

No. 11-17483

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

BENJAMIN JOFFE, *et al.*,

Plaintiffs-Appellees,

v.

GOOGLE INC.,

Defendant-Appellant

On Appeal from the United States District Court
for the Northern District of California, Case No. 5:10-MD-2184-JW
Hon. James Ware, U.S. District Judge

BRIEF OF APPELLANT GOOGLE INC.

David H. Kramer
Michael H. Rubin
Brian M. Willen
Caroline E. Wilson
WILSON SONSINI GOODRICH & ROSATI
PROFESSIONAL CORPORATION
650 Page Mill Road
Palo Alto, CA 94304
(650) 493-9300

Counsel for Appellant Google Inc.

February 8, 2012

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Defendant-Appellant Google Inc. states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

	Page
TABLE OF CONTENTS	ii
TABLE OF AUTHORITIES	v
PRELIMINARY STATEMENT	1
JURISDICTION	2
ISSUE PRESENTED FOR REVIEW	2
STATEMENT PURSUANT TO CIRCUIT RULE 28-2.7	3
STATEMENT OF THE CASE	3
STATEMENT OF FACTS	3
A. Wi-Fi Technology	3
B. Google’s Street View Service and The Collection of Wi-Fi Information	6
C. Plaintiffs’ Lawsuits Against Google	8
D. Google’s Motion To Dismiss Plaintiffs’ Wiretap Act Claim	9
E. The District Court’s Interpretation Of “Radio Communication”	12
SUMMARY OF ARGUMENT	14
ARGUMENT	19
I. THE WIRETAP ACT PERMITS INTERCEPTION OF RADIO COMMUNICATIONS THAT ARE READILY ACCESSIBLE TO THE GENERAL PUBLIC	20
A. Radio Communications Are Presumptively Accessible To The General Public	20

B.	The Act’s Definition Of “Readily Accessible To The General Public” Applies To Section 2511(2)(g)(i)	23
II.	PLAINTIFFS’ WI-FI TRANSMISSIONS ARE “RADIO COMMUNICATIONS” UNDER THE WIRETAP ACT	26
A.	The Term “Radio Communication” Refers To All Transmissions Made Using Radio Waves	26
1.	The ordinary meaning of “radio communication” extends beyond “traditional radio services.”	26
2.	The Communications Act definition of “radio communication” confirms that the term carries its ordinary meaning in the Wiretap Act	30
B.	The Wiretap Act’s History Eliminates Any Doubt That “Radio Communication” Includes Wi-Fi Transmissions	32
C.	Section 2510(16)’s Common-Carrier Exception Confirms That “Radio Communication” Includes All Transmissions Made By Radio Waves	37
D.	The Rule of Lenity Would Require Giving “Radio Communication” Its Ordinary Meaning	42
III.	THE DISTRICT COURT’S REASONS FOR NARROWLY CONSTRUING “RADIO COMMUNICATION” ARE NOT PERSUASIVE	45
A.	Protecting Cellular Telephone Transmissions Does Not Require A Narrow Interpretation of “Radio Communication.”	46
B.	Treating Wi-Fi Transmissions As “Radio Communications” Is Consistent With The Intent of The Wiretap Act	49
C.	Giving “Radio Communication” Its Natural Meaning Would Not Lead To Absurd Results	54

CONCLUSION 58
STATEMENT OF RELATED CASES 60
CERTIFICATE OF COMPLIANCE 61
STATUTORY ADDENDUM
TECHNICAL ADDENDUM

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Boise Cascade Corp. v. E.P.A.</i> , 942 F.2d 1427 (9th Cir. 1991)	24
<i>Cleveland v. United States</i> , 531 U.S. 12 (2000)	43
<i>Commonwealth Scientific & Indus. Research Org. v. Buffalo Tech. (USA), Inc.</i> , 542 F.3d 1363 (Fed. Cir. 2008).....	4
<i>Cooper v. FAA</i> , 622 F.3d 1016 (9th Cir. 2010), <i>cert. granted</i> , 131 S. Ct. 3025 (2011)	31
<i>DirectTV, Inc. v. Barczewski</i> , 604 F.3d 1004 (7th Cir. 2010).....	57
<i>Farina v. Nokia Inc.</i> , 625 F.3d 97 (3d Cir. 2010), <i>cert. denied</i> , 132 S. Ct. 364 (2011)	38
<i>Hamilton v. Lanning</i> , 130 S. Ct. 2464 (2010)	27
<i>In re Application of the United States for an Order Authorizing Roving Interception of Oral Communications</i> , 349 F.3d 1132 (9th Cir. 2003).....	47, 48
<i>In re Doubleclick Inc. Privacy Litig.</i> , 154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	43
<i>Leocal v. Ashcroft</i> , 543 U.S. 1 (2004)	43
<i>LVRC Holdings LLC v. Brekka</i> , 581 F.3d 1127 (9th Cir. 2009)	43
<i>Northcross v. Bd. of Educ. of the Memphis City Sch.</i> , 412 U.S. 427 (1973)	32
<i>Pinney v. Nokia, Inc.</i> , 402 F.3d 430 (4th Cir. 2005)	38
<i>Quon v. Arch Wireless Operating Co.</i> , 529 F.3d 892 (9th Cir. 2008)	42
<i>S.E.C. v. Gemstar-TV Guide Int’l, Inc.</i> , 401 F.3d 1031 (9th Cir. 2005)	20
<i>Skilling v. United States</i> , 130 S. Ct. 2896 (2010)	43
<i>Sorenson v. Sec’y of Treasury</i> , 475 U.S. 851 (1986)	24

United States v. Hermanek, 289 F.3d 1076 (9th Cir. 2002) 32

United States v. Iverson, 162 F.3d 1015 (9th Cir. 1998)..... 27

United States v. Migi, 329 F.3d 1085 (9th Cir. 2003) 24

United States v. Novak, 476 F.3d 1041 (9th Cir. 2007)
 (*en banc*) 31, 32

United States v. Santos, 553 U.S. 507 (2008) 43, 44

United States v. Universal C.I.T. Credit Corp., 344 U.S. 218
 (1952) 43, 44

Statutes

18 U.S.C. § 2510 *et seq.* 1

18 U.S.C. § 2510(1) 11, 29, 39, 47

18 U.S.C. § 2510(12) 9, 21, 25, 29

18 U.S.C. § 2510(16) *passim*

18 U.S.C. § 2510(16)(A) 22

18 U.S.C. § 2510(16)(C) 52

18 U.S.C. § 2510(16)(D) *passim*

18 U.S.C. § 2510(18) 11, 29, 39

18 U.S.C. § 2511(2)(g)(i) *passim*

18 U.S.C. § 2511(2)(g)(ii) 51, 54

18 U.S.C. § 2511(2)(g)(ii)(I) 55, 56, 57

18 U.S.C. § 2511(2)(g)(ii)(II) 23

18 U.S.C. § 2511(2)(g)(ii)(IV) 57, 58

18 U.S.C. § 2511(2)(g)(iii) 32

18 U.S.C. § 2511(4)(b) 41

28 U.S.C. § 1292(b) 2, 14

28 U.S.C. § 1331 2

47 U.S.C. § 151 *et seq.* 31

47 U.S.C. § 153(40)..... 31, 56

47 U.S.C. § 306 30

47 U.S.C. § 322 30

47 U.S.C. § 605 30

47 U.S.C. § 605(a)..... 32, 56, 57

Pub. L. No. 99-508, 100 Stat. 1848 (1986) 10

Pub. L. No. 103-414, 108 Stat. 4279 (1994) 34, 36

Pub. L. No. 104-132, 110 Stat. 1214 (1996) 36

Pub. L. No. 107-296, 116 Stat. 2135 (2002) 41

Legislative Materials

132 Cong. Rec. S14441-04 (1986) 52

132 Cong. Rec. S7987-04 (1986)..... 50

H.R. Rep. No. 99-647 (1986)..... *passim*

H.R. Rep. No. 103-827 (1994)..... 34, 35

H.R. Rep. No. 104-518 (1996) (Conf. Rep.) 36

H.R. Rep. No. 107-609(I) (2002) 41

S. Rep. No. 99-541 (1986) 25, 38, 50

S. Rep. No. 103-402 (1994) 35

Final Report of the Privacy and Technology Task Force
Submitted to Senator Patrick Leahy (May 29, 1991)..... 33, 34

Regulatory Materials

47 C.F.R. § 2.1 31

Engineering & Technology, Bulletin 56, *Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields* (4th Ed. 1999) 27, 28

In the Matter of Authorization of Spread Spectrum and Other Wideband Emissions Not Presently Provided for in the FCC Rules and Regulations, Gen. Docket No. 81-413, 101 F.C.C. 2d 419 (1985) 4

Other Authorities

Emerging Technologies in Wireless LANs (Benny Bing ed., Cambridge Univ. Press 2008) 5

Encyclopedia Britannica Online, “Wi-Fi,” <http://www.britannica.com/EBchecked/topic/1473553/Wi-Fi> (last accessed February 08, 2012) 4

The Focal Illustrated Dictionary of Telecommunications (Focal Press 1999) 31

Handbook of Electronic Security and Digital Forensics (Hamid Jahamkhani *et al.* eds., World Scientific Publ’g Co. Pte. Ltd. 2010)..... 5

Newton’s Telecom Dictionary (18th Ed. CMP Books 2002) 31

Theatre performances available in eight languages, available at <http://news.bbc.co.uk/2/hi/8380266.stm> (last visited Feb. 8, 2012) 5

Webster’s New College Dictionary (Wiley Publ’g, Inc. 2007) 3, 28

Shirley Christie, *Could the Dream of Free Wireless On the Go Soon Be a Reality in Jakarta?* (Oct. 20, 2010) available at <http://www.thejakartaglobe.com/jakarta/could-the-dream-of-free-wireless-on-the-go-soon-be-a-reality-in-jakarta/402262> (last visited Feb. 8, 2012) 6

Rudolph F. Graf, *Modern Dictionary of Electronics* (7th Ed. Newnes 1999) 28

Simon Haykin *et al.*, *Modern Wireless Communications* (Pearson Education Inc. 2005) 4

Gilbert Held, *Dictionary of Communications Technology* (3d Ed. John Wiley & Sons 1998)..... 31

K.V. Shibu, *Introduction to Embedded Systems* (Tata McGraw Hill Education Private Ltd. 2009)..... 4

Daniel Terdiman, *SF Giants bring new tech out to the ballpark* (May 11, 2009), available at http://news.cnet.com/8301-13772_3-10238394-52.html (last visited Feb 8, 2012) 5

Martin H. Weik, *Communications Standard Dictionary* (2d Ed. Van Nostrand Reinhold 1989) 28

PRELIMINARY STATEMENT

The question presented in this appeal is whether Wi-Fi transmissions—radio waves that wirelessly transmit information between computers and other devices—are “radio communications” under the federal Wiretap Act (18 U.S.C. § 2510 *et seq.*). The answer to that question is clear: while the Wiretap Act may not expressly define “radio communication,” the statute’s text, background, and structure all establish that the term refers to any communication transmitted using radio waves. That unquestionably includes the unencrypted Wi-Fi transmissions at issue in this case.

Because Wi-Fi transmissions are “radio communications,” they are expressly defined by the Wiretap Act as “readily accessible to the general public,” and their acquisition is not unlawful unless one of the statute’s specific exceptions applies. Plaintiffs did not plead that any of those exceptions covers their unencrypted Wi-Fi transmissions, and none does. Based on this, the district court should have dismissed Plaintiffs’ Wiretap Act claim.

Instead, however, the court adopted a novel interpretation of “radio communication” that cabined the term to an undefined set of “tradi-

tional radio services.” That approach defies basic canons of statutory construction and is irreconcilable with how the term “radio communication” is used throughout the Wiretap Act. The court’s interpretation also introduced significant ambiguities into the statute that improperly leave the public to guess, on pain of criminal liability, which radio-based communications are lawful to acquire.

This Court should reverse the district court’s ruling and remand with instructions to grant Google’s motion to dismiss.

JURISDICTION

The district court had jurisdiction under 28 U.S.C. § 1331 because Plaintiffs’ Wiretap Act claim arises under federal law. This Court has jurisdiction under 28 U.S.C. § 1292(b), pursuant to which the district court certified its order granting in part and denying in part Google’s motion to dismiss. This Court granted Google’s petition for permission to appeal on October 17, 2011. ER 1.

ISSUE PRESENTED FOR REVIEW

The question certified for appeal is whether Wi-Fi transmissions are “radio communications” under section 2510(16) of the Wiretap Act and thus presumptively “readily accessible to the general public.”

STATEMENT PURSUANT TO CIRCUIT RULE 28-2.7

Pertinent statutes and technical references are included in an addendum at the end of this brief.

STATEMENT OF THE CASE

This case arises out of Google’s limited acquisition of information allegedly sent over Plaintiffs’ unencrypted Wi-Fi networks. On behalf of a putative class, Plaintiffs seek damages and injunctive relief, contending that Google’s acquisition violated the federal Wiretap Act, various state wiretapping laws, and California’s unfair-competition law. The district court granted Google’s motion to dismiss the state-law claims but declined to dismiss the federal Wiretap Act claim based on its interpretation of “radio communication.” Recognizing the novelty and uncertainty of that interpretation, the district court certified its order for interlocutory review, and this Court accepted Google’s petition for permission to appeal.

STATEMENT OF FACTS

A. Wi-Fi Technology.

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 signals are broadcast by radio-transmitting devices known as “access points” or routers. *See* K.V. Shibu, *Introduction to Embedded Systems* 57 (Tata McGraw Hill Education Private Ltd. 2009); *Commonwealth Scientific & Indus. Research Org. v. Buffalo Tech. (USA), Inc.*, 542 F.3d 1363, 1367 (Fed. Cir. 2008) (explaining that Wi-Fi allows “remote devices [to] communicate with the network access points by way of radio wave transmissions”).¹

Every individual Wi-Fi device is assigned by its manufacturer a unique number called a MAC address. ER 55. In addition, wireless routers and other Wi-Fi access points are assigned an alpha-numeric “service set identifier” (“SSID”). *Id.* Routers broadcast MAC addresses and SSIDs, and that identifying information can automatically be detected by most computers and cell phones. *Id.* This is how individuals

¹ In 1985, the Federal Communications Commission (the “FCC”) enabled the development of Wi-Fi technology by amending Part 15 of its rules to allocate a portion of the radio spectrum for unlicensed use by certain communication devices. *In the Matter of Authorization of Spread Spectrum and Other Wideband Emissions Not Presently Provided for in the FCC Rules and Regulations*, Gen. Docket No. 81-413, 101 F.C.C. 2d 419, 428-30 (1985). Today, “Wi-Fi networks comprise the radio technologies associated with IEEE Standards 802.11a, 802.11b, and 802.11g”. Simon Haykin *et al.*, *Modern Wireless Communications* 328 (Pearson Education Inc. 2005); *see generally* Encyclopædia Britannica Online, “Wi-Fi,” <http://www.britannica.com/EBchecked/topic/1473553/Wi-Fi> (last accessed February 08, 2012).

are able to find and connect to available Wi-Fi networks in hotels, airports, and other public places, as well as in their homes and offices.

The Wi-Fi networks that individuals use to connect to the Internet can either be encrypted or unencrypted at the election of the network owner. Wi-Fi encryption options are included in Wi-Fi transmitting devices, and allow network owners to ensure that the transmissions made over their Wi-Fi networks are secured from public acquisition. *See Handbook of Electronic Security and Digital Forensics* 85 (Hamid Jahamkhani *et al.* eds., World Scientific Publ'g Co. Pte. Ltd. 2010). Nevertheless, it is common for Wi-Fi network owners to forego encryption to foster public access to information that is transmitted over their networks.²

² Examples of these public Wi-Fi transmissions abound: operators of Wi-Fi networks often set-up introductory pages that are automatically displayed to users who connect to their network; sports stadiums use Wi-Fi to send interactive digital messages to spectators; theatres use it to transmit subtitles with real-time translation of foreign-language works; and many purveyors of public Wi-Fi networks configure them to broadcast advertisements to users as they browse the Internet. *See, e.g., Emerging Technologies in Wireless LANs* 612, 618 (Benny Bing ed., Cambridge Univ. Press 2008); Daniel Terdiman, *SF Giants bring new tech out to the ballpark* (May 11, 2009), available at http://news.cnet.com/8301-13772_3-10238394-52.html (last visited Feb 8, 2012); *Theatre performances available in eight languages*, available at <http://news.bbc.co.uk/2/hi/8380266.stm> (last visited Feb. 8, 2012);

B. Google's Street View Service and The Collection of Wi-Fi Information.

Google's Street View feature complements Google's online map service by providing users with panoramic, street-level photographs of roads in the United States and abroad. ER 56, 228. Street View images are taken by cameras mounted on cars that drive down public roads and photograph their surroundings. *Id.* For a time, Google's Street View vehicles were also outfitted with off-the-shelf radio equipment and open-source software that enabled them to collect publicly available network information (such as SSIDs and MAC addresses) from Wi-Fi networks along the roads they travelled. ER 55-56.

As Wi-Fi networks have proliferated, the gathering of public data identifying those networks has become a common business practice designed to enable or enhance so-called "location aware" services. Because Wi-Fi networks have a limited range, the presence of any particular network acts as a unique geographical landmark. Knowing the combination of Wi-Fi networks in range of their devices allows individ-

Shirley Christie, *Could the Dream of Free Wireless On the Go Soon Be a Reality in Jakarta?* (Oct. 20, 2010) available at <http://www.thejakartaglobe.com/jakarta/could-the-dream-of-free-wireless-on-the-go-soon-be-a-reality-in-jakarta/402262> (last visited Feb. 8, 2012).

uals to pinpoint their approximate locations in situations where satellite-based Global Positioning Service (GPS) is either unavailable or inconvenient. By detecting the Wi-Fi networks available in a given area, Google and other companies can provide services that enable people to find locally relevant information about weather conditions, shopping and restaurant options, and directions to places of interest, among many other things, using their cell phones or other Wi-Fi enabled devices. ER 50, 55.

In May 2010, Google learned that its Street View vehicles had been collecting more than just identifying information about Wi-Fi networks. ER 47, 50, 244 (¶71). The vehicles had also acquired data that was sent over unencrypted Wi-Fi networks (so-called “payload data”) if that data was being transmitted at the particular moment a Street View car happened to drive by. *Id.* Google had no interest in acquiring payload data, and has never used it in any of its products or services. Upon learning of the unwanted collection, Google promptly grounded its Street View cars, segregated and rendered inaccessible the payload data that had been acquired, and hired a third party to review what had happened. ER 51, 56-57. Google also publicly described these events on

its official blog, apologized for collecting payload data, and put steps in place to prevent such collection from occurring again. ER 50-51, 55-61.

C. Plaintiffs' Lawsuits Against Google.

Starting in May 2010, shortly after Google described its collection of payload information, more than a dozen putative class-actions lawsuits challenging that activity were filed in courts around the country. Those cases were eventually transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California for pretrial coordination. ER 260-62.

Plaintiffs are individuals who allege that payload data transmitted over their unencrypted Wi-Fi networks was collected by Google. ER 231-37 (¶¶18-38), 260.³ In addition to bringing claims on their own behalf, Plaintiffs seek to represent a class consisting of all individuals whose Wi-Fi payload data was collected. ER 252 (¶119). Plaintiffs filed a Consolidated Class Action Complaint in November 2010, asserting

³ Plaintiffs have specifically admitted that the wireless networks they maintained were “open” and “unencrypted.” ER 39-41, 64-65 (¶4), 78 (¶5), 87 (¶1), 118 (¶¶6-7), 130-31 (¶¶5-7), 148 (¶¶10-11), 151 (¶31), 164 (¶3), 175-76 (¶¶3-5), 179 (¶21), 189 (¶¶10-11), 192 (¶31), 208 (¶19); *see also* ER 260 (MDL panel explaining that these actions arise “out of allegations that Google intentionally intercepted electronic communications sent or received over class members’ open, nonsecured wireless networks”).

claims under the federal Wiretap Act, various state wiretap statutes, and California's unfair competition law (UCL). ER 227-59.

D. Google's Motion To Dismiss Plaintiffs' Wiretap Act Claim.

In December 2010, Google filed a motion to dismiss Plaintiffs' complaint. With respect to the federal Wiretap Act claim, Google argued that the acquisition of data allegedly transmitted over Plaintiffs' unencrypted Wi-Fi networks was covered by section 2511(2)(g)(i) of the Wiretap Act, which expressly makes it lawful to "intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i).⁴

Google further argued that because Wi-Fi transmissions are carried on radio waves, they also constitute "radio communications" under the Wiretap Act. As a result, they are governed by section 2510(16) of the statute, which expressly defines a "radio communication" as "readily

⁴ It is undisputed that Plaintiffs' alleged transmissions were "electronic communications," as each was a "transfer of ... data ... transmitted in whole or in part by ... radio" (18 U.S.C. § 2510(12)). See ER 228 (¶¶1-2), 252 (¶119), 253 (¶122(a)) (Plaintiffs pleading that the transmissions at issue were "electronic communications" "sent or received on wireless internet connections ('WiFi connections)').

accessible to the general public” unless it falls within one of five specific exceptions. 18 U.S.C. § 2510(16).⁵ Because Plaintiffs’ unencrypted Wi-Fi transmissions did not fall within any of those exceptions, Google explained that their acquisition, as a matter of law, did not violate the Wiretap Act.

After oral argument, the district court asked the parties to provide supplemental briefs addressing three questions:

- (1) What the term “radio communication” means under the Wiretap Act;
- (2) Whether Wi-Fi transmissions are “radio communications”; and
- (3) Whether cellular telephone calls constitute “radio communications” and, if so, whether such communications fall within any of the section 2510(16) exceptions.

See ER 32-33. In response, Google explained (1) that “radio communication” carries its ordinary meaning of any communication made over radio waves; (2) that Wi-Fi transmissions, which are indisputably transmitted over radio waves, therefore readily come within the mean-

⁵ The provisions defining “electronic communication” and “readily accessible to the general public ... with respect to a radio communication” were added to the Wiretap Act by the Electronic Communications Privacy Act of 1986 (“ECPA”). Pub. L. No. 99-508, 100 Stat. 1848 (1986). As originally enacted in 1968 and before the passage of ECPA, the Wiretap Act did not address electronic communications or radio communications in any way.

ing of the term; and (3) that cellular telephone transmissions (which have never been at issue in this case) both constitute “radio communications” under the Wiretap Act and fall within at least one of section 2510(16)’s exceptions.

With regard to (3), Google showed that the statute’s legislative history makes clear that Congress intended to protect cellular communications from interception through the Common-Carrier Exception in section 2510(16), which applies to a “radio communication” that is “transmitted over a communication system provided by a common carrier” (18 U.S.C. § 2510(16)(D)). *See* H.R. Rep. No. 99-647, at 32 (1986).⁶ In light of this statutory protection, Google reassured the district court that it had no reason to be concerned that giving “radio communication” its ordinary meaning would leave cellular transmissions open to interception under the Wiretap Act.

⁶ Google further explained that cellular transmissions are also protected as “wire communications” insofar as they contain the human voice and are made in whole or in part “by the aid of wire, cable, or other like connection.” 18 U.S.C. §§ 2510(1), 2510(18); H.R. Rep. No. 99-647, at 31 (legislative history explaining Wiretap Act protection for cellular transmissions as “wire communications”).

E. The District Court’s Interpretation Of “Radio Communication.”

This appeal arises from the district court’s decision not to dismiss Plaintiffs’ Wiretap Act claim. ER 11-26.⁷ In addressing that claim, the court recognized that it was confronting an issue 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.” ER 12-13.

The court agreed with Google that if Plaintiffs’ Wi-Fi transmissions were “radio communications,” they would be deemed “readily accessible to the general public” by section 2510(16), which would make their interception lawful under section 2511(2)(g)(i). ER 13-14, 22. And the court acknowledged that “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.” ER 23-24.

⁷ The district court dismissed with prejudice Plaintiffs’ claims under the state wiretap statutes, which it held were preempted by federal law. ER 28. The court also dismissed Plaintiffs’ claims under the UCL for lack of standing. ER 29. Plaintiffs did not seek certification of those rulings, and neither is at issue here.

But the court nevertheless declined to dismiss the Wiretap Act claim because it concluded that a Wi-Fi transmission is not a “radio communication” under the statute. The court declined to give “radio communication” its ordinary meaning of all communications transmitted via radio waves. Instead, the court invoked a “specialized definition” under which “radio communication” was limited to what it termed “traditional radio services.” ER 21. The court did not explain what a “traditional radio service” is, except to suggest that it is limited to communications “designed or intended to be public” and thus excludes radio transmissions made by cellular phones and Wi-Fi networks. ER 24.⁸

Having concluded that the unencrypted Wi-Fi transmissions at issue were not “radio communications” subject to section 2510(16), the district court held that Plaintiffs had adequately pleaded that those transmissions were “electronic communications” and not “readily ac-

⁸ Elsewhere, the court intimated that “radio communication” also included “radio broadcast technology,” but it did not elaborate on what that meant or why Wi-Fi is not such a technology. *See* ER 23 (“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”).

cessible to the general public” under section 2511(2)(g)(i). ER 23-26. On that basis, the court allowed Plaintiffs’ Wiretap Act claim to survive. ER 30.

Google asked the district court to certify its Wiretap Act ruling for interlocutory appeal under 28 U.S.C. § 1292(b). ER 2. Recognizing that the interpretation of “radio communication” presented a question of “first impression” about which “there is a credible basis for a difference of opinion,” the district court granted Google’s request. ER 3-4. On October 17, 2011, this Court granted Google’s Petition for Permission to Appeal. ER 1.

SUMMARY OF ARGUMENT

Google’s alleged acquisition of information sent over Plaintiffs’ unencrypted Wi-Fi networks did not violate the Wiretap Act. The statute makes it lawful to intercept “electronic communications” that are “readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i). And when those electronic communications are also “radio communications,” the statute defines what “readily accessible to the general public” means: such a communication is expressly designated as “readily accessible to the general public” unless it falls within one of five specific

exceptions. 18 U.S.C. § 2510(16). Plaintiffs have not alleged (and cannot plausibly allege) that any of those exceptions applies here.

Instead, Plaintiffs argued below that the definition of “readily accessible to the general public” in section 2510(16) somehow does not apply to the use of that phrase in section 2511(2)(g)(i). The district court properly rejected that argument as contrary to the text and legislative history of the Wiretap Act. But the court nevertheless adopted an alternative approach that allowed Plaintiffs’ claim to survive. It held that even though Wi-Fi transmissions are made using radio waves, they are not “radio communications” because that term should be given a specialized definition limited to “traditional radio services.” The district court’s novel interpretation is untenable for multiple reasons.

First, the court’s definition of “radio communication” is contrary to the term’s ordinary meaning of any communication transmitted by radio waves. It is well settled that ordinary meaning controls where, as here, a term is not specifically defined by the statute. That rule is particularly appropriate in this case given that “radio communication” is expressly defined according to its natural meaning in the Communications Act, a closely related federal statute.

Second, the district court’s ruling that a Wi-Fi transmission is not a “radio communication” is refuted by the history of the Wiretap Act. In 1994, Congress enacted an amendment that extended the Wiretap Act to cover transmissions made over what Congress described as “wireless data networks.” That amendment brought unencrypted data transmissions like Wi-Fi within Wiretap Act protection for the first time. But Congress quickly recognized that this new protection swept too broadly, ***and it was repealed just two years later***. Congress’s actions establish beyond any doubt both that Wi-Fi transmissions are (and always have been) “radio communications” under the Wiretap Act and that acquiring transmissions from unencrypted Wi-Fi networks does not violate the statute.

Third, the district court’s interpretation is irreconcilable with the way “radio communication” is used throughout the Wiretap Act. For example, the statute’s Common-Carrier Exception (§ 2510(16)(D)) shows clearly that the term “radio communication” was intended to sweep broadly and cover all radio-based transmissions, including those involving handheld pagers and cellular telephones. These transmissions would be excluded from the district court’s understanding of “tra-

ditional radio service” because they are not designed to be public. Yet each indisputably is a “radio communication.” What makes them so is that each is transmitted using radio waves. The same is true of Wi-Fi, and there is no basis for treating a Wi-Fi transmission as anything other than a radio communication.

While there is no ambiguity about the meaning of “radio communication,” even if there were, the rule of lenity, under which ambiguous criminal statutes must be construed narrowly, would require that the Wiretap Act not be read to criminalize conduct it does not clearly forbid. Even though the district court believed that the statute’s use of “radio communication” was ambiguous, it failed to apply the rule of lenity and thus impermissibly broadened the scope of conduct that the Wiretap Act proscribes. Compounding that problem, the court adopted an interpretation of “radio communication” that is itself highly ambiguous and leaves members of the public uncertain about what radio-based transmissions are lawful to acquire.

The district court offered various reasons for restricting “radio communication” to “traditional radio services,” but none withstands scrutiny. *First*, the court suggested that interpreting the term accor-

dingly to its ordinary meaning would leave cellular telephone transmissions unprotected from interception. That is not so. The Wiretap Act protects cellular phone transmissions in multiple ways, including by classifying them as “radio communications” transmitted by common carriers. That protection is in no way diminished—indeed it requires—understanding “radio communications” to include all transmissions made by radio.

Second, the district court suggested that treating Wi-Fi transmissions as presumptively “readily accessible to the general public” would contravene congressional intent. But the court erred in asserting that the intent of section 2510(16)—the provision making it generally permissible to intercept radio communications—was solely to protect the interests of radio hobbyists. That provision serves a broader public interest: to declare all transmissions by radio presumptively accessible to the general public. That way, anyone (hobbyist or otherwise) can lawfully acquire radio transmissions unless they fall within one of a few objectively identifiable categories. Transmissions over unencrypted Wi-Fi networks are not among the categories deemed off limits. To the contrary, although Congress in 1994 enacted an exception to the presump-

tion of ready accessibility that actually covered wireless data transmissions like Wi-Fi, that exception was promptly repealed. Congress's repeal of the 1994 amendment makes clear that the result Google seeks is entirely consistent with legislative intent.

Third, the court asserted that a plain-language interpretation of “radio communication” would lead to absurd results, suggesting for example that Wi-Fi transmissions that were encrypted would still be subject to interception if made on board a ship or airplane. But that simply is not so: nothing unanticipated by Congress or out of line with the Wiretap Act's statutory scheme follows from giving “radio communication” its ordinary meaning.

For these reasons, Plaintiffs' Wiretap Act claim fails as a matter of law, and this Court should enter an order requiring its dismissal.

ARGUMENT

The district court's interpretation of the Wiretap Act presents a question of law that this Court reviews *de novo*. *See, e.g., S.E.C. v. Gemstar-TV Guide Int'l, Inc.*, 401 F.3d 1031, 1044 (9th Cir. 2005).

I. THE WIRETAP ACT PERMITS INTERCEPTION OF RADIO COMMUNICATIONS THAT ARE READILY ACCESSIBLE TO THE GENERAL PUBLIC.

Plaintiffs' Wiretap Act claim is premised on the allegation that Google acquired unencrypted Wi-Fi transmissions. But Google's actions did not violate the Wiretap Act. The statute makes it lawful to acquire "electronic communications" that are "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). And it expressly defines as "readily accessible to the general public" any "radio communication" that does not fall into one of five specific exceptions. 18 U.S.C. § 2510(16). Because Plaintiffs' Wi-Fi transmissions do not fall within any of those exceptions, their acquisition was not unlawful.

A. Radio Communications Are Presumptively Accessible To The General Public.

The Wiretap Act provides that it "shall not be unlawful" to "intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). It is undisputed that the transmissions at issue here were "electronic communications." Plaintiffs pleaded as much (ER 228 (¶¶1-2), 252 (¶119), 253 (¶122(a))), and that is confirmed by the Wiretap

Act's definition of "electronic communication," which includes the transfer of "data" "in whole or in part" by "radio." 18 U.S.C. § 2510(12); *see also* H.R. Rep. No. 99-647, at 35.

Plaintiffs' transmissions were also "radio communications" under the Wiretap Act. *Accord* H.R. Rep. No. 99-647, at 36 ("Inclusion of the term 'radio' in the definition of 'electronic communication' in Section 2510(12) reflects the fact that radio communications come within the scope of chapter 119."). Like all Wi-Fi transmissions, those at issue here were made using a radio transmitter (a wireless access point) that conveyed them via radio waves to computers or other similar devices. *See supra* at pp 3-4.

The fact that Wi-Fi transmissions are radio based is fatal to Plaintiffs' claim. Section 2510(16) of the Wiretap Act expressly designates any "radio communication" (*i.e.*, any transmission made over radio waves) as "readily accessible to the general public"—and thus not unlawful to intercept under section 2511(2)(g)(i)—unless it falls within one of five carefully delineated exceptions. 18 U.S.C. § 2510(16); *see also* H.R. Rep. No. 99-647, at 37 ("The new paragraph (16) states 'readily accessible to the general public' means with respect to a radio communica-

tion, that such is not in one of five separate categories.”); ER 13-14. As the district court recognized, Plaintiffs’ complaint makes no allegation that any of those exceptions applies to their Wi-Fi transmissions. ER 23-24.

In fact, Plaintiffs specifically admitted that they left their Wi-Fi networks “open” and “unencrypted,” thereby taking their Wi-Fi transmissions outside section 2510(16)(A)’s Encryption Exception. *See* ER 39-41, 64-65 (¶4), 78 (¶5), 87 (¶1), 118 (¶¶6-7), 130-31 (¶¶5-7), 148 (¶¶10-11), 151 (¶31), 164 (¶3), 175-76 (¶¶3-5), 179 (¶21), 189 (¶¶10-11), 192 (¶31), 208 (¶19). The Encryption Exception—which renders radio communications that are “scrambled or encrypted” off limits from interception—is a way to bring virtually any radio transmission, including those sent over Wi-Fi networks, within the protection of the Wiretap Act. But as Plaintiffs themselves acknowledged, they did not avail themselves of that option.

While Google believes that Plaintiffs cannot plausibly allege that their Wi-Fi transmissions were protected by any of the other section 2510(16) exceptions, this Court need not address that issue. The complaint that the district court evaluated includes no such allegations. On

the record before this Court, therefore, Plaintiffs' Wiretap Act claim is not and cannot be saved by the section 2510(16) exceptions.

B. The Act's Definition Of "Readily Accessible To The General Public" Applies To Section 2511(2)(g)(i).

Unable to bring their Wi-Fi transmissions within any of section 2510(16)'s exceptions, Plaintiffs argued that the Wiretap Act's definition of "readily accessible to the general public" in section 2510(16) does not apply when that phrase is used in section 2511(2)(g)(i) of the statute. The district court rejected this argument (ER 22), and for good reason.

The phrase "readily accessible to the general public" appears in two places in the Wiretap Act. *See* 18 U.S.C. § 2511(2)(g)(i); 18 U.S.C. § 2511(2)(g)(ii)(II). That phrase is defined in section 2510(16), which provides that "readily accessible to the general public means, with respect to a radio communication, that such communication is not" one of the five enumerated exceptions. There is no basis for applying section 2510(16)'s definition of "readily accessible to the general public" to the phrase's second appearance in the statute, but not to its first.

Doing so would violate the plain language of the Wiretap Act. Section 2510 says expressly that its definitions apply to those terms "[a]s used in this chapter." Section 2511(2)(g)(i) is certainly "in" chapter

119, and the statute thus directs that the term “readily accessible to the general public” as used there be given its defined meaning. *Cf. United States v. Migi*, 329 F.3d 1085, 1087 (9th Cir. 2003) (“When we interpret a word in a statute, we use the statute’s definition of that word.”). Giving different definitions to the two appearances of the phrase, as Plaintiffs urged, also violates the rule “that words used more than once in the same statute have the same meaning.” *Boise Cascade Corp. v. E.P.A.*, 942 F.2d 1427, 1432 (9th Cir. 1991); *see also Sorenson v. Sec’y of Treasury*, 475 U.S. 851, 860 (1986).

That section 2511(2)(g)(i) refers to “electronic communication” (and not specifically to “radio communication”) does not advance Plaintiffs’ argument. Under the Wiretap Act, the terms “electronic communication” and “radio communication” are not mutually exclusive. The definition of “electronic communication” makes clear that a communication can be both concurrently. 18 U.S.C. § 2510(12) (“electronic communication” includes communications “transmitted in whole or in part by ... radio”); *see also* H.R. Rep. No. 99-647, at 35-36. During the time that an “electronic communication” is being transmitted by radio it is also a “radio communication,” and may be acquired without liability

under section 2511(2)(g)(i), so long as it does not fall within one of section 2510(16)'s five specific exceptions.

The inter-relationship between those two provisions is confirmed by their legislative history. The Senate Committee Report introducing section 2511(2)(g)(i) says expressly that it:

provides an exception to the general prohibition on interception for electronic communications which are configured to be readily accessible to the general public. Thus, the radio communications specified in proposed subsection 2510(16) are afforded privacy protections under this legislation unless another exception applies.

S. Rep. No. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555; *see also* H.R. Rep. No. 99-647, at 41. This passage shows beyond all doubt that section 2510(16)'s definition of the phrase "readily accessible to the general public" "with respect to a radio communication" applies fully to section 2511(2)(g)(i) whenever the "electronic communication" in question is also a "radio communication."

In sum, the text and structure of the Wiretap Act make clear that insofar as Plaintiffs' Wi-Fi transmissions are "radio communications," they were presumptively "readily accessible to the general public" under section 2510(16), and their interception was lawful under section 2511(2)(g)(i).

II. PLAINTIFFS' WI-FI TRANSMISSIONS ARE "RADIO COMMUNICATIONS" UNDER THE WIRETAP ACT.

Having agreed with Google on all of the points above (ER 13-14, 22), the district court should have dismissed Plaintiffs' Wiretap Act claim. Instead, however, the court held that Plaintiffs' Wi-Fi transmissions were not "radio communications" because they were not what it labeled "traditional radio services." ER 25. Without explaining what a "traditional radio service" is, the court suggested that its new definition covered only communications intended to be public, and thus excluded transmissions from cellular telephones and Wi-Fi networks. ER 24-25. The district court's decision to confine "radio communication" to "traditional radio services" was incorrect. That limiting construction ignores the plain language of the Wiretap Act, ignores fundamental principles of statutory interpretation, and is irreconcilable with the Act's history and structure.

A. The Term "Radio Communication" Refers To All Transmissions Made Using Radio Waves.

1. The ordinary meaning of "radio communication" extends beyond "traditional radio services."

"Radio communication" is not expressly defined by the Wiretap Act. Any interpretation of "radio communication" must therefore begin

with the ordinary meaning of those words. It is a basic rule of statutory construction that when “terms used in a statute are undefined, we give them their ordinary meaning.” *Hamilton v. Lanning*, 130 S. Ct. 2464, 2471 (2010) (quotations and citations omitted); *see also 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.”).

The ordinary meaning of the term “radio communication” is straightforward. “Radio” refers to the radio frequency (“RF”) portion of the electromagnetic spectrum, which is “generally defined as the part of the spectrum where electromagnetic waves have frequencies in the range of about 3 kilohertz to 300 gigahertz.” FCC Office of Engineering & Technology, Bulletin 56, *Questions and Answers about Biological Effects and Potential Hazards of Radiofrequency Electromagnetic Fields*, at 2-3 (4th Ed. 1999) (“FCC Bulletin 56”).⁹ In turn, the dictionary de-

⁹ *See also, e.g.*, Rudolph F. Graf, *Modern Dictionary of Electronics* 615 (7th Ed. Newnes 1999) (defining “radio” as “[a] general term, principally an adjective, applied to the use of electromagnetic waves between 10 KHz and 3000 GHz); Martin H. Weik, *Communications Standard Dictionary* 883 (2d Ed. Van Nostrand Reinhold 1989)

finer “communication” as “the information, signals, or message.” Webster’s New College Dictionary 295; *see also* Communications Standard Dictionary 178 (defining “communication” as “[a] method or means of conveying information of any kind from one person or place to another, except by direct unassisted conversation or correspondence.”).

Accordingly, “radio communication” by its terms refers to any information transmitted using radio waves, *i.e.*, the radio frequency portion of the electromagnetic spectrum. This is an objective definition that allows individuals to determine easily whether something is or is not a radio communication: if a communication is transmitted via radio waves, it is a radio communication. That is true whether or not it is what someone might think of as a “traditional radio service.”

Disregarding these points, the district court gave the term “radio communication” a meaning significantly narrower than the ordinary understanding of those words. In explaining its decision to depart from ordinary meaning, the court pointed to the fact that other compound terms in the Wiretap Act such as “wire communication” and “electronic

(defining radio as “[a] device, or pertaining to a device, that transmits or receives electromagnetic waves in the frequency bands that are between 10 KHz and 3000 GHz.”).

communication” are defined in specialized ways.¹⁰ The court suggested that this indicated that Congress intended all the Act’s compound terms, including “radio communication” to have “more refined definitions than simply combining the independent meanings of each word into a unified whole.” ER 17-18.

That approach gets it backwards. The 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 be defined in a specialized or narrow way. That contrast is all the more reason to understand “radio communication” according to its ordinary meaning. The statutory definitions expressly providing for “electronic communication” and “wire communication” illustrate that Congress knew how to indicate when it wanted terms to have specialized meanings. By not providing such a definition

¹⁰ For example, the Wiretap Act defines “wire communication” to require an “aural transfer,” *i.e.*, a transmission “containing the human voice.” 18 U.S.C §§ 2510(1), 2510(18). And it defines “electronic communication” broadly, but specifically to exclude, among other things, any “wire communication,” “any communication made through a tone-only paging device,” and “any communication from a tracking device.” 18 U.S.C. § 2510(12). These specialized definitions are the careful product of a statute that has been amended multiple times over several decades to adapt to evolving technologies.

for “radio communication,” Congress indicated its expectation that that term would bear its ordinary meaning—not some more “refined” definition. And under that ordinary meaning, Wi-Fi transmissions, which are carried by radio waves, are unquestionably radio communications.

2. The Communications Act definition of “radio communication” confirms that the term carries its ordinary meaning in the Wiretap Act.

Further proof of what “radio communication” means in the Wiretap Act comes from the definition given to that term in a related statute, the Communications Act of 1934, 47 U.S.C. §§ 151 *et seq.*

Like the Wiretap Act, the Communications Act repeatedly uses the term “radio communication.” *See, e.g.*, 47 U.S.C. §§ 306, 322, 605.

And the Communications Act provides an express definition:

The term ‘radio communication’ or ‘communication by radio’ means the ***transmission by radio*** of writing, signs, signals, pictures, and sounds of all kinds, including all instrumentalities, facilities, apparatus, and services ... incidental to such transmission.

47 U.S.C. § 153(40) (emphasis added). This definition is not limited to “traditional radio services,” but instead sweeps in any communication transmitted via radio waves. That is confirmed by the FCC regulation defining “radiocommunication” as “[t]elecommunication by means of ra-

radio waves.” 47 C.F.R. § 2.1. The Communications Act definition illustrates that the ordinary meaning of “radio communication” is broad and includes all transmissions made by radio.¹¹

The Communications Act is a “reliable extrinsic source” for interpreting the term “radio communication” in the Wiretap Act. *Cooper v. FAA*, 622 F.3d 1016, 1032 (9th Cir. 2010), *cert. granted*, 131 S. Ct. 3025 (2011). “[C]ourts generally interpret similar language in different statutes in a like manner when the two statutes address a similar subject matter.” *United States v. Novak*, 476 F.3d 1041, 1051 (9th Cir. 2007) (*en banc*); *see also Northcross v. Bd. of Educ. of the Memphis City Sch.*, 412 U.S. 427, 428 (1973). Applying that rule, this Court has looked to analogous federal statutes to ascertain the meaning of undefined terms in the Wiretap Act. *See, e.g., United States v. Hermanek*, 289 F.3d 1076, 1086 n.3 (9th Cir. 2002).

¹¹ *See, e.g.,* Newton’s Telecom Dictionary 608 (18th Ed. CMP Books 2002) (radio communication means “[a]ny telecommunication by means of radio waves”); Gilbert Held, Dictionary of Communications Technology 437 (3d Ed. John Wiley & Sons 1998) (radio communication means “[c]ommunications by means of radio waves”); Xerxes Mazda *et al.*, The Focal Illustrated Dictionary of Telecommunications 510 (Focal Press 1999) (“radiocommunications” is a “[g]eneric term used to cover any form of communications which occurs using radio waves and operating within the radio frequency spectrum.”).

The Communications Act and the Wiretap Act both regulate the collection of, and permissible access to, information transmitted via various communications media. Moreover, the two statutes expressly depend on one another. They cross reference in several places and together provide an integrated regime regulating the transmission and interception of a wide variety of communications. *See, e.g.*, 47 U.S.C. § 605(a); 18 U.S.C. § 2511(2)(g)(iii). The statutory overlap extends to the regulation of radio communications themselves. In proscribing certain conduct relating to the unauthorized use of “any interstate or foreign communication by ... radio,” the Communications Act expressly exempts conduct “authorized by chapter 119, Title 18”—the Wiretap Act. 47 U.S.C. § 605(a). This intimate relationship between the two statutes provides an especially compelling reason to look to the Communications Act definition to understand what radio communication means in the Wiretap Act.

B. The Wiretap Act’s History Eliminates Any Doubt That “Radio Communication” Includes WiFi Transmissions.

The Wiretap Act’s history confirms the statute’s plain meaning, and establishes beyond any doubt that transmissions made via wireless data networks such as Wi-Fi are “radio communications.”

Shortly after amending the Wiretap Act through ECPA in 1986, Congress commissioned a task force charged with “examining current developments in communications technology and how they relate to the legal framework for protecting communications privacy.” Final Report of the Privacy and Technology Task Force Submitted to Senator Patrick Leahy (May 29, 1991), *reprinted in* S. Hrg. 103-1022, at 179 (Mar. 18 & Aug. 11, 1994). The task force issued its report in 1991. Among the new technologies that the task force studied were “wireless modems” and “wireless local area networks.” S. Hrg. 103-1022, at 179. The task force expressly acknowledged that those “new radio-based communications technologies ... do not fall clearly within the protections afforded by ECPA.” *Id.* at 180.

As the task force explained, that was because of section 2510(16)’s definition of “readily accessible to the general public,” which applied “[w]ith regard to radio-based technologies.” *Id.* at 181. The task force understood that “wireless data communications” (including wireless modems “which can transmit data between computers without the computers being wired together”) were “radio communications” under the Act, and thus that their protection depended on whether they fell with-

in one of the section 2510(16) exceptions. *Id.* at 183. The task force concluded: “Under current FCC proceedings, there is a likelihood that such communications will not be protected unless the user goes to the expense of full data encryption” (thus bringing the communication within the Encryption Exception). *Id.* Accordingly, the task force recommended that Congress consider “appropriate amendments” to protect such communications under the Wiretap Act. *Id.*

In 1994, Congress acted on the task force’s recommendations and amended the Wiretap Act. *See* Pub. L. No. 103-414, § 203, 108 Stat. 4279, 4291 (1994); H.R. Rep. No. 103-827, pt. 1, at 14 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489 (discussing recommendations that “the legal protections of ECPA be extended to cover new wireless data communications, such as those occurring over cellular laptop computers and wireless local area networks (LANs), and cordless phones”); *id.* at 18 (describing how 1994 amendments extended “privacy protections of the Electronic Communications Privacy Act to cordless phones and certain data communications transmitted by radio”).

When Congress acted to protect what it termed “wireless data communications,” it did so by recognizing that such transmissions are

“radio communications” under section 2510(16). The 1994 legislation thus amended section 2510(16) to add “electronic communication” as a new category of radio communication that was specifically excepted from the provision’s presumption that radio communications are readily accessible to the general public. *See* H.R. Rep. No. 103-827, pt. 1, at 30; S. Rep. No. 103-402, at 32 (1994). Congress explained that with this change the Wiretap Act provided “protection for all forms of electronic communications, including data, even when they may be transmitted by radio.” *Id.*

Congress thus premised the 1994 amendments on precisely the understanding of the statute that Google has advanced in this case: (1) under the Wiretap Act, transmissions from wireless data networks are “radio communications”; (2) the Act did not protect those transmissions from interception unless they fell within one of the existing section 2510(16) exceptions; and (3) to protect wireless data communications, Congress had to change the law by creating a *new* exception to section 2510(16)’s presumption of ready accessibility.

Understanding the basis for the 1994 amendment is critical because the statutory protections that Congress created for “wireless data

communications” were short-lived. Just two years later, ***Congress repealed the 1994 amendment.*** Pub. L. No. 104-132, § 731(2), 110 Stat. 1214, 1303 (1996). The 1996 legislation eliminated section 2510(16)’s newly created sixth exception in section 2510(16) for “electronic communications” sent by radio. H.R. Rep. No. 104-518, at 80, 93 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 944; *compare* Pub. L. No.103-414, §203, 108 Stat. 4279, 4291 (1994) *with* Pub. L. No. 104-132, §731, 110 Stat. 1214, 1303 (1996) *and* 18 U.S.C. § 2510(16). The effect of the 1996 repeal was to return the Wiretap Act’s treatment of wireless data communications to the pre-1994 status quo under which they were presumptively deemed “readily accessible to the general public.” *See* H.R. Rep. No. 104-518, at 124. And Congress has not revisited the issue since. From 1996 through the present, therefore, unencrypted wireless data communications (including Wi-Fi transmissions) have enjoyed no Wiretap Act protection.

This history, which the parties discussed in their briefs below but which the district court did not mention, directly undermines the court’s ruling. The 1994 amendment and its repeal confirm both that Wi-Fi transmissions are “radio communications” and that the Wiretap Act

protects Wi-Fi transmissions only if they fall within one of the five remaining section 2510(16) exceptions. That decides this case. None of those exceptions applies to Plaintiffs' unencrypted Wi-Fi transmissions, and Google's acquisition thus did not violate the Wiretap Act.

C. Section 2510(16)'s Common-Carrier Exception Confirms That "Radio Communication" Includes All Transmissions Made By Radio Waves.

That radio transmissions, including Wi-Fi, are "radio communications" under the Wiretap Act is further confirmed by the way that term is used throughout the statute, particularly in section 2510(16)'s Common-Carrier Exception.

That exception provides that a "radio communication" transmitted "over a communication system provided by a common carrier" is protected from interception "unless the communication is a tone only paging system communication." 18 U.S.C. § 2510(16)(D). This provision and its legislative history clearly establish that "radio communication" includes transmissions from cellular telephones and from paging systems. That is so even though neither fits the district court's apparent understanding of "traditional radio service."

Congress enacted the Common-Carrier Exception in 1986 with the intention that it would protect cellular communications from interception. Congress understood that cellular transmissions are radio-based. S. Rep. No. 99-541, at 9 (explaining that cellular telephone technology “uses both radio transmissions and wire”); H.R. Rep. No. 99-647, at 31 (referring to cellular transmissions as “communications utilizing cellular radio”).¹² In light of that, Congress amended the Wiretap Act to ensure protection of cellular transmissions in two distinct ways.

Congress first redefined the term “wire communication” to include any transmission “containing the human voice at any point” so long as it occurred “in whole or in part” though a wire or cable. 18 U.S.C. § 2510(1), (18); H.R. Rep. No. 99-647, at 31, 35, 41. Although this change covered most cellular telephone transmissions at the time (H.R. Rep. No. 99-647, at 31), Congress also recognized that it might not protect all future cellular transmissions. *Id.* at 32 (explaining that cellular trans-

¹² As the district court recognized, cellular technology “uses radio-waves to transmit communications.” ER 21; *see also, e.g., Farina v. Nokia Inc.*, 625 F.3d 97, 104 (3d Cir. 2010), *cert. denied*, 132 S. Ct. 364 (2011) (“A cell phone functions by transmitting information between its low-powered radio transmitter and a base station”); *Pinney v. Nokia, Inc.*, 402 F.3d 430, 439 (4th Cir. 2005) (“A wireless telephone (commonly called a cell phone) is actually a radio containing a low power transmitter.”).

missions would not be protected as wire communications insofar as “the evolution of cellular technology permits the switching or transmission of mobile-to-mobile service (or mobile-to-landline service) without the use of wire, cable, or other like connection).” Purely radio-based cellular transmissions that never touched a “wire or cable,” and those that lacked the human voice would fall out of the definition of “wire communications” and instead be “electronic communications.” *Id.* at 35 (“Communications consisting solely of data, for example, and all communications transmitted only by radio would be electronic communications.”).

It was to ensure that those cellular transmissions would be protected by the Wiretap Act that Congress enacted the Common-Carrier Exception in section 2510(16). The legislative history explains what Congress intended:

Because cellular communication is transmitted over a communications 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.

H.R. Rep. No. 99-647, at 32 (footnote omitted).

This legislative history collapses the district court’s effort to limit “radio communication” to “traditional radio services.” In the court’s view, cellular transmissions are not a “traditional radio service” (and thus not a “radio communication” under the Wiretap Act) because they “are designed to send communications privately.” ER 24. But the Common-Carrier Exception shows clearly that cellular transmissions are radio communications. Because section 2510(16) applies only to “radio communications,” protecting cellular transmissions under the Common-Carrier Exception *requires* that they be radio communications. The district court’s contrary interpretation thus cannot be correct.¹³

¹³ Further confirmation that the term “radio communication” includes cellular communications (and other radio-based telephone transmissions) is provided by a provision that existed in the Wiretap Act from 1986 until 2002. That provision imposed a reduced penalty for the interception of certain kinds of “radio communications,” including “the radio portion of a cellular telephone communication” and “a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.” ECPA § 101(d)(2) (former version of 18 U.S.C. § 2511(4)(b)). While Congress repealed this provision in 2002 (*see* Pub. L. No. 107-296 § 225(j), 116 Stat. 2135, 2158 (2002)), it did so because it came to believe that “the special penalty scheme for cell phone violations should be eliminated” (H.R. Rep. No. 107-609(I), at 17 (2002), *reprinted in* 2002 U.S.C.C.A.N. 1352)—not because it wanted to narrow in any way the scope of the term “radio communication.” The

Cellular transmissions are not the only non-traditional radio service that qualifies as a “radio communication” under the Common-Carrier Exception. The exception by its terms makes clear that it also covers paging-system transmissions. 18 U.S.C. § 2510(16)(D); *see also* H.R. Rep. No. 99-647, at 37. Like cell phone transmissions, paging communications are not “designed or intended to be public.” ER 24. They are private transmissions made to particular individuals. Yet, like cellular transmissions, paging-system communications, which similarly use radio waves to wirelessly transmit information,¹⁴ are “radio communications” for purposes of the Wiretap Act.

Congress’s classification of paging transmissions as “radio communications” further refutes the district court’s interpretation. It shows beyond all doubt that what makes something a radio communication has nothing to do with whether it is a “traditional radio service” (or whether it was meant to be public). What matters is that the communi-

elimination of the penalty provision thus left the meaning of “radio communication” exactly as it was before.

¹⁴ See H.R. Rep. No. 99-647, at 23-24 (explaining that “[r]adio paging” “uses radio signals” to send tones or alphanumeric messages to users’ pagers); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 895 (9th Cir. 2008) (describing paging-system communication as “a radio frequency transmission”).

cation is transmitted using radio waves. Transmissions made using pagers, cellular telephones, wireless modems, and Wi-Fi networks all are “radio communications” for exactly this reason.

D. The Rule of Lenity Would Require Giving “Radio Communication” Its Ordinary Meaning.

Even if understanding “radio communication” by its ordinary meaning did not so clearly follow from the Wiretap Act’s text and history, the proper interpretation of “radio communication” would at the very least be ambiguous. If that were case, the rule of lenity would require that any such ambiguity be resolved in favor of Google’s interpretation.

Under the rule of lenity, any ambiguity in the Wiretap Act would have to be read to minimize the range of potentially criminal conduct created by the statute. *See United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality op.) (“The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them.”); *United States v. Universal C.I.T. Credit Corp.*, 344 U.S. 218, 221-22 (1952) (“[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.”); *LVRC Holdings LLC v. Brekka*,

581 F.3d 1127, 1134 (9th Cir. 2009) (“The Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants.”).¹⁵ Thus, if it really were ambiguous whether the Wiretap Act makes it unlawful to acquire unencrypted Wi-Fi transmissions then the Act would have to be construed to avoid that result.

The district court ignored these principles of lenity, even though the court itself believed that the statute was ambiguous. ER 18 (asserting that reading the term “radio communication,” even in the context of the text, structure, and purpose of the Wiretap Act, “fails to yield a definitive and unambiguous result”). Given its own uncertainty about whether the statute actually proscribes the interception of unencrypted Wi-Fi transmissions, the court was required by the rule of lenity to avoid “deriv[ing] criminal outlawry from some ambiguous implication.”

¹⁵ Although it is being applied civilly here, the Wiretap Act is a criminal statute and it is a “familiar principle that ‘ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.’” *Skilling v. United States*, 130 S. Ct. 2896, 2932 (2010) (quoting *Cleveland v. United States*, 531 U.S. 12, 25 (2000)); accord *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (applying rule of lenity in a civil context to a statute that “has both criminal and noncriminal applications”); *Brekka*, 581 F.3d 1134-35 (same); *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 513 (S.D.N.Y. 2001) (applying lenity in civil action brought under the Wiretap Act).

Universal C.I.T. Credit, 344 U.S. at 222. It did the opposite. By reading “radio communication” narrowly, the court increased for everyone the set of interceptions made criminal by the Wiretap Act without any definite indication from Congress that such a result was intended. That approach “turns the rule of lenity upside down.” *Santos*, 553 U.S. at 519.

The district court’s ambiguous interpretation of “radio communication” only compounds its error. The court did not explain what it meant by a “traditional radio service” or precisely what kinds of radio-based transmissions are supposed to qualify. It is unclear, for example, whether the court’s definition is supposed to turn on objective factors (as do all of the section 2510(16) exceptions) or instead on some subjective determination of whether the broadcaster intended the radio communication to be private. *Cf.* ER 24 (“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.”).¹⁶ In this re-

¹⁶ The district court also intimated, without elaboration, that what it called “radio broadcast technology” would also meet the definition of “radio communication.” ER 23; *see also id.* 22. This aspect of the decision below is particularly mystifying. After all, everyone agreed that Wi-Fi transmissions are radio waves. And they certainly emanate

spect, the court's approach transforms what is supposed to be a clear, definite, and objective term (describing any transmission made using radio frequencies) into an unclear and indeterminate one, which may turn on the subjective intent of the person doing the transmitting. And it does so in a way that exposes members of the public to criminal and civil liability if they guess wrong. Beyond all the other problems with the court's interpretation, and given the imperatives of the rule of lenity, the district court's creation of this ambiguity is reason alone to reject the ruling below.

III. THE DISTRICT COURT'S REASONS FOR NARROWLY CONSTRUING "RADIO COMMUNICATION" ARE NOT PERSUASIVE.

As discussed above, the district court's interpretation of the term "radio communication" is contrary to the Wiretap Act's text, history,

from "radio broadcast technology." Based on that, Wi-Fi transmissions should have qualified as a radio communication even under the district court's reasoning (or any normal understanding of the phrase "radio broadcast technology"). That the district court nevertheless excluded Wi-Fi from its interpretation of "radio communication" only further illustrates the problems with the court's understanding of the term. The court's approach offers members of the public no guidance about which radio-based transmissions are "radio communications" and which are not. This uncertainty about what can lawfully be acquired and what acts can subject a person to criminal punishment is exactly the problem that the rule of lenity is meant to avoid.

and structure—and violates basic canons of statutory construction. The district court offered several explanations for why it reached its erroneous result, but none of them withstands scrutiny.

A. Protecting Cellular Telephone Transmissions Does Not Require A Narrow Interpretation of “Radio Communication.”

The district court expressed concern that giving “radio communication” its ordinary meaning would sweep in transmissions made via cellular telephones. ER 17-18, 21-23, 24. The court assumed that if the term were understood broadly enough to include cellular telephone calls, those calls could be freely intercepted under the Wiretap Act. ER 22. That concern is misplaced.

As explained above, the Wiretap Act fully protects cellular transmissions. A cellular transmission is protected as a “wire communication” provided that it includes the human voice and is made “by the aid of wire, cable or other like connection.” 18 U.S.C. § 2510(1). Wire communications are not subject to the provision making it lawful to intercept electronic communications that are “readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i); *see also* H.R. Rep. No. 99-647, at 41 (“nothing carried by wire is ‘readily accessible to the general pub-

lic”). There thus was no reason for the district court to worry that treating cellular transmissions as radio communications would make them fair game for interception.

The district court apparently believed that Google’s interpretation of “radio communication” would contravene *In re Application of the United States for an Order Authorizing Roving Interception of Oral Communications*, 349 F.3d 1132 (9th Cir. 2003). ER 17-18, 22-23. But *In re United States* merely confirms that “communications using cellular phones are considered wire communications under the statute, because cellular telephones use wire and cable connections when connecting calls.” *Id.* at 1138 n.12. That is quite right, but it says nothing about the meaning of “radio communication.” *In re United States* does not mention the term “radio communication” or purport to interpret it, and certainly provides no support for the district court’s approach.

Even more significantly, the court ignored the alternative form of protection that Congress contemplated for cellular communications—as “radio communications” carried by a common carrier. *See* H.R. Rep. No. 99-647, at 32 (explaining that the common-carrier exception would cover cellular communications that did not qualify as wire communica-

tions). Protecting cellular transmissions under the Common-Carrier Exception is not merely consistent with their being classified as “radio communications,” it demands it. *See supra* pp. 37-42.

The district court thus had it backwards when it asserted that interpreting “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 protection of the Act.” ER 22. Honoring Congress’s intent to protect cellular communications via the Common-Carrier Exception requires interpreting section 2510(16) to apply to communications—including cellular transmissions—made via radio waves, regardless of whether those communications are “traditional radio services.”

Beyond all that, the district court drew the wrong conclusion from the fact that Congress amended the Wiretap Act expressly to include protections for cellular telephone transmissions. While it went out of its way to make it unlawful to intercept cellular telephone calls (and other radio-based communications, such as certain kinds of paging transmissions), Congress has done nothing similar for Wi-Fi. To the contrary,

Congress specifically undid the statutory protections it briefly extended to wireless data transmissions like Wi-Fi. *See supra* pp. 32-37.

In short, Google's interpretation of "radio communication" poses no threat to the security of cellular transmissions, and the protections the Wiretap Act affords to cellular communications provide no basis for misreading the statute to protect unencrypted Wi-Fi transmissions.

B. Treating Wi-Fi Transmissions As "Radio Communications" Is Consistent With The Intent of The Wiretap Act.

The district court appealed in various places to its understanding of Congress's purpose in enacting and amending the Wiretap Act, but it misapprehended the legislative history it discussed.

One reason that the district court gave for limiting "radio communication" to traditional radio services was its belief that section 2510(16) was intended solely to protect radio hobbyists from liability for "the innocent act of scanning radio broadcast frequencies in order to reach public communications." ER 19-20. That mistakes the purpose and effect of section 2510(16).

Section 2510(16) was added to the Wiretap Act in 1986 via ECPA. One aim of the provision was to ensure that the Wiretap Act would not

make it illegal for radio hobbyists to intercept radio transmissions. *See* S. Rep. No. 99-541, at 4; 132 Cong. Rec. S7987-04, at 15 (1986). But that was not the provision’s only purpose—and it certainly is not its only consequence. If Congress’s goal was merely to protect a few discrete forms of radio transmission that were routinely intercepted by hobbyists, it would have been easy for it to identify and exempt those particular transmissions. Indeed, that is precisely what Congress did in enacting section 2511(2)(g)(i)-(ii). That provision expressly makes it lawful to intercept “specific types of radio communications which have traditionally been free from prohibitions on mere interception.” H.R. Rep. No. 99-647, at 41.

But section 2510(16) takes the opposite approach. It creates a presumption that *all* radio communications are “readily accessible to the general public” and then carves out a few specific radio communications from that broad presumption and deems them protected. *See* H.R. Rep. No. 99-647, at 37 (explaining that “if a radio communication fits into one of the five categories then it will have privacy protection (unless some other exception applies to preclude coverage)”). Congress took that tack precisely in order to avoid “listing all the existing radio servic-

es which are exempt from the bar on interceptions”—an approach that it rejected because it “would have been cumbersome, possibly redundant, and would have had a built-in obsolescence.” *Id.* at 42.

Thus, while Congress “listed some of the more common radio services” that it specifically wanted to make open to interception (in the provision that became section 2511(2)(g)(ii)), it simultaneously included (in what became section 2510(16)) “a ‘generic’ exception” making radio communications presumptively free to acquire unless they are specifically exempted from that presumption. And the list of radio communications exempted—which ranges from cellular telephone transmissions (H.R. Rep. No. 99-647, at 32); to “data carried on the vertical blanking interval (VBI) of a television signal” (H.R. Rep. No. 99-647, at 37); to certain transmissions via audio subcarrier (18 U.S.C. § 2510(16)(C))—goes well beyond the types of communications that were regularly (or even could have been) intercepted by radio hobbyists. *See generally* 132 Cong. Rec. S14441-04, at 28-29 (1986).

Nor is it remotely the case, as the district court believed, that “each of the five exceptions” in section 2510(16) “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.” ER 20. Those exceptions cover an array of communications—from paging transmissions to private microwave services—broader than anything that could plausibly be considered traditional radio broadcasting. Particularly bewildering in this respect is the district court’s statement that the section 2510(16) exceptions do not address cell phones. As discussed above, the Common-Carrier Exception (18 U.S.C. § 2510(16)(D)) was specifically intended to cover cellular transmissions. *See supra* pp. 32-37. The set of transmissions encompassed by section 2510(16)’s presumption of ready accessibility (and its exceptions to that presumption) destroys any suggestion that the provision was “solely intended to apply to ‘traditional radio services.’” ER 22.

The district court also expressed concern that treating Wi-Fi transmissions as “radio communications” under section 2510(16) “would contravene the primary stated purpose” of enacting ECPA in 1986. ER 24. Any concern about that is directly answered by the 1994 amendment to section 2510(16) and its prompt repeal in 1996. *See supra* pp. 32-37.

Those actions make clear that Congress understood the issues raised under the Wiretap Act by wireless data networks like Wi-Fi. One Congress acted to extend the statute's protections to cover transmissions from wireless data networks, but *the very next Congress undid those protections.*

Given that history, it is entirely consistent with congressional intent to apply section 2510(16)'s presumption of ready public accessibility to radio transmissions occurring over Wi-Fi networks. That approach advances the purpose of the 1996 amendment: it eliminates a categorical statutory protection for radio-based data transmissions, while leaving those transmissions subject to Wiretap Act protection if they come within one of the other section 2510(16) exceptions, such as the Encryption Exception.

Accordingly, if unencrypted Wi-Fi transmissions are to be protected under the Wiretap Act, the way to achieve that result is for Congress to revisit the statute. It is not for the courts to construe the Act in a way that distorts its meaning and usurps congressional prerogatives.

C. Giving “Radio Communication” Its Natural Meaning Would Not Lead To Absurd Results.

Finally, the district court suggested that understanding “radio communication” to include all transmissions made via radio frequencies would lead to absurd results. Its concern centered on section 2511(2)(g)(ii), which identifies a specific set of radio communications that may always be lawfully intercepted. 18 U.S.C. § 2511(2)(g)(ii). The district court had no reason to worry.

The court first alluded to section 2511(2)(g)(ii)(I). According to the court, this provision

makes it lawful to intentionally intercept any radio communication that [sic] ‘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.

ER 15. This analysis is misguided.

First, the district court appeared to misunderstand what section 2511(2)(g)(ii)(I) actually covers. By its terms, section 2511(2)(g)(ii)(I)

makes it lawful to intercept any “radio communication which is transmitted—**by any station** for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress.” (Emphasis added). As the italicized language shows, the provision focuses on the purpose of the “station” that is responsible for the radio transmission, not (as the district court assumed) on the substance of the particular communication that is transmitted. Radio communications—including private cellular telephone transmissions—that are otherwise protected by the Wiretap Act, would not be exempted from protection by section 2511(2)(g)(ii)(I) merely because their contents happened to relate to a person (or ship or airplane) in distress.

Second, the idea that unintended results would flow from section 2511(2)(g)(ii)(I) unless “radio communication” is limited to traditional radio services is refuted by 47 U.S.C. § 605(a). That provision of the Communications Act generally makes it unlawful to divulge the contents of an intercepted communication without the authorization of the sender. But that prohibition does not apply to “any radio communication **which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in**

distress, or which is transmitted by an amateur radio station operator ...” (emphasis added).

That is significant because, as discussed above (*See supra* pp. 30), the Communications Act expressly defines “radio communication” to include any information transmitted by radio. 47 U.S.C. § 153(40). Yet, despite that broad definition, Congress still considered it appropriate to immunize the interception (and use) of radio communications insofar as they related to “ships, aircraft, vehicles, or persons in distress.” This provision thus directly counters the district court’s suggestion that the use of “radio communication” in section 2511(2)(g)(ii)(I) of the Wiretap Act “does not lend itself to a broad interpretation of the term.” ER 15. Section 605(a) makes clear that Congress saw nothing absurd about the result that concerned the district court here.

The district court also referred to section 2511(2)(g)(ii)(IV) of the Wiretap Act, which “makes it lawful to intentionally intercept any radio communication transmitted by ‘any marine or aeronautical communications system.’” ER 15. The court suggested that a broad understanding of radio communication “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.” *Id.* This concern is equally unwarranted.

As the only reported decision interpreting section 2511(2)(g)(ii)(IV) confirms, the phrase “marine or aeronautical communications system” focuses narrowly on the systems used by ships or airplanes to communicate with one another or with controllers. *DirecTV, Inc. v. Barczewski*, 604 F.3d 1004, 1006 (7th Cir. 2010) (“aeronautical communication system” means “a system of communications to and from airplanes”—more specifically, “a system for issuing navigation instructions to aircraft or receiving their distress calls”). The Seventh Circuit’s ruling puts the district court’s fear to rest. Adopting the plain meaning of “radio communication” will not leave all radio-based communications used by airplane passengers open to interception. Only the narrow set of radio transmissions occurring over specialized systems relating to aeronautical or marine navigation or interaction are interceptable under section 2511(2)(g)(ii)(IV).

The district court’s misplaced concerns provide no basis for construing “radio communication” in a way contrary to its ordinary meaning, to the structure and legislative history of the Wiretap Act, and to

the definition that the term is expressly given in the Communications Act.

CONCLUSION

For the reasons given above, the district court's decision should be reversed.

Respectfully submitted,

DATED: February 8, 2012

/s/ Michael H. Rubin

David H. Kramer

Michael H. Rubin

Brian M. Willen

Caroline E. Wilson

WILSON SONSINI GOODRICH & ROSATI

PROFESSIONAL CORPORATION

650 Page Mill Road

Palo Alto, CA 94304

(650) 493-9300

Counsel for Appellant Google Inc.

STATEMENT OF RELATED CASE

Appellant is not aware of any related case pending before this Court.

DATED: February 8, 2012

/s/ Michael H. Rubin

David H. Kramer

Michael H. Rubin

Brian M. Willen

Caroline E. Wilson

WILSON SONSINI GOODRICH & ROSATI

PROFESSIONAL CORPORATION

650 Page Mill Road

Palo Alto, CA 94304

(650) 493-9300

Counsel for Appellant Google Inc.

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 12,676 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirement of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Century Schoolbook font.

DATED: February 8, 2012

/s/ Michael H. Rubin

David H. Kramer

Michael H. Rubin

Brian M. Willen

Caroline E. Wilson

WILSON SONSINI GOODRICH & ROSATI

PROFESSIONAL CORPORATION

650 Page Mill Road

Palo Alto, CA 94304

(650) 493-9300

Counsel for Appellant Google Inc.

STATUTORY ADDENDUM

ADDENDUM OF STATUTORY REFERENCES

TABLE OF CONTENTS

	<u>Tab</u>
18 U.S.C. § 2511(2)(g).....	1
18 U.S.C. § 2510	2

18 U.S.C. § 2511(2)(g) provides:

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;
- (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[.]

18 U.S.C. § 2510 provides:

As used in this chapter—

- (1) “wire communication” means any 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;

* * *

- (12) “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 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 communications system used for the electronic storage and transfer of funds;

* * *

- (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) “aural transfer” means a transfer containing the human voice at any point between and including the point of origin and the point of reception[.]

TECHNICAL ADDENDUM

ADDENDUM OF TECHNICAL REFERENCES

TABLE OF CONTENTS

	<u>Tab</u>
<i>Emerging Technologies in Wireless LANs</i> 612, 618 (Benny Bing ed., Cambridge University Press 2008).....	1
The Focal Illustrated Dictionary of Telecommunications 510 (Focal Press 1999)	2
<i>Handbook of Electronic Security and Digital Forensics</i> 85 (Hamid Jahankhani <i>et al.</i> eds., World Scientific Publ'g Co. Pte. Ltd. 2010).....	3
Newton's Telecom Dictionary 608 (18th Ed. CMP Books 2002).....	4
Webster's New College Dictionary 295, 1636 (Michael Agnes ed., Wiley Publishing, Inc. 2007)	5
Rudolf F. Graf, <i>Modern Dictionary of Electronics</i> 615-616 (7th Ed. Newnes 1999).....	6
Simon Haykin <i>et al.</i> , <i>Modern Wireless Communications</i> 328 (Pearson Education Inc. 2005).....	7
Gilbert Held, <i>Dictionary of Communications Technology</i> 437 (3d Ed. John Wiley & Sons 1998)	8
K.V. Shibu, <i>Introduction to Embedded Systems</i> 57 (Tata McGraw Hill Education Private Ltd. 2009).....	9
Martin H. Weik, <i>Communications Standard Dictionary</i> 178, 883 (2d Ed. Van Nostrand Reinhold 1989).....	10

Emerging Technologies in Wireless LANs

Theory, Design, and Deployment

Edited by

BENNY BING

Georgia Institute of Technology



CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo, Delhi

Cambridge University Press
32 Avenue of the Americas, New York, NY 10013-2473, USA

www.cambridge.org
Information on this title: www.cambridge.org/9780521895842

© Cambridge University Press 2008

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2008

Printed in the United States of America

A catalog record for this publication is available from the British Library.

ISBN 978-0-521-89584-2

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party Internet Web sites referred to in this publication and does not guarantee that any content on such Web sites is, or will remain, accurate or appropriate.

All trademarks mentioned in this publication are the property of the respective owners. Use of a term in this publication should not be regarded as affecting the validity of any trademark or service mark.

While the publisher, editor, and contributors have used their best efforts in preparing this publication, they make no representation or warranties with respect to the accuracy or completeness of this publication and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher, editor, or contributors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

612 Hot Spots: Public Access using 802.11

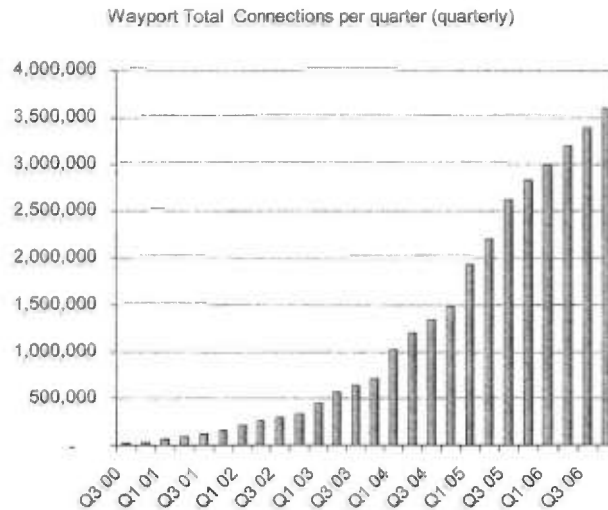


Figure 28.2: Non-cumulative quarterly use at Wayport-provided hotspots on a per-quarter basis. Two factors are at work here, use rate (percent of people using the network) increased, and the number of locations also increased.

Access control is usually done via a gateway that controls access to the Internet via a firewall rule set. In the case of access control, the process of getting connected at a hotspot goes like this:

- 1) The user's Wi-Fi network interface card associates with an access point by selecting an SSID (service set identifier) from a list of available SSIDs.
- 2) If the user is configured for DHCP, the computer obtains an IP address from the gateway (usually this is a private, RFC1918-space address)
- 3) If the device is configured for a static IP address, the gateway will masquerade the address by performing network address translation of that address to another address.
- 4) DNS servers are assigned.
- 5) The user opens a browser going to their homepage.
- 6) The gateway detects Web proxy settings and listens for an http request on proxied ports.
- 7) The firewall prevents the connection to the homepage and performs a 302-re-direct to a "splash page" (also called a forced first page).
- 8) The user interacts with this Web page to either purchase or otherwise accept terms and conditions.
- 9) After the appropriate access/payment credentials and/or terms and conditions are accepted, the firewall rule set is changed to allow access to the Internet at large for the time period purchased (typically 24 hours). Some sites charge per minute.
- 10) If the user wishes to use e-mail, many gateways provide transparent SMTP proxy to an SMTP e-mail server, or provide instructions on how to set up e-mail to use the server.
- 11) If the user wishes to use a VPN, they are provided an option (usually on the first page) to use a public IP address rather than a 1918-space private address because some VPNs do not function well with network address translation.
- 12) The access control is usually done via the MAC address of the network interface card. Thus, if the user changes locations (e.g., goes to a different part of the building), the

618 Hot Spots: Public Access using 802.11

deployed in Anaheim last summer with eventual plans for covering 50 square miles. In the initial deployment, some of the issues with propagation of Wi-Fi signal in the hills of Anaheim surfaced as difficulties that would have to be overcome. One of the problems that has surfaced has to do with the difficulty of getting decent signal-to-noise ratio of the Wi-Fi signal from outside to the inside of a building.

Several cities have jumped on board with muni-Wi-Fi plans. Tropos announced in January [4] that the 500th city to use their mesh solution had signed a contract. It should be noted, however, that whereas there are major new initiatives being signed every month, the initial results of these deployments are mixed with even some initial success stories reporting ongoing troubles [5]. Moreover, there are several legal issues regarding the muni-Wi-Fi systems being deployed. For example, Pennsylvania passed a state law requiring a waiver from local broadband providers (with Philadelphia grandfathered in). This has been challenged at the Federal level with the Communications, Consumer's Choice, and Broadband Deployment Act in the Senate and a similar bill with different wording proposed in the House of Representatives. It is unclear at this time what the future holds on the legal, business, and technical front for these networks.

28.6 Trends in Advertising on Wi-Fi Networks

One of the most interesting business models that has been proposed is to fund access to Wi-Fi networks via advertising. The basic idea is similar to how radio and television programs are funded through advertising – sponsored advertisements could be presented to a user (e.g., on the splash page of a web-browser connection), and this advertising revenue stream can be used to fund the Wi-Fi network. Moreover, seeing as a Wi-Fi signal can be localized, the advertising can be targeted towards local businesses. Imagine being at a hotel and seeing an advertisement for a restaurant 3 blocks away. Google and Earthlink have teamed up in San Francisco to pilot this kind of system. It should be noted, however, that there are several technical challenges to be overcome. One clear issue is how does this kind of a business model work for non-browser-based access as described above? Also, this is not really a new idea and there are several patents around local advertising and services in a Wi-Fi environment [6].

28.7 Trends in WiMax

In addition to Wi-Fi networks, WiMax (802.16d) is a new technology that can run over private or public RF channels. The new mobile WiMax standard (802.16e) is also potentially disruptive. Some have even gone as far to say that WiMax may be the death of Wi-Fi. Whereas WiMax (in the 802.16d version) is an excellent last-mile connectivity alternative to DSL, cable, T-1 or other broadband methods of distribution, it is not well suited for mobile computing access. It is an excellent alternative for muni-Wi-Fi deployments, and may present a strong competitive alternative to these networks. 802.16e is designed to address the mobile computing issues, but it has a long way to go to catch the economic curve of 802.11 with 500 million chipsets already in production and costs decreasing every year.

The Focal Illustrated Dictionary of Telecommunications

Xerxes Mazda

Fraidoon Mazda



FOCAL PRESS

OXFORD JOHANNESBURG BOSTON MELBOURNE NEW DELHI SINGAPORE

Focal Press

An imprint of Butterworth-Heinemann

Linacre House, Jordan Hill, Oxford OX2 8DP

225 Wildwood Avenue, Woburn, MA 01801-2041

A division of Reed Educational and Professional Publishing Ltd

 A member of the Reed Elsevier plc group

First published 1999

© Reed Educational and Professional Publishing Ltd 1999

All rights reserved. No part of this publication may be reproduced in any material form (including photocopying or storing in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) without the written permission of the copyright holders except in accordance with the provisions of the Copyright, Design and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London, England W1P 9HE. Applications for the copyright holders' written permission to reproduce any part of this publication should be addressed to the publishers.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0 240 51544 7

Printed in Great Britain by Biddles Limited, Guildford and King's Lynn



FOR EVERY TITLE THAT WE PUBLISH, BUTTERWORTH-HEINEMANN
WILL PAY FOR BTCC TO PLANT AND CARE FOR A TREE.

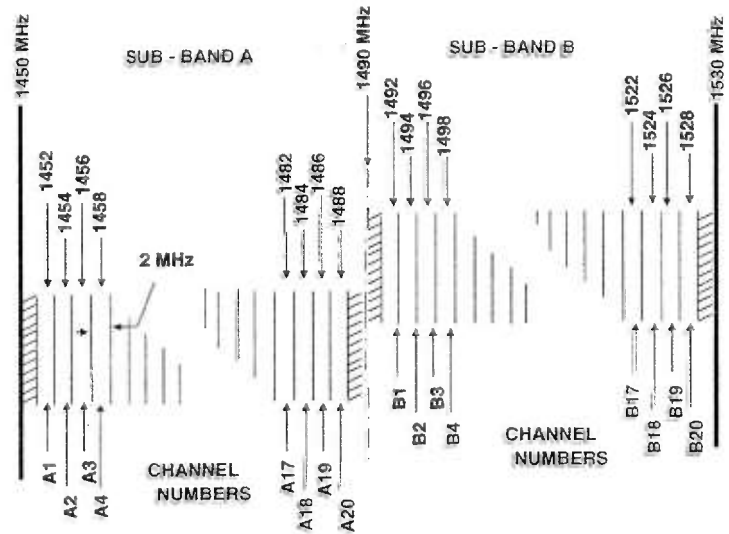


Figure R.2 Radio channelling plan

transmission, so two of the channels (e.g. A1 and B1) would be needed for a bi-directional link.

Radio Common Carrier (RCC): A common carrier who provides radiocommunications services.

radiocommunications: Generic term used to cover any form of communications which occurs using radio waves and operating within the radio frequency spectrum.

Radiocommunications Advisory Group (RAG): Part of the ITU-R (see Figure I.10), it monitors and provides guidance to the ITU-R Study Groups, as well as undertaking other tasks, such as recommending actions to be taken to increase cooperation with other organisations and advising the Director of the Radiocommunications Bureau.

Radiocommunications Assembly: Part of the organisation of the ITU-R (see Figure I.10) it contains the Study Groups which carry out the standardisation development work within the ITU-R.

Radiocommunications Bureau: Part of the ITU-R organisation (see Figure I.10) the Radiocommunications Bureau is run by a Director who is responsible for organising and coordinating the work of the ITU-R. It provides all the administrative and technical support to the Conferences and Study Groups, applies the provisions of the *Radio Regulations*, coordinates the preparation and publication of all documents, and records and registers frequency assignments and orbital characteristics of



HANDBOOK OF ELECTRONIC SECURITY AND DIGITAL FORENSICS

edited by

Hamid Jahankhani
University of East London, UK

David Lilburn Watson
Watson Business Solutions Ltd., UK

Gianluigi Me
Università degli Studi di Roma "Tor Vergata", Italy

Frank Leonhardt
Independent Consultant and Commentator

 **World Scientific**

NEW JERSEY • LONDON • SINGAPORE • BEIJING • SHANGHAI • HONG KONG • TAIPEI • CHENNAI

Published by

World Scientific Publishing Co. Pte. Ltd.

5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

HANDBOOK OF ELECTRONIC SECURITY AND DIGITAL FORENSICS

Copyright © 2010 by World Scientific Publishing Co. Pte. Ltd.

All rights reserved. This book, or parts thereof, may not be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system now known or to be invented, without written permission from the Publisher.

For photocopying of material in this volume, please pay a copying fee through the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, USA. In this case permission to photocopy is not required from the publisher.

ISBN-13 978-981-283-703-5

ISBN-10 981-283-703-5

Typeset by Stallion Press

Email: enquiries@stallionpress.com

Printed in Singapore by Mainland Press Pte Ltd.

4.3.1. *Change Default Administrator Passwords (and Usernames)*

At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide a web-page interface that allows owners to enter their network addresses and account information. These web configuration tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.

4.3.2. *Turn on (compatible) WPA/WEP Encryption*

All Wi-Fi equipment supports some form of *encryption*. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally, you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore, you may need to find a “lowest common denominator” setting.

4.3.3. *Change the Default SSID*

Access points and routers all use a network name called the *SSID*. Manufacturers, normally, ship their products with the same SSID set. For example, the SSID for Linksys devices is normally “linksys”. Whilst knowing the SSID does not, by itself, allow your neighbours to break into your network, it is a start. More importantly, when someone finds a default SSID, they see it as a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network.

4.3.4. *Enable MAC Address Filtering*

Each piece of Wi-Fi gear possesses a unique identifier called the *physical address* or *MAC address*. Access points and routers keep track of the *MAC addresses* of all devices that connect to them. Many such products offer the owner an option to enter the *MAC addresses* of their home equipment and restrict the network to only allow connections from those devices. Do this, but also know that the feature is not as powerful as it may seem. Hackers can use software to fake *MAC addresses* easily.

4.3.5. *Disable SSID Broadcast*

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. At home, this roaming feature is unnecessary, and it increases the likelihood

NEWTON'S TELECOM DICTIONARY

NEWTON's TELECOM DICTIONARY

copyright © 2002 Harry Newton
email: Harry@HarryNewton.com
personal web site: www.HarryNewton.com
business web site: www.TechnologyInvestor.com

All rights reserved under International and Pan-American Copyright conventions, including the right to reproduce this book or portions thereof in any form whatsoever.

Published by CMP Books
An imprint of CMP Media LLC.
12 West 21 Street
New York, NY 10010

ISBN Number 1-57820-104-7

February 2002

Eighteenth Edition

For individual orders, and for information on special discounts for quantity orders, please contact:

CMP Books
6600 Silacci Way
Gilroy, CA 95020
Tel: 1-800-500-6875 or 408-848-3854
Fax: 408-848-5784
Web: www.cmpbooks.com
Email: cmp@rushorder.com

This book is also sold through www.Amazon.com, www.Fatbrain.com and www.BarnesAndNoble.com

Distributed to the book trade in the U.S. and Canada by Publishers Group West
1700 Fourth St., Berkeley, CA 94710

Manufactured in the United States of America

Ratchet Factor / Radio Frequency Interference Shield

Ratchet Factor The ratchet factor is part of CABS — Carrier Access Billing System. It is used to describe the apportionment of channels on a trunk between switched and facility usage. It's a percentage. Both switched usage and leased (facility) lines can be co-resident on the same trunk. The ratchet percentage refers to the percentage of the trunk dedicated to facility. Obviously, you would want to know this because switched usage is tariffed and facility usage is charged at flat contract rates.

Rack 1. An equipment rack. In our industry, the standard equipment rack is 19 inches (48.26 cm) wide at the front. Much equipment is designed to fit into a standard rack. A rack is typically made of aluminum or steel, onto which equipment is mounted. A rack is typically attached to a building ceiling or wall. Cables are laid in and fastened to the rack. Sometimes a rack is called a tray. What a rack is to equipment, so a frame is to wiring. See also Distribution Frame.

2. Rack (the digits), a term which implies the storing or registering of numerical data. See Register.

Rack Unit RU. Unit of measure of vertical space in an equipment rack. One rack unit is equal to 1.75 inches (4.45 cm).

Rackmount Designed to be installed in a cabinet, usually 19" wide.

RACON RADar transponder beaCON. Short-range navigation devices that provide target images on a ship's maritime navigation radar system. The transponder beacons transmit, either automatically or in response to a predetermined received signal, a pulsed radio signal with specific characteristics. RACONS generally operate in the 9300-9500 MHz band, and are used to identify specific locations such as hazards to navigation; think of them as replacements for lighthouses and you won't be far off. Most RACONS are operated by the U.S. Coast Guard. See also Radar.

Rad 1. The unit used to measure the absorption of ionizing radiation.

2. A British Term. Recorded Announcement Device, a device which automatically answers a line and delivers a pre-recorded message. Often used to tell a caller to a telebusiness unit that the call is in a queue and will be dealt with soon. More sophisticated RADs gather information, take messages or work in conjunction with interactive fax machines.

3. An abbreviation for Rapid Application Development. Most relate it to a quick programming environment.

Radar RADio Detection And Ranging. See Radar Detector.

Radar Detector Picture a trooper sitting in his car aiming his radar gun down the highway. The gun emits a beam of electrons at microwave frequency. Those beams bounce off approaching vehicles and reflect back to the trooper's radar at an altered frequency (the Doppler Effect). By measuring the change in frequency, the trooper calculates the speed of the oncoming vehicle. The trouble is the radar beam fans out like a searchlight. At a distance of 1,000 feet, the beam is about as wide as the highway itself. That makes it difficult for the trooper to know which vehicle he's tracking.

Also, his reading can be thrown off by any number of operating errors or by interference from power lines, neon lights or even the fan motor in the trooper's car. According to some estimates, Esquire Magazine reported, as many as 30% of all radar-generated speeding tickets were given in error. In 1979 a Miami TV station showed a police radar clocking a house going 28 miles per hour and a banyan tree doing 86! Radar detectors are very much like FM receivers. They can pick up radar signals more than a mile from the source. At that distance the beam is too weak to bounce all the way back to the trooper's car but strong enough to make the detector beep.

Radar Screen 1. A typically circular cathode ray tube (CRT) showing movement of the sweep of a swirling radar beam and the objects it hits.

2. A slang expression typically deriding something. "I'm studying the market for computers laptops, but Winbook is not on my radar screen." This typically means that Winbook, as a manufacturer, is so small they're not worth studying. To be on my radar screen means they're large enough and significant enough for me to study them.

Radial Acceleration The rate at which a track on an optical disc accelerates toward and away from the center, because it is not perfectly aligned or perfectly round.

Radials See Ground Radials.

Radiant Energy Energy as measured in joules which is transferred via electromagnetic waves. There is no associated transfer of matter. And typically the giver or energy and the receiver of energy are not touching.

Radiation Pattern The propagation characteristics of an antenna.

Radichio A forum established to promote common public key infrastructure standards for e-commerce using wireless phones.

Radio RF. System of communication employing electromagnetic waves propagated through

space. Because of their varying characteristics, radio waves of different lengths are employed for different purposes and are usually identified by their frequency. The shortest waves are the highest frequency, or numbers of cycles per second; the longest waves have the lowest frequency, or fewest cycles per second. In honor of the German radio pioneer Heinrich Hertz, his name has been given to the cycle per second (hertz, Hz); 1 kilohertz (KHz) is 1000 cycles per second, 1 megahertz (MHz) is 1 million cycles per second, and 1 gigahertz (GHz) is 1 billion cycles per second. Radio waves range from a few kilohertz to several gigahertz. Waves of visible light are much shorter. In a vacuum, all electromagnetic waves (but not audio waves) travel at a uniform speed of about 300,000 km (about 186,000 miles) per second.

Radio waves are used not only in radio broadcasting but in wireless devices, telephone transmission, television, radar, navigational systems, and communication. In the atmosphere the physical characteristics of the air cause slight variations in velocity, which are sources of error in such radio-communications systems as radar. Also, storms or electrical disturbances produce anomalous phenomena in the propagation of radio waves.

Because electromagnetic waves in a uniform atmosphere travel in straight lines and because the earth's surface is spherical, long distance radio communication is made possible by the reflection of radio waves from the ionosphere. Radio waves shorter than about 10 m (about 33 ft.) in wavelength — designated as very high, ultrahigh, and super high frequencies (VHF, UHF, and SHF) — are usually not reflected by the ionosphere; thus, in normal practice, such very short waves are received only within line-of-sight distances. Wavelengths shorter than a few centimeters are absorbed by water droplets or clouds; those shorter than 1.5 cm (0.6 in) may be absorbed selectively by the water vapor present in a clear atmosphere.

A typical radio-communication system has two main components, a transmitter and a receiver. The transmitter generates electrical oscillations at a radio frequency called the carrier frequency. Either the amplitude or the frequency itself may be modulated to vary the carrier wave. An amplitude-modulated signal consists of the carrier frequency plus two sidebands resulting from modulation. Frequency modulation produces more than one pair of sidebands for each modulation frequency. These produce the complex variations that emerge as speech or other sound in radio broadcasting, and in the alterations of light and darkness in television broadcasting.

Radio Broadcast Data System RBDS. A new system designed to let radio stations broadcasters send text messages, such as emergency warnings and traffic alerts to radios equipped with special LCD screens. The system is designed ultimately to replace the Emergency Broadcast System.

Radio Button 1. A call center term. A button used for selecting from a group of options that are mutually exclusive. As with a car radio, selecting a particular button deselects the previously selected button.

2. An World Wide Web term. Radio buttons are used in forms on Web sites to indicate a list of items. Only one button can be selected at one time.

Radio Common Carrier RCC. A common carrier engaged in Public Mobile Service, which also is not the business of providing land line local exchange telephone service. These carriers were once known as Miscellaneous Common Carriers.

Radio Communication Any telecommunication by means of radio waves.

Radio Frequency That group of electromagnetic energy whose wavelengths are between the audio and the light range. Electromagnetic waves transmitted usually are between 500 KHz and 300 GHz.

Radio Frequency Filter Fit A Northern Telecom Norstar device designed to alleviate problems associated with radio frequency interference that may be experienced when a headset or external Auxiliary Ringer is used with a telephone.

Radio Frequency Flooding Radio frequency flooding turns a telephone into a room listening device by transmitting a high power radio signal down a telephone line. The high power radio frequency is able to bypass the open hookswitch in the mouthpiece circuit. Room sounds cause the carbon microphone to modulate the RF signal. Radio frequency flooding is hard to implement but can only be detected by security professionals with the right equipment.

Radio Frequency Identity See RFID.

Radio Frequency Interface shield RFI. A metal shield enclosing the printed circuit boards of the printer or computer to prevent interference with radio and TV reception.

Radio Frequency Interference The disruption of radio signal reception caused by any source which generates radio waves at the same frequency and along the same path as the desired wave.

Radio Frequency Interference Shield RFI Shield. A metal shield enclosing the printed circuit boards of the printer or computer to prevent radio and TV inter-

WEBSTER'S
NEW
COLLEGE
DICTIONARY

Michael Agnes
EDITOR IN CHIEF

Copyright © 2007 by Wiley Publishing, Inc., Cleveland, Ohio

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-750-4470, or on the Web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Legal Department, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, 317-572-3447, fax 317-572-4447, or online at <http://www.wiley.com/go/permissions>.

Trademarks: Webster's New World, the Webster's New World logo, and We Define Your World are registered trademarks of Wiley Publishing, Inc., in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

Limit of Liability/Disclaimer of Warranty: While the publisher and the author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor the author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the U.S. at 800-762-2974, outside the U.S. at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books. For more information about Wiley products, visit our web site at www.wiley.com.

ISBN 978-0-470-17777-8

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

popular song, Vulgar Latin See also MUTUAL —ANT. unusual, exceptional

com-mon-able (-ə bəl) *adj.* [see prec., *n.* 1] 1 allowed to pasture on land owned by the village, town, etc. 2 held in common: said of land

com-mon-age (-ij) *n.* [see COMMON, *n.* 1 & -AGE] 1 the right to pasture on land owned by the village, town, etc. 2 the state of being held in common 3 public or common land 4 the common people; commonalty

com-mon-al-ity (kām'ən əl'ə tē) *n.* [ME *communalitie* < OFr *communalité*: see COMMUNAL & -TY¹] 1 the common people; commonalty 2 a sharing as of common features or characteristics

com-mon-alty (kām'ən əl' tē) *n., pl. -ties* [ME & OFr *communalte*: see COMMUNAL] 1 the common people; people not of the upper classes 2 a general body or group 3 a corporation or its membership

common carrier a person or company in the business of transporting passengers or goods for a fee, at uniform rates available to all persons

common cold COLD (*n.* 4)

common denominator 1 a common multiple of the denominators of two or more fractions [10 is a *common denominator* of $\frac{1}{2}$ and $\frac{1}{3}$] 2 a characteristic, element, etc. held in common

common difference the positive or negative constant added to each term in an arithmetic progression

com-mo-ner (-ər) *n.* [ME *communer* < *commun*, COMMON] 1 a person not of the nobility; member of the commonalty 2 [Brit.] at some universities, a student who does not have a scholarship and therefore pays for food (called *commons*) and other expenses

Common Era CHRISTIAN ERA

common fraction a fraction whose numerator and denominator are both whole numbers: cf. COMPLEX FRACTION, DECIMAL

common law the law of a country or state based on custom, usage, and the decisions and opinions of law courts: it is now largely codified by legislative definition: distinguished from STATUTE LAW

common-law marriage (kām'ən lə' tē) *Law* a marriage not solemnized by religious or civil ceremony but effected by agreement to live together as husband and wife and, usually, by the fact of such cohabitation

common logarithm *Math.* a logarithm having 10 for its base

com-mon-ly (kām'ən lē) *adv.* 1 in a common manner 2 in the usual course of events; ordinarily

common market 1 an association of countries formed to effect a closer economic union, esp. by means of mutual tariff concessions 2 [C- M-] the European Economic Community

common measure *Music* COMMON TIME

common multiple *Math.* a number or quantity evenly divisible by each element of a given set [12 is a *common multiple* of the set 2, 3, 4, 6]

common-place (-plās') *n.* [lit. transl. of *L locus communis*, Gr *koīnos topos*, general topic] 1 [Obs.] a passage marked for reference or included in a COMMONPLACE BOOK 2 a trite or obvious remark; truism; platitude 3 anything common or ordinary —*adj.* neither new nor interesting; obvious or ordinary —*SYN.* PLATITUDE, TRITE

commonplace book a book in which extracts, poems, aphorisms, etc. are copied down for future reference, often together with one's ideas and reflections

common pleas *Law* *1 in some States, a court having general and original jurisdiction over civil and criminal trials 2 in England, a former superior court with jurisdiction over civil suits

common room [Brit.] a room at a college used by faculty members or students for socializing, relaxation, etc.

com-mons (kām'onz) *pl.n.* [see COMMON] 1 the common people; commonalty 2 [often with *sing. u.*] a) the body politic that is made up of commoners b) [C-] HOUSE OF COMMONS 3 [often with *sing. u.*] a) food provided for meals in common for all members of a group b) a room, building, table, or tables where such food is served, as at a college c) an allowance or ration of food

***common school** a public elementary school

common sense ordinary good sense or sound practical judgment —*com'mon-sense' adj.* or *com'mon-sen'sical* (-sen'si kəl)

***common-situs picketing** (kām'ən sīt'əs) the picketing of an entire construction site by a union striking against a particular contractor or subcontractor working on only one section

***common stock** ordinary capital stock in a company without a definite dividend rate or the privileges of preferred stock, but usually giving its owner a vote at shareholders' meetings in proportion to the owner's holdings

common time *Music* a meter of four beats to the measure; 4/4 time

common-weal (kām'ən wēl') *n.* [ME *commun wele*: see COMMON & WEAL²] 1 the public good 2 [Archaic] a commonwealth

common-wealth (-wēlh') *n.* [ME *commun welthe*: see COMMON & WEALTH] 1 the people of a nation or state; body politic 2 a) a nation or state in which there is self-government; democracy or republic b) a federation of states [the *Commonwealth* of Australia] (*Commonwealth* is also the official designation of Puerto Rico, in its special status under the U.S. government) *3 loosely, any state of the U.S.; strictly, Ky., Mass., Pa., or Va., which were so designated in their first constitutions 4 a group of people united by common interests 5 [Obs.] the general welfare; commonweal —*the Commonwealth* 1 the government in England under the Cromwells and Parliament from 1649 to 1660: see also PROTECTORATE

2 association of independent nations (53 in September, 2004), all former components of the British Empire, united for purposes of consultation and mutual assistance: all members acknowledge the British sovereign as symbolic head of the association: in full **the Commonwealth of Nations**

Commonwealth Day a holiday celebrated on any of various days throughout the Commonwealth

Commonwealth of Independent States a loose confederation of countries that were part of the U.S.S.R.: it includes Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan: abbrev. *CIS*

com-mo-tion (kə mō'shən) *n.* [L *commotio* < *commotus*, pp. of *commovere*, to move, disturb < *com-*, together & *movere*, to MOVE] 1 violent motion; turbulence 2 a noisy rushing about; confusion; bustle 3 [Archaic] a civil uprising 4 [Archaic] mental agitation

com-move (kə mōōv') *vt. -moved', -mov'ing* [ME *commoeven* < OFr *commoveir* < L *commovere*: see prec.] to move strongly; agitate; disturb; excite

com-mu-nal (kə myōōn'əl, kām'yə nəl) *adj.* [ME & OFr < LL *communalis*] 1 of a commune or communes 2 of or belonging to the community; shared, or participated in, by all; public 3 designating or of social or economic organization in which there is common ownership of property —*com-mu-nal-i-ty* (kām'yōō nəl'ə tē) *n.* —*com'mu-nally adv.*

com-mu-nal-ism (-iz'əm) *n.* [Fr *communalisme*] 1 a theory or system of government in which communes or local communities, sometimes on an ethnic or religious basis, have virtual autonomy within a federated state 2 the conflicting allegiance resulting from this 3 communal organization —*com'mu-nal-ist n., adj.*

com-mu-nal-ize (-iz') *vt. -ized', -iz'ing* to make communal; make public property of —*com'mu-nal-i-za'tion n.*

Com-mu-nard (kām'yōō nārd') *n.* [Fr] 1 a person who supported or took part in the Commune of Paris (1871) 2 [C-] a resident or member of a COMMUNE² (sense 5)

com-mune¹ (kə myōōn'; for *n.* kām'yōōn') *vi. -muned', -mun'ing* [ME *communen* < OFr *comuner*, to make common, share < *comun* (see COMMON); also < OFr *communier*, to administer the sacrament < L *communicare*, to share (LL(Ec), to receive the sacrament): see COMMUNICATE] 1 a) to talk together intimately b) to be in close rapport [to *commune* with nature] 2 [Archaic] to receive Holy Communion —*n.* [Old Poet.] intimate conversation —*commune with oneself* to think; ponder

com-mune² (kām'yōōn') *n.* [ME & OFr < ML *communia*, orig. pl. of L *commune*, lit., that which is common < *communis*, COMMON] 1 [Archaic] the common people 2 a community; specif., a) a local body for self-government, esp. in medieval towns b) [Obs.] a mir 3 the smallest administrative district of local government in France, Belgium, and some other countries in Europe 4 a strictly organized collective farm, as in China *5 a small group of people living communally and sharing in work, earnings, etc. —*the Commune* 1 the revolutionary government of Paris from 1792 to 1794 2 the revolutionary government established in Paris from March 18 to May 28, 1871

com-mu-ni-cable (kə myōō'nī kə bəl) *adj.* [ME < LL *communicabilis*] 1 that can be communicated, as an idea 2 that can be transmitted, as a disease 3 [Archaic] talkative —*com-mu-ni-cabil'i-ty n.* —*com-mu-ni-cably adv.*

com-mu-ni-cant (kə myōō'nī kənt) *n.* [L *communicans*, prp.: see fol.] 1 a person who receives Holy Communion or belongs to a church that celebrates this sacrament 2 [Rare] a person who communicates information; informant —*adj.* [Rare] communicating

com-mu-ni-cate (kə myōō'nī kāt') *vt. -cat'ed, -cat'ing* [L *communicatus*, pp. of *communicare*, to impart, share, lit., to make common < *communis*, COMMON] 1 to pass along; impart; transmit (as heat, motion, or a disease) 2 to make known; give (information, signals, or messages) —*vi.* 1 to receive Holy Communion 2 a) to give or exchange information, signals, or messages in any way, as by talk, gestures, or writing b) to have a sympathetic or meaningful relationship 3 to be connected [the living room *communicates* with the dining room] —*com-mu-ni-ca'tor n.*

com-mu-ni-ca-tion (kə myōō'nī kā'shən) *n.* 1 the act of transmitting 2 a) a giving or exchanging of information, signals, or messages as by talk, gestures, or writing b) the information, signals, or message 3 close, sympathetic relationship 4 a means of communicating; specif., a) [pl.] a system for sending and receiving messages, as by telephone, telegraph, radio, etc. b) [pl.] a system as of routes for moving troops and materiel c) a passage or way for getting from one place to another 5 [often pl., with *sing. u.*] a) the art of expressing ideas, esp. in speech and writing b) the science of transmitting information, esp. in symbols

com-mu-ni-ca-tive (kə myōō'nī kāt'iv, -ni kə tiv) *adj.* 1 giving information readily; forthcoming 2 of communication —*com-mu-ni-ca-tive-ly adv.* —*com-mu-ni-ca-tive-ness n.*

com-mun-ion (kə myōōn'yən) *n.* [ME *communioun* < OFr *communio* < L *communio*, a sharing (in LL(Ec), the sacrament of communion) < *communis*, COMMON] 1 the act of sharing; possession in common; participation [a *communion* of interest] 2 the act of sharing one's thoughts and emotions with another or others; intimate converse 3 an intimate relationship with deep understanding 4 a group of Christians professing the same faith and practicing the same rites; denomination 5 [C-] a) a sharing in, or

See the inside front cover for pronunciation information.
The symbol * is used to mark terms of American origin.

widespread / wild carrot 1636

film made for projection on a screen much wider than it is; high: usually from a ratio of 1.66 to 1 up to 2.55 to 1 2 designating, of, or designed for a similar format for video, with a ratio of 1.78 to 1 or more [a *widescreen* TV set]

wide-spread (-sprəd) *adj.* spread widely; esp., a) widely extended [widespread arms] b) distributed, circulated, or occurring over a wide area or extent [widespread benefits, widespread rumors]

widgeon (wij'ən) *n., pl.* -eons or -eon *alt. sp.* of WIGEON

★ **widget** (wij'it) *n.* [altered < GADGET] any small, unspecified gadget or device, esp. one that is hypothetical

widow (wid'ō) *n.* [ME *widwe* < OE *widewe*, akin to Ger *witwe*, L *vidua* < IE **widhewo-*, separated < base **widh-*, to separate: see DIVIDE] 1 a woman who has outlived the man to whom she was married at the time of his death; esp., such a woman who has not remarried ★2 *Card Games* a number of cards dealt into a separate pile, typically for the use of the highest bidder 3 *Printing* an incomplete line, as that ending a paragraph, carried over to the top of a new page or column: generally avoided by rewriting copy to eliminate the line or fill it out ★4 [Informal] a woman whose husband is often away indulging in a specified hobby, sport, etc. [a golf widow] —*vt.* to cause to become a widow or widower: usually in the past participle [widowed by the war] —**wid'ow-hood** *n.*

wid-ow-bird (wid'ō bərd') *n.* [calque of Port *viuva*, widowbird, lit., widow < L *vidua*: see prec.:] from the resemblance of its dark plumage to a widow's mourning clothes] WHYDAH (BIRD)

wid-ower (wid'ō ər) *n.* [ME *widower*, extended < *wedow*, widower < OE *widewa*, masc. of *widewe*, WIDOW] a man who has outlived the woman to whom he was married at the time of her death; esp., such a man who has not remarried —**wid'ower-hood** *n.*

widow's cruse an apparently inexhaustible supply: 2 Kings 4:1-7
widow's mite a small gift or contribution freely given by one who can scarcely afford it: Mark 12:41-44

widow's peak a point formed by hair growing down in the middle of a forehead: formerly supposed to foretell early widowhood

★ **widow's walk** a platform with a rail around it, built onto the roof of some New England houses, as along the coast, formerly for observing ships at sea

width (width, with) *n.* [< WIDE, by analogy with LENGTH, BREADTH] 1 the fact, quality, or condition of being wide; wideness 2 the size of something in terms of how wide it is; distance from side to side 3 a piece of something of a certain width [two widths of cloth]

width-wise (-wīz') *adv., adj.* in the direction of the width: also **width'ways** (-wāz')

Wi-du-kind (vē'dū kint) 8th cent. A.D.; Saxon warrior: leader of the Saxons against Charlemagne

Wie-land (vē'lānt) 1 **Chris-top'h Mar-tin** (kris'tōf mār'tēn) 1733-1813; Ger. novelist, poet, & translator 2 **Heinrich (Otto)** 1877-1957; Ger. chemist

wield (wēld) *vt.* [ME *wielden*, blend of OE *wealdan* & *wieldan*, with form < the latter: akin to Ger *walten* < IE base **wal-*, to be strong > L *valere*, to be strong] 1 to handle and use (a tool or weapon), esp. with skill and control 2 to exercise (power, influence, etc.) 3 [Obs.] to govern or rule —*SYN.* HANDLE —**wield'er** *n.*

wieldy (wēldē) *adj.* **wield'i-er**, **wield'i-est** that can be wielded easily; manageable

Wien (vēn) *Ger. name for VIENNA*

★ **wie-ner** (vē'nər) *n.* [short for *wienerwurst* < Ger *Wiener wurst*, Vienna sausage] 1 a smoked sausage of beef or beef and pork, etc., enclosed in a membranous casing and made in cylindrical links a few inches long; frankfurter: the casing is now usually removed before packaging: also **wie'ner-wurst** (-wərst') 2 [Slang] a) WEENIE (sense 2) b) WEENIE (sense 3)

Wie-ner (vē'nər), **Nor-ber-t** (nōr'bərt) 1894-1964; U.S. mathematician & pioneer in cybernetics

Wie-ner schnit-zel (vē'nər shnit'səl) [Ger < *Wiener*, of Vienna + *schnitzel*, cutlet: see SCHNITZEL] a breaded veal cutlet with a garnish on it, esp. a lemon slice and rolled anchovy

wie-nie (vē'nē) *n.* 1 [Informal] WIENER (sense 1) 2 [Slang] a) WEENIE (sense 2) b) WEENIE (sense 3)

Wies-ba-den (vēs'bād'n) resort city in W Germany, on the Rhine: capital of the state of Hesse: pop. 270,000

Wie-sel (vē zel', wi-), **Elie** (el'ē) 1928-; U.S. writer, born in Romania

wife (wif) *n., pl.* **wives** (wivz) [ME < OE *wif*, woman, akin to Swed *viu*, Ger *weib* < ? IE base **wēip-*, to twist, turn, wrap, in sense "the hidden or veiled person"] 1 a woman: still so used in such compounds as *midwife*, *housewife*, etc. 2 a married woman; specif., a woman in her relationship to her husband —**take to wife** [Archaic] to marry (a specified woman) —**wife'hood** *n.* —**wife'less** *adj.* —**wife'ly** *adj.* —**li-er**, —**li-est**

★ **Wiffle ball** (wif'əl) [< *Wiffle*, a trademark] WHIFFLE BALL

★ **Wi-Fi** (wī'fī) [< *wi(reless) fi(delity)*, after HI-FI] service mark for a wireless local area network that uses radio waves to connect computers and other devices to the Internet: also written **WiFi'**

wig (wig) *n.* [shortened < PERIWIG] 1 a) a false covering of real or synthetic hair for the head, worn as part of a costume, to conceal baldness, etc. b) **TOUPEE** ★2 [Slang] variously, the hair, head, or mind —*vt.* **wigged**, **wig'ging** 1 to furnish with a

wig or wigs ★2 [Slang] a) to annoy, upset, anger, etc. b) to make excited, ecstatic, frenzied, crazy, etc. (often with *out*) 3 [Brit. Informal] to scold, censure, rebuke, etc.: archaic except as a verbal noun [gave him a *wigging*] —*vi.* [Slang] to be or become wigged, or upset, excited, crazy, etc.: often with *out*

wigan (wig'ən) *n.* [after fol., where first made] a canvaslike cotton cloth used to stiffen hems, lapels, etc.

Wigan (wig'ən) city in Greater Manchester, NW England: county district pop. 307,000

wi-geon (wij'ən) *n.* [prob. < MFr *vigeon* < L *vipio*, small crane, of Balearic orig.] any of certain wild freshwater ducks; esp., a) the Eurasian **wigeon** (*Anas penelope*), the male of which has a cream-colored crown and reddish-brown head and neck b) **BALDPATE**

Wig-gin (wig'in), **Kate Douglas** (born *Kate Smith*) 1856-1923; U.S. educator & writer of children's novels

wig-gle (wig'əl) *vt., vi.* —**gled**, —**gling** [ME *wigelen*, prob. < MDu & MLowG *wiggelen*, freq. of *wiggen*, to move from side to side, akin to OE *wegan*, to move: for IE base see WAG¹] to move or cause to move with short, jerky or twisting motions from side to side; wriggle shakily or sinuously —*n.* the act or an instance of wiggling

wig-gler (wig'lər) *n.* 1 a person or thing that wiggles 2 **WRIGGLER**

wig-gly (-lē) *adj.* —**glier**, —**gli-est** 1 that wiggles; wiggling 2 having a form that suggests wiggling; wavy [a *wiggly* line]

wiggy (wig'ē) *adj.* —**gier**, —**gi-est** 1 [Now Rare] a) wearing a wig b) pompously formal or elegant ★2 [Slang] wild, exciting, crazy, etc.

wight¹ (wit) *n.* [ME *wiht* < OE, akin to Ger *wicht*, creature, Goth *waihts*, thing < IE base **wekti-*, thing > OSlav *veštī*, thing] 1 [Obs.] a living being; creature 2 [Archaic] a human being; person: now sometimes used in a patronizing or commiserating sense

wight² (wit) *adj.* [ME *wiht* < ON *wigt*, neut. of *wigr*, skilled in arms, akin to OE *wigan*, to fight: for IE base see VICTOR] [Now Chiefly Dial.] strong, brisk, active, brave, etc.

Wight (wit), **Isle of** island in the English Channel, off the S coast of Hampshire, constituting a county of England: 147 sq mi (381 sq km); pop. 125,000

★ **wig-let** (wig'lit) *n.* a small wig; specif., a woman's hairpiece designed to supplement her own hair

Wig-ner (wig'nər), **Eugene Paul** 1902-95; U.S. physicist, born in Hungary

Wig-town (wig'tən) former county & former district of SW Scotland

wig-wag (wig'wag) *vt., vi.* —**wagged**, —**wag'ging** [< obs. *wig*, to move + WAG¹] 1 to move back and forth; wag 2 to send (a message) by waving flags, lights, etc. back and forth using a code —*n.* 1 the act of sending messages in this way 2 a message so sent —**wig'wag'ger** *n.*

★ **wig-wam** (wig'wām', -wōm') *n.* [< Abenaki *wikawam*, house] a traditional dwelling of Indian peoples of E North America, consisting typically of a dome-shaped framework of poles covered with rush mats or sheets of bark



CHEROKEE WIGWAM

Wil-ber-force (wil'bər fōrs'), **William** 1759-1833; Eng. statesman & vigorous opponent of slavery

Wil-ber-t (wil'bərt) *n.* [Ger *Willebert* < OHG *willeo*, WILL¹ + *beraht*, *berht*, BRIGHT] a masculine name

Wil-bur (wil'bər) *n.* [OE *Wilburh*: prob. a place name < **Wiligburh*, lit., willow town] a masculine name

★ **wil-co** (wil'kō) *interj.* [wilt(l) *colmply*] I will comply with your request: used in radio communication

wild (wild) *adj.* [ME *wilde* < OE, akin to Ger *wild*, prob. < IE base **wel-*, shaggy hair, unkempt > WOOL, VOLÉ¹] 1 living or growing in its original, natural state and not normally domesticated or cultivated [wild flowers, wild animals] 2 not lived in or cultivated; overgrown, waste, etc. [wild land] 3 not civilized; savage [a wild tribe] 4 not easily restrained or regulated; not controlled or controllable; unruly, rough, lawless, etc. [wild children] 5 characterized by a lack of social or moral restraint; unbridled in pursuing pleasure; dissolute, orgiastic, etc. [a wild rake, a wild party] 6 violently disturbed; turbulent; stormy [a wild seacoast] 7 in a state of intense excitement; specif., a) eager or enthusiastic, as with desire or anticipation [wild with delight] b) angered, frenzied, frantic, crazed, etc. [wild with desperation] 8 in a state of disorder, disarrangement, confusion, etc. [wild hair] 9 fantastically impractical; visionary [a wild scheme] 10 showing a lack of sound judgment; reckless; imprudent [a wild wager] 11 going wide of the mark aimed at; missing the target [a wild swing in boxing] 12 [Slang] extraordinary; remarkable [a wild success] 13 *Card Games* having any value specified by the holder: said of a card [deuces, when wild in poker, may be counted as aces, kings, etc.] —*adv.* in a wild manner; wildly; without aim or control [to shoot wild] —*n.* [usually pl.] a wilderness or wasteland —**run wild** to grow, exist, or behave without control —**the wild** the wilderness, nature, the out-of-doors, etc. —**wild'ly** *adv.* —**wild'ness** *n.*

★ **wild allspice** SPICEBUSH (sense 1)

wild boar a hog (*Sus scrofa*) living wild in Europe, Africa, and Asia, from which domestic hogs were derived

wild card 1 *Card Games* a card that has been declared wild ★2 *Sports* any of the teams, other than those that finish in first and sometimes second place, that qualify for a championship playoff 3 [Slang] an element that cannot be predicted or controlled

wild carrot a common, inedible, biennial weed (*Daucus carota*) of



ELIE WIESEL

MODERN
DICTIONARY
of
ELECTRONICS

SEVENTH EDITION

REVISED AND UPDATED

Rudolf F. Graf



Boston Oxford Auckland Johannesburg Melbourne New Delhi


Newnes is an imprint of Butterworth-Heinemann.


Copyright © 1999 by Rudolf F. Graf

 A member of the Reed Elsevier Group.

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

 Recognizing the importance of preserving what has been written, Butterworth-Heinemann prints its books on acid-free paper whenever possible.

 Butterworth-Heinemann supports the efforts of American Forests and the Global ReLeaf program in its campaign for the betterment of trees, forests, and our environment.

Library of Congress Cataloging-in-Publication Data

Graf, Rudolf F.
Modern dictionary of electronics / Rudolf F. Graf. — 7th ed.,
revised and updated.
p. cm.
ISBN 0-7506-9866-7 (alk. paper)
I. Electronics — Dictionaries. I. Title
TK7804.G67 1999
621.381'03 — dc21 99-17889
CIP

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

The publisher offers special discounts on bulk orders of this book.

For information, please contact:

Manager of Special Sales
Butterworth-Heinemann
225 Wildwood Avenue
Woburn, MA 01801-2041
Tel: 781-904-2500
Fax: 781-904-2620

For information on all Butterworth-Heinemann publications available, contact
our World Wide Web home page at: <http://www.bh.com>

10 9 8 7 6 5 4 3 2 1

Typeset by Laser Words, Madras, India
Printed in the United States of America

encountered in space. The principle involved in applying this hardening to the device is to change the characteristics of the component by the preapplication of gamma or neutron rays, so as to permanently fix its electrical characteristics. Entering the hostile space environment, the preconditioned or hardened components will no longer be affected by additional gamma and neutron ray exposure.

radiation hazard—1. The health hazard caused by exposure to ionizing radiation. 2. The possible harmful effect of powerful electromagnetic radiation on the human body or on electrical components.

radiation intensity—In a given direction, the power radiated from an antenna per unit solid angle in that direction.

radiation lobe—*See* lobe.

radiation loss—In a transmission system, the portion of the transmission loss due to radiation of the radio-frequency power.

radiation monitor—A device for determining amount of exposure to radioactivity. May be periodic or continuous, may monitor an area or an individual's breath, clothing, etc.

radiation pattern—1. *See* directional pattern. 2. For a fiber or bundle, a curve of the output radiation intensity plotted against the exit angle. 3. For an optical fiber or fiber bundle, the curve of the output radiation intensity plotted as a function of the angle between the optical axis of the fiber or bundle and a normal to the surface on which the radiation intensity is being measured, i.e., the output radiation versus direction of measurement relative to the optical axis.

radiation potential—The voltage required to excite an atom or molecule and cause the emission of one of its characteristic radiation frequencies.

radiation pyrometer—Also called a radiation thermometer. 1. A pyrometer that uses the radiant power from the object or source whose temperature is being measured. Within wide- or narrow-wavelength bands filling a definite solid angle, the radiant power impinges on a suitable detector—usually a thermocouple, thermopile, or a bolometer responsive to the heating effect of the radiant power, or a photosensitive device connected to a sensitive electric instrument. 2. A temperature-measuring device that uses an optical system to focus radiant energy from an object onto a detector. The detector converts this energy into an electrical signal that varies with the temperature of the object.

radiation report—A formal report of radiation measurements made by an engineer skilled in interference control techniques. Usually required by the FCC prior to certification of industrial heating equipment.

radiation resistance—1. The power radiated by an antenna, divided by the square of the effective antenna current referred to a specified point. 2. The resistance that, if inserted in place of the antenna, would consume the

same amount of power radiated by the antenna. 3. The characteristic of a material that enables it to retain useful properties during or after exposure to nuclear radiation.

radiation sensitivity—The ratio of photoinduced current to incident radiant energy, the latter measured at the plane of the lens of a photodevice.

radiation sickness—An illness resulting from exposure to radiation.

radiation survey meter—An instrument that measures instantaneous radiation.

radiation temperature—1. The temperature to which an ideal blackbody must be heated so it will have the same emissive power as a given source of thermal radiation. 2. The temperature of a complete radiator that has a total radiant emittance identical with that of an unknown source.

radiation thermocouple—A thermocouple that is used in infrared spectroscopy to detect a sample's infrared emittance. *See* thermocouple.

radiation thermometer—*See* radiation pyrometer.

radiation transfer index—Abbreviated RTI. A parameter that describes the transmission performance of optical fiber cables. It measures cable performance and includes both coupling and propagation losses.

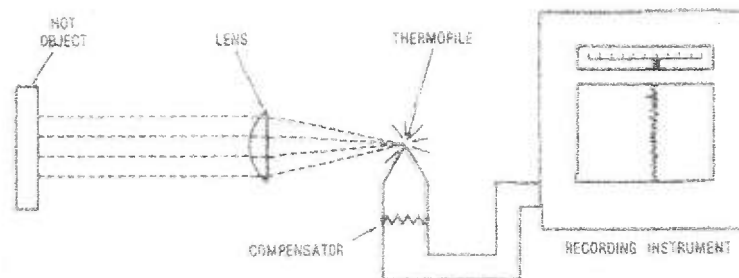
radiation trapping—That process whereby radiation spontaneously emitted by a volume of optical material is resonantly reabsorbed within the same volume before it escapes. This effect is manifested in a reduction in the observed rate of spontaneous emission from the material relative to the rate for single atoms or ions.

radiative equilibrium—The constant-temperature condition that exists in a material when the radiant energies absorbed and emitted are equal.

radiative recombination—In an electroluminescent diode in which electrons and holes are injected into the p-type and n-type regions by application of a forward bias, the recombining of injected minority carriers with the majority carriers in such a manner that the energy released on recombination results in the emission of photons of energy $h\nu$, which is approximately equal to the bandgap energy. Radiative recombination produces the light in a LED, which can be modulated for signaling purposes using optical fibers for transmission or integrated optical circuits for switching.

radiator—1. Any device that emits radiation. *See also* radiating element. 2. Any of the parts of an antenna that radiate electromagnetic waves, either directly into space or against a reflector.

radio—1. Communication by electromagnetic waves transmitted through space. 2. A general term, principally an adjective, applied to the use of electromagnetic waves between 10 kHz and 3000 GHz. 3. Electronic equipment for the wireless transmission or reception, or both, of electromagnetic waves, especially when used to transmit and receive sounds, activate a remote-control mechanism, etc.;



Radiation pyrometer.

a radio set. 4. The science of communicating over a distance by converting sounds or signals to electromagnetic waves and radiating these through space.

radioacoustic position finding—A method of determining distance through water. This is done by closing a circuit at the same instant a charge is exploded under water. The distance to the observing station can then be calculated from the difference in arrival times between the radio signal and the sound of the explosion.

radioacoustics—A study of the production, transmission, and reproduction of sounds carried from one place to another by radiotelephony.

radioactive—Pertaining to or exhibiting radioactivity.

radioactive isotope—*See* radioisotope.

radioactive series—A succession of radioactive elements, each derived from the disintegration of the preceding element in the series. The final element, known as the end product, is not radioactive.

radioactivity—A property exhibited by certain elements whose atomic nuclei spontaneously disintegrate and gradually transmute the original element into stable isotopes of that element or into another element with different chemical properties. The process is accompanied by the emission of alpha particles, beta particles, gamma rays, positrons, or similar radiations.

radioactivity detector—An instrument used to detect radioactive materials: alpha particles, or helium nuclei; beta particles, or free electrons; and gamma rays, which are X-rays of very short wavelength. They may be detected by their chemical effects, by ionization produced in gases at low pressure, and by their tracks formed in a cloud chamber.

radio altitude—*See* radar altitude.

radio approach aids—Equipment making use of radio to determine the position of an aircraft with considerable accuracy from the time it is in the vicinity of an airfield or carrier until it reaches a position from which a landing can be carried out.

radioastronomy—The branch of astronomy in which the radio waves emitted by certain celestial bodies are used for obtaining data about them.

radio attenuation—For one-way propagation, the ratio of the power delivered by the transmitter to the transmission line connecting it with the transmitting antenna, to the power delivered to the receiver by the transmission line connecting it with the receiving antenna.

radio beacon—Also called a radiophone or, in air operations, an aerophare. A radio transmitter, usually nondirectional, that emits identifiable signals for direction finding.

radio-beacon station—In the radionavigation service, a station whose emissions are intended to enable a mobile station to determine its bearing or direction in relation to the radio-beacon station.

radio beam—1. A radio wave in which most of the energy is confined within a relatively small angle. 2. A low-frequency radio transmitter used in direction finding for determining fixes and homing—a process of navigation whereby the pilot directs the aircraft toward the station to which it is tuned.

radio bearing—The angle between the apparent direction of a source of electromagnetic waves and a reference direction determined at a radio direction-finding station. In a true radio bearing, this reference direction is true north. Likewise, in a magnetic radio bearing, it is magnetic north.

radiobiology—The study of the effects on living matter (or substances derived therefrom) of high-energy radiation extending from X-rays to gamma rays, including

high energy beams of neutrons and charged particles, e.g., alpha particles, electrons, protons, deuterons.

radio breakthrough—The breakthrough of modulated radio signals into the channels of an audio amplifier due to the presence of high-level radio signal fields. The effect is that the base/emitter junction of the low-level input transistor rectifies the signals picked up by the wiring or circuit components, and the resulting audio is then handled by the amplifier in the ordinary way so that the radio program appears as a disconcerting background on the wanted source signal.

radio broadcast—A program of music, voice, and/or other sounds broadcast from a radio transmitter for reception by the general public.

radio broadcasting—*See* radio broadcast.

radio channel—A band of frequencies wide enough to be used for radiocommunication. The width of a channel depends on the type of transmission and on the tolerance for the frequency of emission.

radio circuit—1. A means for carrying out one radiocommunication at a time in either direction between two points. 2. A communication circuit between two points via radio. One circuit may be comprised of many channels, which may be used for teletypewriter, voice, or data communication.

radiocommunication—An overall term for transmission by radio of writing, signs, signals, pictures, and sounds of all kinds.

radiocommunication circuit—A radio system for carrying out one communication at a time in either direction between two points.

radiocommunication guard—A communication station designated to listen for and record transmission and to handle traffic on a designated frequency for a certain unit or units.

radio compass—*See* direction finder.

radio control—Remote control of apparatus by radio waves (e.g., model airplanes, boats).

radio deception—Sending false dispatches, using deceptive headings or enemy call signs, etc., by radio to deceive the enemy.

radio detection—Also called radio warning. Determining the presence of an object by radiolocation, but not its precise position.

radio detection and location—Use of an electronic system to detect, locate, and predict future positions of an earth satellite.

radio detection and ranging—Abbreviated radar. 1. Any of certain methods or systems of using beamed and reflected electromagnetic energy for detecting and locating objects; for measuring distance, velocity, or altitude; or for other purposes such as navigating, homing, bombing, missile tracking, mapping, etc. 2. In Federal Communications Commission regulations, a radiodetermination system based on the comparison of reference signals with radio signals reflected or retransmitted from the position to be determined. *See also* radar.

radio direction finder—A radio receiver that pinpoints the line of travel of the received waves.

radio direction finding—Abbreviated RDF. Radiolocation in which only the direction, not the precise location, of a source of radio emission is determined by means of a directive receiving antenna.

radio direction-finding station—A radiolocation station that determines only the direction of other stations, not their location, by monitoring their transmission.

radio Doppler—A device for determining the radial component of the relative velocity of objects by observing the frequency change due to such velocity.

radioelectrocardiogram—A broadcast electrocardiogram signal from the subject to a remote receiver. It

Modern Wireless Communications

Simon Haykin

*McMaster University
Hamilton, Ontario, Canada*

and

Michael Moher

*Space-Time DSP Inc.
Ottawa, Ontario, Canada*



Upper Saddle River, NJ 07458

Library of Congress Cataloging-in-Publication

Haykin, Simon S.
Modern wireless communications / Simon Haykin and Michael Moher.
p. cm.
Includes bibliographical references and index.
ISBN 0-13-022472-3
1. Wireless communication systems. 2. Spread spectrum communications. I. Moher,
Michael. II. Title

TK5103.2.H39 2003
621.382--dc22

2003061139

Vice President and Editorial Director, ECS: *Marcia J. Horton*
Vice President and Director of Production and Manufacturing, ESM: *David W. Riccardi*
Executive Managing Editor: *Vince O'Brien*
Managing Editor: *David A. George*
Production Editor: *Craig Little*
Director of Creative Services: *Paul Belfanti*
Art Director: *Jayne Conte*
Cover Designer: *Bruce Kenselaar*
Art Editor: *Greg Dulles*
Manufacturing Manager: *Trudy Piscioti*
Manufacturing Buyer: *Lisa McDowell*
Marketing Manager: *Holly Stark*



© 2005 Pearson Education, Inc.
Pearson Prentice Hall
Pearson Education, Inc.
Upper Saddle River, NJ 07458

All rights reserved. No part of this book may be reproduced in any form or by any means, without permission in writing from the publisher.

Pearson Prentice Hall® is a trademark of Pearson Education, Inc.

The author and publisher of this book have used their best efforts in preparing this book. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

ISBN 0-13-022472-3

Pearson Education Ltd., *London*
Pearson Education Australia Pty. Ltd., *Sydney*
Pearson Education Singapore, Pte. Ltd.
Pearson Education North Asia Ltd., *Hong Kong*
Pearson Education Canada, Inc., *Toronto*
Pearson Educación de Mexico, S.A. de C.V.
Pearson Education—Japan, *Tokyo*
Pearson Education Malaysia, Pte. Ltd.
Pearson Education, Inc., *Upper Saddle River, New Jersey*

328 Chapter 5 Spread Spectrum and Code-Division Multiple Access

3. This third-generation system also has several options in its scrambling and spreading strategy that will simplify the use of techniques such as *transmit diversity* and *multiuser detection*.

Problem 5.23 One advantage of higher spread bandwidths is their ability to handle higher information rates. Are there any other advantages? Are there any disadvantages? ■

5.16 THEME EXAMPLE 5: WI-FI

The abbreviation *Wi-Fi* stands for wireless fidelity and refers to wireless local area network technology for home, office, and transient users. For example, Wi-Fi base stations are being set up in locations such as airports, hotels, coffee shops, and other public areas to connect transient users. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wired Ethernet networks.

Wi-Fi networks comprise the radio technologies associated with IEEE Standards 802.11a, 802.11b, and 802.11g to provide secure, reliable, fast wireless connections. Equipment based on the IEEE 802.11a standard operates in the unlicensed 5-GHz radio band and can provide data rates up to 54 Mbps; this standard was discussed in Section 2.11. Equipment based on the IEEE 802.11b standard operates in the unlicensed 2.4-GHz radio bands and can provide data rates up to 11 Mbps. The more recent IEEE 802.11g standard provides up to 54 Mbps in the 2.4-GHz band. The objective of these standards is to furnish a service similar to the basic wired Ethernet networks available in many offices.

In this section, we will discuss the IEEE 802.11b component of Wi-Fi. This standard, which applies to operation in the unlicensed 2.4-GHz band, requires a minimum 10-dB processing gain by regulation. The minimum processing gain forces some spreading of the transmitted signal to reduce interference. There are, in fact, two spreading options provided in the standard for spread spectrum operation at 2.4 GHz: a direct-sequence approach and a frequency-hopped approach. We will describe the direct-sequence approach here.

Basic service with the 802.11b gives a data throughput rate of either 1 Mbps or 2 Mbps, depending upon whether BPSK or QPSK modulation is used. The packet structure is illustrated in Fig. 5.37.

The fields in this packet structure are defined as follows:

- *Sync*. This is part of the preamble and consists of 128 bits used for bit, frequency, and code synchronization. Sync is a field of all ones that has been scrambled.
- *SFD, or start-of-frame delimiter*. The rest of the preamble, this is a 16-bit field used for frame synchronization.

128 bits	16 bits	8 bits	8 bits	16 bits	8 bits	3 – 8191 bits
SYNC	SFD	SIGNAL	SERVICE	LENGTH	CRC	DATA PAYLOAD

FIGURE 5.37 Packet structure for IEEE 801.11b standard (adapted with permission, from IEEE).

DICTIONARY OF COMMUNICATIONS TECHNOLOGY

**Terms, Definitions and Abbreviations
Third Edition**

Gilbert Held

4-Degree Consulting
Macon, Georgia, USA

JOHN WILEY & SONS

Chichester · New York · Weinheim · Brisbane · Singapore · Toronto

First edition published in 1989 as *Data and Computer Communications*
Copyright © 1995, 1996, 1998 by John Wiley & Sons Ltd.
Baffins Lane, Chichester
West Sussex, PO 19 1UD, England

National 01243 779777
International (+44) 1234 779777

e-mail (for orders and customer service enquiries): cs-books@wiley.co.uk

Visit our Home Page on <http://www.wiley.co.uk> or <http://www.wiley.com>

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency, 90 Tottenham Court Road, London W1P 9HE, UK, without the permission in writing of the Publisher.

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Other Wiley Editorial Offices

John Wiley & Sons, Inc., 605 Third Avenue,
New York, NY 10158-0012, USA

WILEY-VCH Verlag GmbH
Pappelallee 3, D-69469 Weinheim, Germany

Jacaranda Wiley Ltd, 33 Park Road, Milton,
Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01,
Jin Xing Distripark, Singapore 129809

John Wiley & Sons (Canada) Ltd, 22 Worcester Road,
Rexdale, Ontario M9W 1L1, Canada

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0 471# 97516 8; 0 471 97517 6 (pbk)

Typeset in 10/12 pt Times by Laser Words, Madras, India.

Printed and bound in Great Britain from Post Script files by Bookcraft (Bath) Ltd

This book is printed on acid-free paper responsibly manufactured from sustainable forestry, in which at least two trees are planted for each one used for paper production.

R

R Resistance.

R interface In ISDN, the 2-wire physical interface which is used for a single customer termination between the TE2 and TA.

RACE Research and Development in Advanced Communications Technologies for Europe.

raceway A channel fabricated from steel or another metal, used for holding electrical wires and/or communications cables. Raceways are usually suspended within false ceilings from the above structural floor or under a raised floor.

RACF Resource Access Control Facility.

rack Same as cabinet.

rack-mount Designed to be installed in a cabinet.

radial wiring Wiring in which all cable runs from a common point to the point requiring service by the most direct means possible.

radiate To send out energy into space, as in the case of radio frequency (RF) waves.

radio channel A band of adjacent frequencies having sufficient width to permit its use for radio communications.

radio communication Communications by means of radio waves.

Radio Frequency (RF) That portion of the electromagnetic spectrum between 10 kHz and 300 MHz where propagation occurs without a guide in free space.

radio frequency amplification The amplification of a radio wave by a radio receiver before detection or by a radio transmitter before radiation.

Radio Frequency (RF) noise Noise caused by an electronic spark developed across relay contacts or electronic motor brush contacts. Usually suppressed by a resistor in series with a capacitor.

radio frequency spectrum The chart overleaf illustrates the radio frequency spectrum.

radio paging The use of radio waves to activate a paging device or beeper.

radio telephone Telephones which operate over radio frequencies.

radio wave Electromagnetic waves of frequencies between 30 kHz and 3 000 000 MHz, propagates without guide in free space.

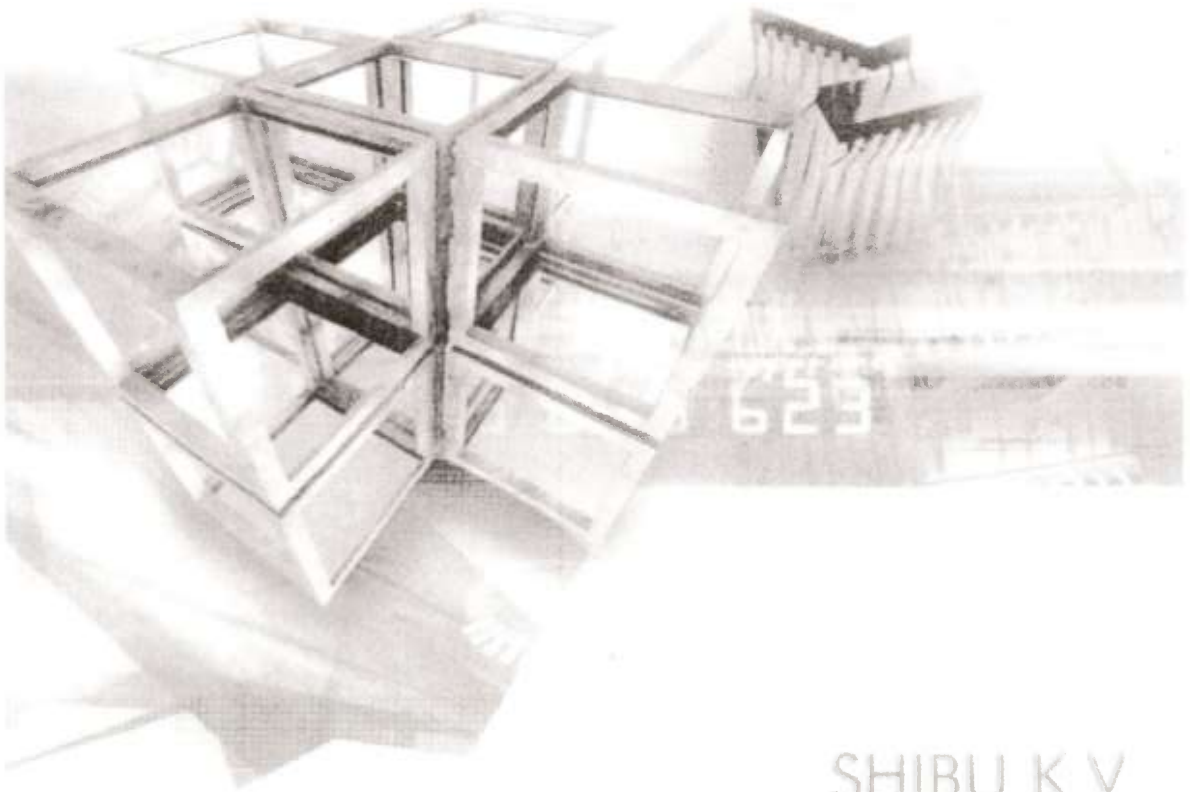
radio wave emission classification The International Telecommunications and Radio Conference (ITRC) which met in Cairo in 1938 devised the following classification for amplitude-modulated continuous waves:

Designator Type of emission

A0 Waves the successive oscillations of which are identical under fixed conditions.

A1 Telegraphy on pure continuous waves. A continuous wave that is keyed according to a telegraph code.

Introduction to EMBEDDED SYSTEMS



SHIBU K V



Tata McGraw Hill

Published by the Tata McGraw Hill Education Private Limited,
7 West Patel Nagar, New Delhi 110 008.

Copyright © 2009 by Tata McGraw Hill Education Private Limited.

No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication.

This edition can be exported from India only by the publishers,
Tata McGraw Hill Education Private Limited

ISBN (13): 978-0-07-014589-4

ISBN (10): 0-07-014589-X

Managing Director: *Ajay Shukla*

General Manager: Publishing—SEM & Tech Ed: *Vibha Mahajan*

Manager—Sponsoring: *Shalini Jha*

Associate Sponsoring Editor: *Nilanjan Chakravarty*

Development Editor: *Surbhi Suman*

Jr Executive—Editorial Services: *Dipika Dey*

Jr Manager—Production: *Anjali Razdan*

General Manager: Marketing—Higher Education: *Michael J Cruz*

Senior Product Manager: SEM & Tech Ed: *Biju Ganesan*

General Manager—Production: *Rajender P Ghansela*

Asst General Manager—Production: *B L Dogra*

Information contained in this work has been obtained by Tata McGraw Hill, from sources believed to be reliable. However, neither Tata McGraw-Hill nor its authors guarantee the accuracy or completeness of any information published herein, and neither Tata McGraw-Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that Tata McGraw-Hill and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.

Typeset at The Composers, 260, C.A. Apt., Paschim Vihar, New Delhi 110 063 and printed at
Lalit Offset Printer 219, FIE, Patpar Ganj, Industrial Area, Delhi-10092

Cover: SDR Printers

RAXLCRAFDDBYX

The McGraw-Hill Companies

for defining the rules of communication. The physical link works on the wireless principle making use of RF waves for communication. Bluetooth enabled devices essentially contain a Bluetooth wireless radio for the transmission and reception of data. The rules governing the Bluetooth communication is implemented in the 'Bluetooth protocol stack'. The Bluetooth communication IC holds the stack. Each Bluetooth device will have a 48 bit unique identification number. Bluetooth communication follows packet based data transfer.

Bluetooth supports point-to-point (device to device) and point-to-multipoint (device to multiple device broadcasting) wireless communication. The point-to-point communication follows the master-slave relationship. A Bluetooth device can function as either master or slave. When a network is formed with one Bluetooth device as master and more than one device as slaves, it is called a Piconet. A Piconet supports a maximum of seven slave devices.

Bluetooth is the favourite choice for short range data communication in handheld embedded devices. Bluetooth technology is very popular among cell phone users as they are the easiest communication channel for transferring ringtones, music files, pictures, media files, etc. between neighbouring Bluetooth enabled phones.

The Bluetooth standard specifies the minimum requirements that a Bluetooth device must support for a specific usage scenario. The Generic Access Profile (GAP) defines the requirements for detecting a Bluetooth device and establishing a connection with it. All other specific usage profiles are based on GAP. Serial Port Profile (SPP) for serial data communication, File Transfer Profile (FTP) for file transfer between devices, Human Interface Device (HID) for supporting human interface devices like keyboard and mouse are examples for Bluetooth profiles.

The specifications for Bluetooth communication is defined and licensed by the standards body 'Bluetooth Special Interest Group (SIG)'. For more information, please visit the website www.bluetooth.org.

2.4.2.6 Wi-Fi Wi-Fi or Wireless Fidelity is the popular wireless communication technique for networked communication of devices. Wi-Fi follows the IEEE 802.11 standard. Wi-Fi is intended for network communication and it supports Internet Protocol (IP) based communication. It is essential to have device identities in a multipoint communication to address specific devices for data communication. In an IP based communication each device is identified by an IP address, which is unique to each device on the network. Wi-Fi based communications require an intermediate agent called Wi-Fi router/Wireless Access point to manage the communications. The Wi-Fi router is responsible for restricting the access to a network, assigning IP address to devices on the network, routing data packets to the intended devices on the network. Wi-Fi enabled devices contain a wireless adaptor for transmitting and receiving data in the form of radio signals through an antenna. The hardware part of it is known as Wi-Fi Radio.

Wi-Fi operates at 2.4GHz or 5GHz of radio spectrum and they co-exist with other ISM band devices like Bluetooth. Figure 2.33 illustrates the typical interfacing of devices in a Wi-Fi network.

For communicating with devices over a Wi-Fi network, the device when its Wi-Fi radio is turned ON, searches the available Wi-Fi network in its vicinity and lists out the Service Set Identifier (SSID) of the available networks. If the network is security enabled, a password may be required to connect to a particular SSID. Wi-Fi employs different security mechanisms like Wired Equivalency Privacy (WEP) Wireless Protected Access (WPA), etc. for securing the data communication.

Wi-Fi supports data rates ranging from 1Mbps to 150Mbps (Growing towards higher rates as technology progresses) depending on the standards (802.11 a/b/g/n) and access/modulation method. Depending on the type of antenna and usage location (indoor/outdoor), Wi-Fi offers a range of 100 to 300 feet.

**Communications
Standard
Dictionary**

Second Edition

Martin H. Weik, DSc.
Dynamic Systems, Inc.
Reston, Virginia



VAN NOSTRAND REINHOLD
New York

Copyright © 1989 by Van Nostrand Reinhold

Library of Congress Catalog Card Number: 87-31582
ISBN 0-442-20556-2

All rights reserved. Certain portions of this work © 1982 by Van Nostrand Reinhold.
No part of this work covered by the copyright hereon may be reproduced or used in any
form or by any means—graphic, electronic, or mechanical, including photocopying, recording,
taping, or information storage and retrieval systems—without permission of the publisher.

Printed in the United States of America

Published by Van Nostrand Reinhold
115 Fifth Avenue
New York, New York 10003

Van Nostrand Reinhold International Company Limited
11 New Fetter Lane
London EC4P 4EE, England

Van Nostrand Reinhold
480 La Trobe Street
Melbourne, Victoria 3000, Australia

Macmillan of Canada
Division of Gage Publishing Limited
164 Commander Boulevard
Agincourt, Ontario M1S 3C7, Canada

15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

Weik, Martin H.

Communications standard dictionary.

1. Telecommunication—Dictionaries. 2. Communication
—Dictionaries. I. Title.

TK5102.W437 1988 001.5'03'21 87-31582
ISBN 0-442-20556-2

178 common-user communication service

common-user communication service. A *communication service* established to provide *communication service* and support to a group of *users* that have a common interest, such as a group of users in a single organization. Also see *dedicated communication service*.

common-user network. A *network* in which *circuits* or *channels* are allocated to furnish *communication paths* between *switching centers* to provide *communication facilities* and *services* on a common basis to all connected *stations* or *users*. Synonymous with *general-purpose network*.

common-user service. A type of *communication service* that is provided by a *common-user network*.

communication. 1. The transfer of *information* between a *source* (*transmitter, light source*), and a *sink* (*receiver, photodetector*) over one or more *channels* in accordance with a *protocol* and in a manner suitable for interpretation or comprehension by the receiver. 2. A method or means of conveying *information* of any kind from one person or place to another, except by direct unassisted conversation or correspondence. See *code-independent data communication; data communication; dedicated communication; duplex communication; ground-to-air communication; long-haul communication; one-way communication; public relations communication; radio-telegraph communication; radio-telephone communication; surface-to-air communication; teletypewriter communication; two-way-alternate communication; two-way-simultaneous communication*. Synonymous with *message*.

communication adapter. See *integrated communication adapter*.

communication agency. A *facility* that uses personnel and *equipment* to provide *communication services* to public or private organizations or to the general public, and performs other communication-related functions such as allowing communication-related charges to be appended to *telephone bills*, such as for the sending of *telegrams* or flowers or the purchasing of theater tickets.

communication axis. See *signal-communication axis*.

communication base section. See *base communications*.

communication board. 1. A *printed circuit (PC) board* that is placed in each of two or more *computer systems* or other *systems*, such as *microcomputer* or *personal computer (PC) systems*, and used to enable the systems to share or use each other's capabilities, i.e., use each other's *storage, printers, monitors, PC boards*, et al., thus forming a kind of *local-area network*, e.g., 3COM's Etherlink PC board or a built-in *modem printed circuit board*. 2. A *printed circuit (PC) board* that enables one *computer* to *communicate* with another, e.g., a *gateway board*.

communication cable. See *intrusion-resistant communication cable*.

such a manner that the energy released upon recombination results in the *emission* of *photons* of energy hf , which is approximately equal to the *band-gap energy*. *Radiative recombination* produces the *light* in an *LED*, which can be *modulated* for *signaling* purposes using *optical fibers* for *transmission* or *integrated optical circuits* for *switching*. Also see *nonradiative recombination*.

radiator. A device that *emits radiation*, such as a *radio* or *television transmitting antenna*, a *light source*, or *radioactive material*. See *isotropic radiator*.

radii loss. See *mismatch-of-core-radii loss*.

RADINT. *Radar intelligence*.

radio. 1. A method of *communicating* over a distance by *modulating electromagnetic waves* by means of an *intelligence-bearing signal* and *radiating* these modulated waves by means of a *transmitter* and an *antenna*. 2. A device, or pertaining to a device, that *transmits* or receives *electromagnetic waves* in the *frequency bands* that are between 10 *KHz* and 3000 *GHz*. See *cellular radio*; *combat-net radio*; *high-frequency radio*; *teleprinter-on-radio*.

radioactive atom. An atom whose *electrons*, *photons*, or other atomic *components* are undergoing *energy band transitions* that result in *absorption* or *emission* of high-energy *quanta*.

radioactive particle. A particle of matter that is attached to *radioactive atoms* and therefore seems to be experiencing *radioactivity* itself.

radioactivity. The activity of *radioactive atoms*, such as the *emission* or *absorption* of *gamma radiation*, *x rays*, or other high-energy *quanta*.

radio altimeter. A device that is used on board an aircraft and that makes use of the *reflection* of *radio waves* from the ground to determine the height of the aircraft above the ground. The equipment uses *beamed* and *reflected electromagnetic energy* to measure height above ground by means of a *phase displacement* between the *transmitted radio signal* and its *echo* reflected from the ground. The altitude in *meters* is 150 *m/μs* of phase displacement.

radio-and-wire integration (RWI). See *radio-wire integration*.

radio-approach aid. Equipment that makes use of *radio* to determine the position of an aircraft with considerable *accuracy* from the time it is in the vicinity of an airfield until it reaches a position from which landing can be carried out by direct visual means.

radio astronomy. Astronomy that is based on the *reception* of *radio waves* of *cosmic origin*.

radio-astronomy service. A service that involves the use of *radio astronomy*.

9th Circuit Case Number(s): 11-17483

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on February 8, 2012.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

s/ Deborah Grubbs

Deborah Grubbs