Finally, Section 2511(5)(a)(i)(B) makes unlawful and authorizes a right of action for the federal government to bring suit in federal court for the interception of “a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not

scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain.” 18 U.S.C. § 2511(5)(a)(i)(B). Title 47, part 74 of the rules of the Federal Communications Commission pertains to “Experimental Radio, Auxiliary, Special Broadcast and Other Program Distributional Services.” 47 C.F.R. § 74. Subpart D of part 74 regulates “Remote Pickup Broadcast Stations.” *Id.* Remote pickup broadcast stations are defined under the regulations as either a mobile or fixed “pickup broadcast transmitter, and its associated accessory equipment necessary to the radio communication function.” 47 C.F.R. § 74.401.

The drafting of these provisions predated the spread of wireless internet technologies and, thus, the lack of any explicit reference to wireless internet technologies does not itself preclude an interpretation of “radio communications” that would include these later-developed technologies. However, the usage of “radio communication” throughout the Act does not lend itself to a broad interpretation of the term. In particular, references to “radio communication” throughout the Act predominantly pertain to and are drafted for the particular design of radio broadcast technologies, and do not address other communications technologies that transmit using radio waves. For example, Section 2511(2)(g) makes it lawful to intentionally intercept any radio communication that “that relates to ships, aircraft, vehicles, or person in distress,” without reference to whether such radio communication was readily accessible to the general public and not scrambled or encrypted. Should the Court interpret radio communication so broadly within the Act to include such technologies as wireless

internet and cellular phones, this exception could lead to absurd results. Specifically, pursuant to this interpretation, an unauthorized intentional monitoring of a cellular phone call could be lawful should the content of the communication relate to vehicles or persons in distress, but unlawful otherwise. Further, Section 2511(2)(g) makes it lawful to intentionally intercept any radio communication transmitted by “any marine or aeronautical communications system,” which could lead to equally arbitrary results when applying the exception to communications technologies other than radio broadcast technologies, e.g., a Wi-Fi network aboard an airplane.

#### **b. Dictionary Reference**

Gleaning a plain meaning reading of “radio communication” from dictionary references is equally as inconclusive. The Oxford Dictionaries Online (“ODO”) defines “radio” as “[t]he transmission and reception of electromagnetic waves of radio frequency, especially those carrying sound messages.” Further, the ODO lists a number of more specific definitions for “radio”: (1) “the activity or industry of broadcasting sound programs”; (2) “radio programs”; (3) “an apparatus for receiving radio programs”; (4) “an apparatus capable of both receiving and transmitting radio messages between individuals, ships, planes, etc.”; (5) “ ... a broadcasting station or channel.” The ODO defines “communication,” in pertinent part, as “the imparting or exchanging of information or news.” However, the ODO, Merriam-Websters and the Oxford English Dictionary do not contain any definition for “radio communication” and, thus, fail to provide an authoritative interpretation for the compound formulation of the two words. On one hand, Congress

could have intended “radio communication” to simply combine the definition of “radio” with the definition of “communication,” thereby creating a compound that incorporates all communications transmitted using radio waves. Yet, on the other hand, Congress could have intended the compound of “radio” and “communication” to denote communications that involved a radio apparatus or a communication that solely involved the transmission of sound over radio waves. Moreover, should Congress have intended the compound term “radio communication” to mean simply “communication by radio waves,” it could have so specified. Rather, Congress chose to use the compound term, “radio communication,” a term that shares a likeness with other compound terms used throughout the Act that prefix “communication” with reference to a particular form of media; each of which are provided specialized definitions within the Act. The Court now examines the statutory text to discern how Congress intended compound terms to modify the independent meaning of each word, if at all.

### c. Compound Terms

While the ECPA does not define the compound term “radio communication,” the Act does provide definitions for three other compound terms that combine a form of media with the term “communication”: “wire communication,”<sup>5</sup> “oral communication”<sup>6</sup> and “electronic communication.”<sup>7</sup> A “wire communication,” as defined by the Act, means:

---

<sup>5</sup> See 18 U.S.C. § 2510(1).

<sup>6</sup> See 18 U.S.C. § 2510(2).

<sup>7</sup> See 18 U.S.C. § 2510(12).

[A]ny aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

18 U.S.C. § 1210(1). The Act defines “oral communication” as “any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication.”  
18 U.S.C. § 1210(2). Finally, an “electronic communication” is defined as:

[A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

- (A) any wire or oral communication;
- (B) any communication made through a tone-only paging device;
- (C) any communication from a tracking device (as defined in section 3117 of this title);

or

- (D) electronic funds transfer information stored by a financial institution in a communication

system used for the electronic storage and transfer of funds ...

18 U.S.C. § 1210(12).

In defining these compound terms, Congress intended more refined definitions than simply combining the independent meanings of each word into a unified whole, e.g., electronic communication is not defined as any communication transmitted by electronic means. Rather, Congress provided nuanced definitions of each compound term; in part, to mitigate confusion in light of the inevitable overlap between terms. For example, electronic communication expressly includes electronic communications transmitted in whole or in part by wire, but excludes wire communications. Moreover, Congress did not define “wire communication” as any communication transmitted by wire, but limited the definition to incorporate solely “aural communications” transmitted by wire. Congress also expressly included communications transmitted in whole or in part by radio as a form of electronic communication, such that an interpretation of the compound “radio communication” as all communications by radio would render all communications technologies that transmit using radio waves electronic communications. An interpretation of “radio communication” that presumptively included all technologies that transmit over radio waves, such as cellular phones, under the purview of electronic communications and held that technology bound by Section 2510(16)’s definition of “readily accessible to the general public,” would contravene Ninth Circuit precedent holding that cellular phone communications are wire



communications for purposes of the Wiretap Act.<sup>8</sup> The Ninth Circuit based its holding on the legislative history of the Act, finding that, despite the apparent wireless nature of cellular telephones, Congress intended cellular phone technology to fall into the meaning of wire communication based on the fact that cellular phones transmit the communications over wire at some point during the course of the transmission. *Id.* at 1138, n.12. Rather than simply interpret “wire communications” as all communications by wire, the Ninth Circuit found that Congress intended compound terms that prefixed “communication” with a type of media to have specialized and, at times, counter-intuitive definitions. In this case, Congress did not provide a specialized definition of “radio communication,” unlike wire, oral and electronic communication. However, such an omission does not preclude a finding that Congress intended a more sophisticated compound meaning and, as consequence, the meaning of “radio communication” remains open to multiple interpretations.

Thus, the Court finds that a plain reading of “radio communication” from the statutory text, as well as reading the text in the context of the structure and purpose of the Act, fails to yield a definitive and unambiguous result. The Court now turns to the legislative history for clarification.

## **2. Legislative History**

The ECPA was passed by Congress in 1986 to amend the Omnibus Crime Control and Safe Streets

---

<sup>8</sup> In the Matter of the Application of the United States for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d 1132 (9th Cir. 2003).

Action of 1968, commonly known as the Wiretap Act, in order to “update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.” S. Rep. No. 99-541, at 1 (1986). Prior to the amendment, Title III of the Omnibus Crime Control and Safe Streets Act provided a private right of action for interception of communications, however, the statute was expressly limited to unauthorized aural interception of wire or oral communications. Id. at 2. In 1986, the statute was, in the words of Senator Leahy, one of the senators who introduced the amendment, “hopelessly out of date.” Id.

In particular, Congress intended the 1986 amendment to bring the statute in line with “technological developments and changes in the structure of the telecommunications industry.” S. Rep. No. 99-541, at 2 (1986). Congress explicitly acknowledged the new privacy concerns faced by individuals and businesses in light of developments in the personal and commercial computing industries. Id. Developments of particular interest to the Senate Committee included the protection of privacy rights in offsite data storage, the computer-to-computer transmission of this data, and electronic mail. Id. In fact, the initial development of the amendment came on the heels of a 1984 interaction between Senator Leahy and the Attorney General where the Senator asked the Attorney General if electronic mail and computer-to-computer communications were covered by the Wiretap Act. Id. In response, the Department of Justice expressed concern that in areas of rapid technological development, “distinctions such as [whether or not a reasonable expectation of privacy exists] are not always clear or obvious.” Id. at 3. To

this end, Congress amended the Wiretap Act in order to provide statutory privacy protection and a civil right of action for interceptions of electronic communications, including, *inter alia*, computer-to-computer transmissions and electronic mail; contexts in which Congress suspected the Fourth Amendment may only dubiously apply. Id.

Another matter of importance to Congress in the drafting of the amendment was to address concerns expressed by radio hobbyists and users of radio scanners that the amendment would impose liability upon the innocent act of scanning radio broadcast frequencies in order to reach public communications, should the hobbyist inadvertently encroach upon protected communication that shares the same spectrum, for instance a cellular phone . S. Rep. No. 99-541, at 4-5 (1986). An earlier version of the amendment, the Electronic Communications Privacy Act of 1985, S. 1667, did not include the Section 2510(16) definition of “readily accessible to the general public” and applied both exemptions G1 and G2 to “electronic communication,” without any use of the term “radio communication.” 131 Cong. Rec. S. 11795, at 4. Following a year of hearings, at which concerns were raised by radio hobbyists, Senator Leahy, joined by Senator Mathias, introduced a superseding version of the bill that incorporated explicit mention of “radio communication,” including Section 2510(6) and reference in exemption G2, as well as a heightened mens rea requirement from “willful” to “intentional” to find criminal liability for interception. S. Rep. No. 99-541, at 3, 5 (1986); 132 Cong. Rec. S7987-04, at 18 (“In order to address radio hobbyists’ concerns, we modified the original language of S. 1667 to clarify that

intercepting traditional radio services is not unlawful.”).

It was in light of these dual considerations that Congress drafted the text that became Sections 2510 and 2511. Section 2510(12) defines “electronic communication” as a broad category that includes “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system ... .” 18 U.S.C. § 2510(12). As defined in the statute, a communication transmitted by radio is a specific type of electronic communication, such that exemption G1—which exempts from liability any interception of an electronic communication that is readily accessible to the general public—would exempt communications transmitted by radio as well, should those communications be “readily accessible to the general public.” 18 U.S.C. § 2511(2).

However, to clarify that “intercepting traditional radio services” was not a violation of the Act in order to quiet the concerns raised by radio hobbyists, Congress added, *inter alia*, Section 2510(16). See, e.g., 132 Cong. Rec. S7987-04, at 18. Section 2510(16) provides a definition for “readily accessible to the general public” with respect to “radio communication” that establishes a presumption of accessibility, should the communication not fit within one of five delineated exceptions. 18 U.S.C. § 2510(16). Notably, each of the five exceptions, as well as the presumption of accessibility, are drafted for the particular technology of traditional radio broadcast mediums and do not address any broader radio-based communications technology of the time, including cellular phones. The first exception to the Section 2510(16) is for “scrambled or encrypted” communications, which the Senate

Report describes as “to convert the signal into unintelligible form by means intended to protect the contents of a communication from unintended recipients.” 18 U.S.C. § 2510(16)(A); S. Rep. No. 99-541, at 11 (1986). The second exception is for communications that have been “transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication.” 18 U.S.C. § 2510(16)(B). The Senate Report clarified that “paragraph (B) refers to spread spectrum radio communications,” which was a technology that allowed for the transmission of a signal on “different frequencies where the receiving station must possess the necessary algorithm [sic] in order to reassemble the signal.” S. Rep. No. 99-541, at 11 (1986). The third exception is for communications “carried on a subcarrier or other signal subsidiary to a radio transmission,” which, according to the Senate Report, included “data and background music services carried on FM subcarriers.” *Id.* at 11-12. The fourth exception is for communications that are “transmitted over a communication system provided by a common carrier,” excluding “tone only paging system communication.” 18 U.S.C. § 2510(16)(D). The fifth exception was for communications that were transmitted on frequencies allocated under the Rules of the Federal Communications Commission for: (1) Part 25 (“Satellite Communications”); (2) subparts of Part 74 (“Experimental Radio, Auxiliary, Special Broadcast and Other Program Distributional Services”); and (3) Part 94 (“Microwave Services”). 18 U.S.C. § 2510(16)(E); 47 C.F.R. § 47(24), (74), (94).

Although the ECPA never explicitly defines “radio communication,” what the legislative history and the

context of the term's use in Section 2510(16) make clear is that Congress intended "radio communication" to include "traditional radio services," such that public-directed radio broadcast communication, as the technology was understood at the time, would be clearly excluded from liability under the Act. What the legislative history also reveals, however, is that Congress did not intend "radio communications" to be defined so broadly such that it would encompass all communications transmitted over radio waves. This was made explicit in the Senate Report's consideration of cellular phone technology, which also uses radio waves to transmit communications, and the clear intent to include such technology under the protections of the Act as a "wire communication" without any express limitation by Section 2510(16). S. Rep. No. 99-541, at 6, 11 (1986) ("Thus, a wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fiber optic cable or by radio—as in the case of cellular telephones ...").

As the legislative history demonstrates, despite the insistence of radio scanning enthusiasts, Congress stopped short of including a full exception to liability under the Act for the willful monitoring of cellular telephone calls.<sup>9</sup> S. Rep. No. 99-541, at 6 (1986). According to the Senate Report, this hesitation was based on two considerations. *Id.* First, Congress had made willful monitoring of telephone calls illegal in the original 1968 Wiretap Act should at least part of the call pass through a wire. *Id.* Second, the design of the cellular phone technology made intentional monitoring

---

<sup>9</sup> 132 Cong. Rec. S7987-04, 1986 WL 776264, at \*18 ("Under this revised Electronic Communications Privacy bill, cellular phones, private and public microwave services and voice or display pagers are protected against interception.").

of the communication more difficult than other signals commonly scanned. Id. Rather than exclude cellular phone communications from the protections of the act, the Senate Committee highlighted the possibility that the Federal Communications Commission should consider labeling cellular phone and radio scanning equipment to alert the user that such technologies are “radio-based communications” and, as such, intentional interception of the communication could violate the Wiretap Act. Id.

The presumption of accessibility established in Section 2510(16) for traditional radio broadcast technology was an appropriate response to the balance being struck between particular electronic forms of communication that were designed to be public, like traditional radio broadcast, and others that were designed to be private, like cellular phone technology. Id. However, to apply the presumption to all communications transmitted using radio technology by interpreting “radio communication” broadly would contravene congressional intent to provide protection for technology like cellular phones, which use radio waves to transmit communications, but are architected in such a way as to be private.

Thus, the Court finds that the legislative history and text of the statute demonstrate congressional intent to apply Section 2510(16)’s definition of “readily accessible to the general public” to exemption G1, and not merely to limit the application of Section 2510(16) to “radio communications” in exemption G2. However, in light of the legislative history and text of the statute, the Court also finds that Section 2510(16)’s presumption of accessibility and the requirement that a communications technology must fit within one of five exceptions were solely intended to apply to “traditional

radio services.” To interpret Section 2510(16) so broadly as to apply its strict presumption of accessibility to all communications technology that uses radio waves, regardless of the technology’s design, would disregard explicit congressional intent to include cellular phone technology within the protections of the Act and clear Ninth Circuit precedent, holding that cellular phone technologies are, in fact, “wire communications.”<sup>10</sup> Rather, for all electronic communications that could not be fairly classified as “traditional radio services,” or radio broadcast technology, regardless of the technology’s use of radio waves as the medium of transmission, the Court finds that Congress did not intend Section 2510(16)’s narrow definition of “readily accessible to the general public” to apply for purposes of exemption G1. The Court now turns to examine the sufficiency of the pleadings in light of these findings.

### **3. Sufficiency of the Pleadings**

Here, Plaintiffs allege in pertinent part:

Defendant intentionally intercepted electronic communications sent or received on wireless internet connections (“WiFi connections”) by the Class from at least May 25, 2007 through the present ... . (CCAC ¶ 1.) Defendant intercepted the Class members’ electronic communications with its Google Street View vehicles. (*Id.* ¶ 2.) When Defendant’s engineers created the data collection system for its Google Street View vehicles, most commonly known as a packet analyzer or wireless

---

<sup>10</sup> In the Matter of the Application of the United States for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d at 1138, n.12.



sniffer, they intentionally included computer code in the system that was designed to and did sample, collect, decode, and analyze all types of data sent and received over the WiFi connections of class members. (*Id.* ¶ 4.)

This data included Class members' unique, secret WiFi network identifiers (known as Service Set Identifier or SSID) and unique WiFi router numbers (Media Access Control or MAC addresses). (CCAC ¶ 4.) The data also included all or part of any personal emails, passwords, videos, audio, documents, and Voice Over Internet Protocol ("VOIP") information (collectively, "payload data") transmitted over Class members' WiFi networks in which plaintiffs had a reasonable expectation of privacy. (*Id.*) The WiFi networks from which the Google Street View vehicles collected payload data were not configured so that such data were reasonably accessible by the general public. (*Id.* ¶ 5.) Indeed, the data, as captured by the wireless sniffer, are not even readable by members of the public absent use of sophisticated decoding and processing technology. (*Id.*)

Based on the allegations above, the Court finds that Plaintiffs plead facts sufficient to state a claim for violation of the Wiretap Act. In particular, Plaintiffs plead that Defendant intentionally created, approved of, and installed specially-designed software and technology into its Google Street View vehicles and used this technology to intercept Plaintiffs' data packets, arguably electronic communications, from Plaintiffs' personal Wi-Fi networks. Further, Plaintiffs plead that the data packets were transmitted over Wi-Fi networks that were configured such that the packets

were not readable by the general public without the use of sophisticated packet sniffer technology. Although Plaintiffs fail to plead that the wireless networks fall into at least one of the five enumerated exceptions to Section 2510(16)'s definition of "readily accessible to the general public" for radio communications, the Court finds that the wireless networks were not readily accessible to the general public as defined by the particular communication system at issue, wireless internet networks, which are not "radio communications," as the term was intended by Congress in drafting Section 2510(16).

Rather, application of the Section 2510(16) definition of "readily accessible to the general public" as narrowly defined for traditional radio broadcast technology, would be inapplicable to the determination of whether Plaintiffs' allegedly intercepted data packets from their Wi-Fi networks are readily accessible to the general public for purposes of exemption G1, despite the fact that wireless networks transmit data using radio waves. As the Court has found, Congress intended Section 2510(16)'s definition to resolve the issue of radio scanning devices used to intercept radio broadcasts by establishing a presumption that traditional radio services were "readily accessible to the general public," in accord with the design of the medium as one where most communications over that medium are intended to be public. Unlike in the traditional radio services context, communications sent via Wi-Fi technology, as pleaded by Plaintiffs, are not designed or intended to be public. Rather, as alleged, Wi-Fi technology shares a common design with cellular phone technology, in that they both use radio waves to transmit communications, however they are both designed to send communications

privately, as in solely to select recipients, and both types of technology are architected in order to make intentional monitoring by third parties difficult. S. Rep. No. 99-541, at 6 (1986).

Further, applying Section 2510(16)'s narrow definition of "readily accessible to the general public" to wireless networks, a technology unknown to the 99th Congress who drafted and passed the ECPA, would contravene the primary stated purpose of the amendment, which was to update the Wiretap Act to include within the Act specific protections against intentional interceptions of computer-to-computer communications and so-called "electronic mail" or email; data Plaintiffs plead was included in the data packets intercepted by Defendant. Interpreting the ECPA such that the statute provides obscure limitations on the protection of emails and other computer-to-computer communications based on the particular medium that transmitted the electronic communication would render the Wiretap Act, and the efforts of the 99th Congress to provide such protections, absurd. Under such an interpretation, the Act would provide a private civil right of action, and even impose criminal liability, for the interception of emails transmitted over an ethernet cable through a wired network, but would stop short at protecting those very same emails should they pass momentarily over radio waves through a Wi-Fi network established to transmit data within a home. Such an interpretation cannot pass muster in the face of an explicit limitation that Section 2510(16)'s specialized definition of "readily accessible to the general public" solely apply to "radio communications," a term undefined within the statutory text, and where the legislative history of the Act makes plain that Congress intended "radio

communications” to mean traditional radio services or broadcast radio.

Defendant’s contention that Plaintiffs fail to state a claim for violation of the Wiretap Act, as Plaintiffs plead that their networks were “open” and “unencrypted,” is misplaced. (Motion at 8-11.) While Plaintiffs plead that their networks, or electronic communications systems, were configured such that the general public may join the network and readily transmit electronic communications across that network to the Internet, Plaintiffs plead that the networks were themselves configured to render the data packets, or electronic communications, unreadable and inaccessible without the use of rare packet sniffing software; technology allegedly outside the purview of the general public. Thus, the Court finds that Plaintiffs plead facts sufficient to support a claim that the Wi-Fi networks were not “readily accessible to the general public,” such that exemption G1 would not apply.

Defendant’s interpretation of United States v. Ahrndt<sup>11</sup> as standing for the principle that all unencrypted wireless networks are readily accessible to the general public and, thus, any interceptions from those networks are obviated from liability under exemption G1, unduly extends the doctrine. (Motion at 10-11.) In Ahrndt, a neighbor was connected to the Internet via her own wireless network when her network malfunctioned and her computer automatically logged in to another open wireless network operated by the defendant. Id. at \*1. The defendant had administered his iTunes software as set to “share,” such that other users on the same network would be able to access all files that the defendant had stored in

---

<sup>11</sup> No. 08-468, 2010 WL 373994 (D. Or. Jan. 28, 2010).

his iTunes libraries. Id. After being automatically logged into the defendant's wireless network, the plaintiff in Ahrndt began using her own iTunes program and noticed that the defendant's iTunes library was accessible. Id. In accessing the defendant's iTunes library, the plaintiff located a number of files containing child pornography in a subfolder within the shared directory. Id. Based on these facts, Judge King held that the plaintiff's interception was not illegal and was, in fact, "expressly lawful" under the Wiretap Act as the defendant's network and iTunes software were configured to be readily accessible to the general public. Id. at \*8. However, the court did not base its holding merely on the fact the defendant's network was unencrypted. Id. Rather, Judge King found that "defendant's conduct in operating his iTunes software with the preferences set to share, in conjunction with maintaining an unsecured wireless network router, diminished his reasonable expectation of privacy to the point that society would not recognize it as reasonable." Id. at \*8. Unlike in Ahrndt, here, Plaintiffs plead that, although the networks themselves were unencrypted, the networks were configured to prevent the general public from gaining access to the data packets without the assistance of sophisticated technology. (CCAC ¶ 5.) Thus, the Court finds that, without more, merely pleading that a network is unencrypted does not render that network readily accessible to the general public and serve to remove the intentional interception of electronic communications from that network from liability under the ECPA.

Accordingly, the Court DENIES Defendant's Motion to Dismiss Plaintiffs' First Cause of Action for violation of the Federal Wiretap Act, 18 U.S.C. §§ 2511, *et seq.*

## **B. State Wiretap Statutes**

Defendant moves to dismiss Plaintiffs' Third Cause of Action for violation of various state wiretap statutes on the grounds that claims under state wiretap statutes are preempted by the Federal Wiretap Act on express, field and conflict preemption grounds. (Motion at 12-16.)

“Pursuant to the Supremacy Clause of the United States Constitution, federal law can preempt and displace state law through: (1) express preemption; (2) field preemption (sometimes referred to as complete preemption); and (3) conflict preemption.” Ting v. AT&T, 319 F.3d 1126, 1135 (9th Cir. 2003) (citations omitted). “Express preemption exists where Congress enacts an explicit statutory command that state law be displaced.” Id. (citations omitted). “Absent explicit preemptive text, we may still infer preemption based on field or conflict preemption ... .” Id. A court may find that federal law displaces state law on field preemption grounds “when the federal statutory scheme is sufficiently comprehensive to infer that Congress left no room for supplementary regulation by the states.” Public Utility Dist. No. 1 of Grays Harbor Cty. Washington v. Idacorp, Inc., 379 F.3d 641, 647 (9th Cir. 2004) (citations and quotations omitted). “When the federal government completely occupies a given field or an identifiable portion of it ... , the test of preemption is whether ‘the matter on which the state asserts the right to act is in any way regulated by the federal government.’” Id. (citations and quotations omitted). However, “[i]n all cases, congressional intent to preempt state law must be clear and manifest.” In re Cybernetic Services, Inc., 252 F.3d 1039, 1046 (9th Cir. 2001).

Here, the Court finds that, while the ECPA contains no express preemptive statement on the part of Congress,<sup>12</sup> the ECPA was intended to comprehensively regulate the interception of electronic communications such that the scheme leaves no room in which the states may further regulate. See Bunnell v. Motion Picture Ass'n of America, 567 F. Supp. 2d 1148, 1154-55 (C.D. Cal. 2007). In particular, the ECPA was enacted, in part, to provide legal certainty to users and developers of innovative communications technologies with bright line rules for liability. S. Rep. 99-541 at 4. In so regulating, Congress struck a balance between the right to the privacy of one's electronic communications against the ability of users to access communications technologies without fear of liability for inadvertent interception. S. Rep. 99-541 at 5-6. State regulation acting in addition to the ECPA might serve to obscure the legislative scheme surrounding innovative communications technologies that Congress intended to clarify through the Act, or could serve to upset the fragile balance considered by Congress between those who transmit electronic communications and those who may inadvertently intercept those communications. Further, the statute provides for

---

<sup>12</sup> The Court finds that Defendant's interpretation of Section 2518(10)(c) as an express preemption clause misinterprets the provision. (Motion at 13.) The legislative history supports the proposition that the provision was appended to the ECPA solely to address suppression of evidence by criminal defendants. In re NSA Telecomms. Records Order Litigation, 483 F. Supp. 2d 934, 939 (N.D. Cal. 2007) (Walker, J.) (holding that Section 2518(10)(c) was drafted with the limited intent to prevent "criminal defendants from suppressing evidence based on electronic communications or customer records obtained in violation of ECPA's provisions"). Accordingly, the Court declines to adopt Defendant's position.

criminal penalties, as well as a civil right of action for violation of its provisions, such that the statute provides broad protections for interceptions under the Act. Thus, the Court finds that the federal Wiretap Act preempts state wiretap statutory schemes.

Accordingly, the Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Third Cause of Action for violation of various state wiretap statutes with prejudice.

**C. Cal. Bus. & Prof. Code §§ 17200, et seq.**

Defendant moves to dismiss Plaintiff's Second Cause of Action for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, on the grounds that claim is preempted by the Federal Wiretap Act on express, field and conflict preemption grounds; and (2) assuming *arguendo* that the claim is not preempted, Plaintiffs fail to state a claim and fail to plead Proposition 64 standing. (Motion at 17-19.) The Court addresses each ground in turn.

**1. Preemption**

At issue is whether Plaintiffs' claims for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, is preempted by the federal Wiretap Act.

Here, unlike in the context of the state wiretap statutes, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, does not seek to regulate the same field as the federal Wiretap Act. Rather, the statute was intended to broadly enable "tribunals to enjoin wrongful business conduct in whatever context such activity might occur." Barquis v. Merchants Collection Ass'n., 7 Cal. 3d 94, 111 (Cal. 1972). To this end, Section 17200's prohibition of "unlawful" acts does not proscribe specified conduct;



rather, the statute incorporates violations of other substantive law as the basis for imposing liability in order to address the added harm to the marketplace of undertaking such violations in a business context. Cal-Tech Comm'ns, Inc. v. Los Angeles Cellular Tel. Co., 20 Cal. 4th 163, 180 (Cal. 1999). Further, the Federal Wiretap Act provides no additional protection or particular civil right of action for interceptions that result in anticompetitive conduct or harm to the market, nor do such additional protections conflict with the stated purpose of the ECPA.

Thus, the Court finds that Plaintiffs' Second Cause of Action for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, is not preempted by the federal Wiretap Act.

## **2. Proposition 64 Standing**

At issue is whether Plaintiffs have properly pleaded Proposition 64 standing sufficient to support their Second Cause of Action for violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.*

To have standing to state a claim for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, as amended by the 2004 passage of Proposition 64, a plaintiff must establish that he has suffered an "injury in fact" and has "lost money or property as a result of such unfair competition." Hall v. Time Inc., 158 Cal. App. 4th 847, 852 (Cal. Ct. App. 2008). Further, allegations of an invasion of privacy are insufficient to invoke Proposition 64 standing. Ruiz v. Gap, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008).

Here, Plaintiffs allege in pertinent part:

Plaintiffs and National Class members have suffered injury in fact and lost property as a result of the unfair and unlawful business practices.

(CCAC ¶ 138.)

Based on the allegations above, the Court finds that Plaintiffs fail to plead facts sufficient to support Proposition 64 standing. In particular, interception of data packets that a plaintiff has sent over a wireless network are not lost property for purposes of determining Proposition 64 standing. Such an indefinite claim of lost property would circumvent the intent of voters, when passing the amendment, to increase the pleading requirements to state a claim for Section 17200 violation. Further, Plaintiffs contentions that merely incurring attorney fees and expenses as a result of bringing a Section 17200 claim are equally inapposite,<sup>13</sup> and would effectively eviscerate the heightened standing requirements of Proposition 64.

Accordingly, the Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Second Cause of Action for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, without prejudice to Plaintiffs to amend their pleadings to add facts sufficient to support Proposition 64 standing, if so desired.<sup>14</sup>

---

<sup>13</sup> (Opp'n at 25.)

<sup>14</sup> In amending its UCL claim, Plaintiffs must also allege more than a loss of personal information. A plaintiff's "personal information" does not constitute property under the UCL. Thompson v. Home Depot, Inc., No. 07cv1058 IEG, 2007 WL 2746603, at \*3 (S.D. Cal. Sept. 18, 2007).

**V. CONCLUSION**

The Court GRANTS in part and DENIES in part Defendant's Motion to Dismiss as follows:

- (1) The Court DENIES Defendant's Motion as to Plaintiffs' First Cause of Action for violation of the Federal Wiretap Act, 18 U.S.C. §§ 2511, *et seq.*;
- (2) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Third Cause of Action for violation of various state wiretap statutes with prejudice; and
- (3) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Second Cause of Action for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, with leave to amend.

On or before **August 1, 2011**, Plaintiffs shall file an Amended Complaint consistent with the terms of this Order.

Dated: June 29, 2011

/s/ James Ware \_\_\_\_\_  
JAMES WARE  
United States District Chief Judge



**APPENDIX D**

**STATUTORY PROVISIONS**

**18 U.S.C. § 2510. Definitions**

\* \* \*

(16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

\* \* \*

**18 U.S.C. §2511. Interception and disclosure of wire, oral, or electronic communications prohibited**

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

\* \* \*

[(2)](g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

105a

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

\* \* \*