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

GOOGLE'S PETITION FOR REHEARING AND REHEARING EN BANC

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

Seth P. Waxman
WILMER CUTLER PICKERING HALE
AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, D.C. 20006
(202) 663-6800

Counsel for Petitioner/Appellant Google Inc.

September 24, 2013

TABLE OF CONTENTS

Page

RULE 35(B)(1) STATEMENT 1

SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. The Panel's Novel Definition Of "Radio Communication" Is Contrary To The Wiretap Act And Creates Uncertainty About The Legal Status Of Numerous Technologies 4

II. The Panel's Ruling That Unencrypted Wi-Fi Transmissions Are Not "Readily Accessible" Improperly Resolved A Factual Issue That Was Not Before The Court 12

CONCLUSION 18

ADDENDUM A

ADDENDUM B

TABLE OF AUTHORITIES

CASES

Allen B. Dumont Labs. v. Carroll,
184 F.2d 153 (3d Cir. 1950) 9

DirecTV, Inc. v. FCC,
110 F.3d 816 (D.C. Cir. 1997) 9

In re Innovatio IP Ventures, LLC Patent Litig.,
886 F. Supp. 2d 888 (N.D. Ill. 2012) 16

Lee v. City of Los Angeles,
250 F.3d 668 (9th Cir. 2001) 15

LVRC Holdings LLC v. Brekka,
581 F.3d 1127 (9th Cir. 2009) 12

On/TV of Chicago v. Julien,
763 F. 2d 839 (7th Cir. 1985) 9

Rodriguez v. Widener Univ.,
No. 13-1336, 2013 WL 3009736 (E.D. Pa. June 17, 2013) 14

Singleton v. Wulff,
428 U.S. 106 (1976) 15

United States v. Ahrndt,
475 F. App'x 656 (9th Cir. 2012) 17

United States v. Hall,
488 F.2d 193 (9th Cir. 1973) 14, 15

Winchester TV Cable Co. v. FCC,
462 F.2d 115 (4th Cir. 1972) 8-9

ADMINISTRATIVE PROCEEDINGS

In re Amendment of Parts 2, 73, & 76,
101 F.C.C.2d 973 (1985) 6

In re Petition by Hawaiian Tel. Co.,
16 F.C.C.2d 308 (1969) 9

STATUTES

18 U.S.C. § 2510(1) 7, 10

18 U.S.C. § 2510(16) 5, 6, 9, 11

18 U.S.C. § 2510(18) 10

18 U.S.C. § 2511(2)(g)(i) ..... *passim*

18 U.S.C. § 2511(2)(g)(ii) ..... *passim*

18 U.S.C. § 2511(2)(g)(iii) 10

47 U.S.C. § 153(40) 7

LEGISLATIVE HISTORY

H.R. Rep. No. 99-647 (1986) 6, 8, 11

S. Rep. 99-541 (1986) 5, 6, 12

MISCELLANEOUS

A.J. Meadows *et al.*, Dictionary of New Information Technology 151 (Kogan Page 1982) [Addendum A, Tab 4] 7

Apple, About Wireless Diagnostics [Addendum B, Tab 4] 16, 17

Avinash Kak, Purdue University College of Engineering, *Lecture 23: Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing* (Apr. 2, 2013) 17

Cambridge Dictionary of Science and Technology 737 (Cambridge University Press 1988) [Addendum A, Tab 5] 7

Charles Waltner, *Long Range Wifi: Filling the Gaps in the Broadband Map*, The Network: Cisco's Technology News Site (Oct. 18, 2010) [Addendum B, Tab 2] 15-16

Cisco IOS Embedded Packet Capture [Addendum B, Tab 3] 16, 17

Dennis Longley & Michael Shain, Dictionary of Information Technology 284 (John Wiley & Sons 1982) [Addendum A, Tab 3] 7

FCC, Consumer Guide, Interception & Divulgence of Radio Communications [Addendum B, Tab 1] 9

The Focal Illustrated Dictionary of Telecommunications 510 (Focal Press 1999) [Addendum A, Tab 10] 7

Frederic Swing Crispin, Dictionary of Technical Terms 322 (8th Ed. Bruce Publ'g Co. 1948) [Addendum A, Tab 2] 7

Gilbert Held, Dictionary of Communications Technology 437 (3d Ed. John Wiley & Sons 1998) [Addendum A, Tab 8] 7

McGraw-Hill Dictionary of Scientific and Technical Terms 1552 (Sybil P. Parker Ed., 4th Ed. McGraw-Hill 1989) [Addendum A, Tab 6] 7

Microsoft, How to Capture Network Traffic with Network Monitor [Addendum B, Tab 5] 16, 17

Nelson M. Cooke & John Markus, Electronics Dictionary 303 (1st Ed. McGraw-Hill 1945) [Addendum A, Tab 1] 7

Newton's Telecom Dictionary 856 (26th ed. Flatiron Publishing 2011)..... 8

Newton's Telecom Dictionary 458 (2d Ed. Telecom Library 1989) [Addendum A, Tab 7] 7

Newton's Telecom Dictionary 948 (26th Ed. Flatiron Publishing 2011) [Addendum A, Tab 11] 7

Response to Defendant Google, Inc.'s Motion To Dismiss Consolidated Class Action Complaint (Jan. 25, 2011) ECF No. 64, at 8-9 [Addendum B, Tab 6] 14

Rudolf F. Graf, Modern Dictionary of Electronics 616 (7th Ed. Newnes 1999) [Addendum A, Tab 9] 7

RULE 35(B)(1) STATEMENT

This case warrants rehearing because the panel overlooked key points of law and fact in the course of resolving incorrectly two exceptionally important questions about the Wiretap Act.

First, Google seeks panel rehearing and/or rehearing en banc of the panel's holding that a "radio communication" for purposes of the Wiretap Act is limited to "predominantly auditory broadcast[s]." Op. 17. That ruling is squarely at odds with the Wiretap Act. The panel overlooked that the Act itself expressly identifies many kinds of "radio communications" that are *not* predominantly auditory. The panel's novel definition also will undermine the integrity of the statute. It removes the specific legal protections that Congress intended to provide for various radio-based transmissions—including television broadcasts—thereby raising questions about the lawfulness of everyday behavior.

Second, Google seeks panel rehearing and/or rehearing en banc on the panel's ruling that unencrypted Wi-Fi broadcasts are not "readily accessible to the general public" under the ordinary meaning of that phrase. Op. 32-35. In making that seemingly categorical determination, the panel overlooked that this case is here on interlocutory review of a ruling on a motion to dismiss. It was manifest error to resolve a contested question of fact when the parties had no opportunity to develop a record, let alone present one to the district court. The panel's ruling on an issue that was neither addressed below nor raised on appeal de-

prived Google of its right to be heard, rests on mistaken factual premises, and casts a legal cloud over everyday activities involving Wi-Fi networks.

SUMMARY OF ARGUMENT

1. The term "radio communication" is critical to the Wiretap Act. Congress' use of that term was intended to establish clear rules about which transmissions are available for the public to receive. And when it was added to the Wiretap Act in 1986, "radio communication" had for decades carried a straightforward meaning in federal law and industry practice: any communication transmitted using radio waves. The panel swept aside that broadly accepted definition and instead limited "radio communication" to "predominantly auditory broadcast[s]." Op. 16-17. Rehearing of that ruling is warranted because the panel's novel interpretation is demonstrably wrong and will create legal uncertainties about a number of widely used technologies.

The panel's definition is refuted by the Wiretap Act itself, which expressly classifies various transmissions as "radio communication" that are not predominantly auditory. The panel suggested that "radio communication" could not include all communications carried by radio because that would sweep in television broadcasts, which the panel thought contrary to ordinary usage. Op. 14. But telecommunications law has *always* treated television transmissions as radio communications. Anyone in the field, and certainly Congress, would have under-

stood that. Indeed, it is precisely because broadcast television is a "radio communication" under the Wiretap Act that the public's right to acquire those signals is guaranteed.

This error is exceptionally important. It promises to have a substantial, long-lasting effect on the application of the Wiretap Act in an environment of rapid technological change. If allowed to stand, the panel's ruling will create confusion about the Wiretap Act's prohibitions, threaten the development of new radio-based technologies, and raise questions about whether activities that Congress intended to protect may now be deemed unlawful.

2. The second question that merits rehearing is the panel's apparently categorical holding that data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i). Because this case came to this Court on interlocutory review of the partial denial of a motion to dismiss, the panel had no basis to decide that question of fact. The district court was required to limit itself to the complaint's allegations, and it did exactly that. In going beyond the pleadings to rule on this question, the panel effectively granted partial summary judgment to the plaintiffs on Google's motion to dismiss. And it did so based on an incorrect understanding of extra-record facts that have yet to be tested in any adversarial process.

The panel's error would warrant correction even if it only deprived Google of its right to develop a factual record and be heard on this point.

But the harmful consequences of the panel's ruling will be far-reaching, creating significant uncertainty about the legal status of ordinary activities involving Wi-Fi networks. By categorically declaring that data transmitted via unencrypted Wi-Fi are not readily accessible, the panel has potentially made it unlawful to use ubiquitous tools that help protect Wi-Fi systems and raised questions about whether the routine operation of Wi-Fi-connected devices is now unlawful. Rehearing is warranted to limit this Court's decision to the issues properly before it and to ensure that important questions about the uses of Wi-Fi today and in the future are resolved based on a proper record.

ARGUMENT

I. The Panel's Novel Definition Of "Radio Communication" Is Contrary To The Wiretap Act And Creates Uncertainty About The Legal Status Of Numerous Technologies

The issue Google presented in this interlocutory appeal was how to define "radio communication" under the Wiretap Act. Google Br. at 2. Google argued that Congress intended to give that term the meaning it has always had—any information transmitted by radio waves. The panel rejected that definition and instead concluded that the Wiretap Act limits a "radio communication" to a "predominantly auditory broadcast." Op. 16-17. That is clear error. It is contrary to the Wiretap Act's own terms. It is contrary to the way "radio communication" was universally understood in the communications industry at the time Congress

amended the Wiretap Act to add "radio communication." It is contrary to many contemporary common uses of the term "radio." And it undermines the Act, creating uncertainty where Congress intended clarity.

A. The panel arrived at its restrictive definition entirely on its own. Neither the district court, the plaintiffs, nor any case had even suggested the unprecedented interpretation the panel devised. Google thus did not have occasion to address it before now.

The panel's limitation of "radio communication" to "predominantly auditory broadcast[s]" is expressly refuted by the text and legislative history of the Wiretap Act. We know this because two provisions in the Act—§ 2510(16), which defines "readily accessible to the general public" specifically "with respect to a radio communication," and § 2511(2)(g)(ii), which identifies types of "radio communication[s]" that are lawful to intercept—expressly list examples of transmissions that constitute "radio communication[s]." Many of the listed forms of "radio communication"—apparently overlooked by the panel—are clearly not "predominantly auditory." These include:

- **Display paging systems.** These are pagers "equipped with screens that can display visual messages." S. Rep. 99-541, at 2 (1986). The Wiretap Act protects their transmissions by treating them as "radio communication[s] … transmitted over a communication system provided by a common carrier." 18 U.S.C. § 2510(16)(D). *See* S. Rep. 99-541, at 15.

- **Data carried on the Vertical Blanking Interval (VBI) of a television signal.** This includes "textual and graphic infor-

mation intended for display on viewing screens." *In re Amendment of Parts 2, 73, & 76*, 101 F.C.C.2d 973, 973-74 (1985). VBI data, which is not auditory (and is not subsidiary to a predominantly auditory broadcast), is classified as a "radio communication" under § 2510(16)(C) of the Act. S. Rep. 99-541, at 15.

- **Television broadcasts.** As discussed below, Congress clearly understood broadcast television as a "radio communication" permitted to be intercepted under § 2511(2)(g)(ii)(I). *See* H.R. Rep. No. 99-647, at 37, 42 n.86 (1986).

- **Satellite (including satellite television) transmissions.** The Wiretap Act protects satellite broadcasts by treating them as "radio communication[s]" … transmitted on frequencies allocated under part 25 … of the Rules of the Federal Communications Commission." 18 U.S.C. § 2510(16)(E); *see* H.R. Rep. 99-647, at 38.

- **Private operational fixed microwave services.** These services "carr[y] confidential business data [or] transmit certain types of television material." H. Rep. 99-647, at 38. They are classified as radio communications under § 2510(16)(E), which covers "radio communication[s] … transmitted on frequencies allocated" under various FCC rules.

- **Video transmissions from news reporters in the field.** Congress understood these transmissions, though not predominately auditory, as "radio communication[s]" covered by § 2510(16)(E). *See* H.R. Rep. 99-647, at 38.

These examples show that, contrary to the panel's conclusion, the term "radio communication" in the Wiretap Act is not limited to predominantly auditory transmissions. Rather, what these disparate types of communications have in common is that they use radio waves to transmit information. Indeed, when Congress wanted to limit a term in the Wiretap Act based on the nature of what is transmitted, rather than

how it is transmitted, it did so expressly. *See* 18 U.S.C. § 2510(1) (defining "wire communication" to require an "aural transfer" of information.

The panel's definition also conflicts with the settled meaning of "radio communication" in communications law and practice. When Congress added "radio communication" to the Wiretap Act, that term had been understood for decades to mean any transmissions made via radio waves. That was how a long line of dictionaries had defined it (*see* Addendum A) (definitions of "radio communication" starting in 1945)) and how the Communications Act had used it since 1934, 47 U.S.C. § 153(40). It thus is not surprising that Congress saw no need to define the term in the Wiretap Act; its meaning was perfectly clear to everyone in the communications world.[1]

The panel's decision to limit "radio communication" to "predominantly auditory broadcasts" is also at odds with how the term "radio" is used in everyday parlance. Various technologies regularly described as "radio" are not predominantly auditory. For example, "packet radio" in-

[1] The panel suggested that because the Wiretap Act does not expressly incorporate the Communications Act's definition of "radio communication"—while it does incorporate the Communications Act's definition of another term—Congress must have intended "radio communication" to mean something different. Op. 25-26. The panel has it backward. Congress was well aware of how the Communications Act treated key terms and thus how a term such as "radio communication" would be understood. If it intended to depart from that accepted definition, Congress surely would have said so, rather than leaving the public to guess at what it really meant.

volves "the transmission of data over radio." Newton's Telecom Dictionary 856 (26th ed. Flatiron Publishing 2011). This technology—and similar ones, such as "Radio Frequency IDentity ("RFID"), which uses radio waves … to send data," *id.* at 789, 979—demonstrates that "radio" in common usage extends well beyond *audio* transmissions.

B. As its central reason for departing from the settled meaning of "radio communication," the panel suggested that "[o]ne would not ordinarily consider, say television a form of 'radio communication.'" Op. 14. That is wrong.

Congress itself considered television a form of "radio communication" when it wrote the Wiretap Act. Section 2511(2)(g)(ii) lists "some of the more common radio services" that are legal to intercept. H.R. Rep. No. 99-647, at 42. The first is "any radio communication which is transmitted … by any station for the use of the general public." 18 U.S.C. § 2511(2)(g)(ii)(I). This provision was *specifically intended* to cover television broadcasts. H.R. Rep. No. 99-647, at 42 n.86 ("…all communications transmitted for the use of the general public, including radio and television broadcast signals…"); *id.* at 37 (provision covers transmission of "closed-captioning of television programming for the hearing-impaired"). Congress' understanding that television was "radio communication" reflected the common usage. *E.g.*, *Winchester TV Cable Co. v. FCC*, 462 F.2d 115, 118 n.9 (4th Cir. 1972) ("Radio communica-

tion, of course, includes television."). That is illustrated in caselaw[2] and FCC guidelines,[3] and indeed even the Plaintiffs acknowledge "that television broadcasts are 'traditional radio services.'" Op. 7 n.3.

In short, there is nothing to suggest that Congress intended the established term "radio communication" to mean anything other than what it had meant for decades. All of the evidence shows otherwise.

C. The panel's erroneous definition of "radio communication" warrants rehearing not merely because it is wrong, but also because it undermines the integrity of the Wiretap Act.

The term "radio communication" does considerable work in the statute. It is the means by which Congress specified that it is always permissible to receive certain communications (18 U.S.C. § 2511(2)(g)(ii)) while other communications should not be intercepted (*id.* § 2510(16)(A)-(E)). The panel's unprecedentedly narrow interpretation undoes that structure, and thus unsettles the legal status of nu-

---

[2] *See, e.g.*, *On/TV of Chicago v. Julien*, 763 F. 2d 839, 842 (7th Cir. 1985) ("'Radio communication' as defined in [the Communications Act] has been construed to include television transmissions"); *Allen B. Dumont Labs. v. Carroll*, 184 F.2d 153, 155 (3d Cir. 1950) (same); *DirecTV, Inc. v. FCC*, 110 F.3d 816, 821 (D.C. Cir. 1997) (satellite television "is a radio communication service").

[3] *In re Petition by Hawaiian Tel. Co.*, 16 F.C.C.2d 308, 310 (1969) ("A [television] broadcast signal is a radio communication…"); FCC, Consumer Guide, Interception & Divulgence of Radio Communications, (Addendum B, Tab 1) ("[R]adio communications include transmissions of a local radio or television broadcast station…").

merous radio-based transmissions. For example, Congress sought to ensure that viewing broadcast-television transmissions would always be permissible despite the Wiretap Act's general prohibitions on interception by classifying them as "radio communication[s]" transmitted "by any station for use of the general public." *Id.* § 2511(2)(g)(ii)(I). The panel's determination that television transmissions are *not* "radio communications," Op. 16, strips television viewing of that categorical legal protection. That directly contradicts what Congress intended.[4]

Similarly, the Wiretap Act expressly makes it lawful to intercept a "radio communication" transmitted by a "public safety communications system" or by "any marine or aeronautical communications system." 18 U.S.C. § 2511(2)(g)(iii), (i). Under the panel's opinion, however, that blanket protection no longer includes transmissions that consist mostly

[4] The panel's reinterpretation of the term "radio communication" thus creates questions about whether it might, at least in some circumstances, violate the Wiretap Act to receive broadcast television signals. There is a serious argument that some television broadcasts would be "wire communications," which are ineligible for protection under § 2511(2)(g)(i). Television often contains "the human voice" and generally proceeds, at least in part, "by the aid of wire, cable, or other like connection," thus satisfying the two key elements of the definition of "wire communication." 18 U.S.C. § 2510(1), (18). If categorized that way, television transmissions could not be "electronic communications" and would not be covered by (g)(1). At a minimum, the panel's reinterpretation of the term "radio communication" injects uncertainty into an area where Congress intended clarity.

of data or of pictures.[5] That makes no sense, will create confusion about what radio-based signals can be lawfully received, and is not what Congress intended.

The panel itself acknowledged that its reliance on the novel and undefined term "predominantly auditory" and its use of "broadcast" in a new context would create legal uncertainty. The panel, for example, refused to address whether, under its definition, cell phone calls would be considered radio communications, because whether they are "broadcast" would be a "close question." Op. 17 n.5. (The panel's analysis would also seem to suggest that data transmitted via cellular networks would not qualify as radio communications.) But the Wiretap Act's legislative history leaves no doubt that Congress intended a key basis for protection of cellular transmissions to be their status as "radio communications … transmitted by a common carrier." 18 U.S.C. § 2510(16)(D); *see* H.R. Rep. No. 99-647, at 32. Here, too, the panel's definition creates questions where there were meant to be answers.

The panel's cryptic definition of this core statutory term will sow confusion, leaving the public to guess, at pain of criminal liability, about

---

[5] While such communications (insofar as they are "electronic communications") would still be lawful to acquire if they are "readily accessible to the general public" under § 2511(2)(g)(i), that provision provides a more ambiguous standard (that, under the panel's decision, may require analysis of the distance the communication traveled and the sophistication of the equipment used to receive it) in place of the clear rule provided by § 2511(2)(g)(ii).

which radio-based communications are legal to acquire. That is contrary to the rule of lenity and this Court's rule "against interpreting criminal statutes in surprising and novel ways." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009). It also contravenes the Wiretap Act's own goal of ending "legal uncertainty." S. Rep. No. 99-541, at 18. Rehearing is warranted to alleviate the myriad problems that the panel's holding creates.[6]

II. The Panel's Ruling That Unencrypted Wi-Fi Transmissions Are Not "Readily Accessible" Improperly Resolved A Factual Issue That Was Not Before The Court

Having decided that Wi-Fi transmissions are not "radio communications," the panel then addressed a separate issue: whether so-called "payload" data transmitted on unencrypted Wi-Fi networks are "readily accessible to the general public" as "electronic communications" under § 2511(2)(g)(i). The panel held that they are not. Op. 32-35. The panel should not have decided that issue, and this aspect of its opinion should be stricken. The factual question the panel resolved was not decided by the district court; it was not argued by the parties; and it was beyond the proper scope of the appeal. In addition, the panel's improper ruling,

[6] Any belief that "radio communication" needs to be defined in a restrictive manner to address warrantless searches by law enforcement is unfounded. That issue is not implicated by this case, and of course the Wiretap Act is only one element in the cluster of laws that regulate government surveillance, including the Fourth Amendment, the Stored Communications Act, and other statutes.

which was premised on erroneous assumptions drawn from its own ad hoc factfinding, creates a cloud of legal uncertainty around routine activities involving Wi-Fi.

A. The panel's decision overlooks the procedural posture of this appeal. This case came to the Court on an interlocutory appeal from a partial denial of Google's motion to dismiss. There has been no discovery, and the only question before the district court was whether Plaintiffs' complaint stated a legally viable claim. The district court thus appropriately limited its ruling. It found simply that "Plaintiffs *plead facts sufficient to support a claim* that the Wi-Fi networks were not 'readily accessible to the general public, such that exemption G1 would not apply." ER25 (emphasis added). That holding gave Google the opportunity, if the case proceeded, to test plaintiffs' factual allegations through discovery, summary judgment, and, if necessary, trial.

Accordingly, Google did not include this aspect of the decision below in its request for 1292(b) certification or its petition for appeal. And, contrary to what the panel suggested (Op. 12, 34 n.8), Google never argued that transmissions made on unencrypted Wi-Fi networks are "readily accessible to the general public" under the ordinary meaning of that phrase that applies to "electronic communications." To the contrary, Google told the panel that that issue was "irrelevant" to the appeal. Google Reply Br. at 6 n.1. The plaintiffs likewise did not argue it; they merely asserted that they "properly pled" that Wi-Fi transmissions are

not readily accessible. Pl. Br. 37-38. That approach was consistent with their acknowledgement in the district court that whether "electronic communications are readily accessible to the general public *is a factual determination that cannot be resolved on a motion to dismiss*." Pls.' Resp. to Def. Google, Inc.'s Mot. To Dismiss Consolidated Class Action Compl. (Jan. 25, 2011), ECF No. 64, at 8 (emphasis added) (Addendum B, Tab 6).

The panel nonetheless seems to have categorically concluded—for purposes of this case and presumably all future cases—that data transmitted over an unencrypted Wi-Fi network are not "readily accessible." That was a mistake. As the plaintiffs themselves understood, whether their unencrypted Wi-Fi communications were "readily accessible to the general public," based on the ordinary meaning of that phrase, is a question of fact. *Id.* at 9.[7] In resolving it, the panel effectively granted partial summary judgment to the plaintiffs—on Google's motion to dismiss. The panel did so by ascribing to Google an argument

[7] *See also, e.g.*, *Rodriguez v. Widener Univ.*, No. 13-1336, 2013 WL 3009736, at *9-10 (E.D. Pa. June 17, 2013) (holding that whether material was "readily accessible to the general public" under § 2511(g)(i) was a factual issue and finding "no legal basis from which we can conclude as a matter of law that [] Facebook images are generally available to the public"); *cf. United States v. Hall*, 488 F.2d 193, 198 (9th Cir. 1973) (whether defendants "had a reasonable expectation that the communications were not subject to interception" under the Wiretap Act "is an issue of fact to be determined by the trial court").

that it did not make and by analyzing extra-record material that was not referenced in the pleadings and not properly before the Court.

This error warrants rehearing. The panel's factfinding defies black-letter rules of civil and appellate procedure. *See, e.g.*, *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001) ("court may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion"). These rules ensure that "litigants may not be surprised on appeal by final decision there of issues upon which they have had no opportunity to introduce evidence." *Singleton v. Wulff*, 428 U.S. 106, 120 (1976). That is precisely what happened here.

B. The problems with the panel's ruling do not stop there. In broadly declaring unencrypted Wi-Fi transmissions—which everyone agrees are broadcast by radio—to be not "readily accessible," the panel disregarded this Court's previous observation that "[b]roadcasting communications into the air by radio waves is more analogous to carrying on an oral communication in a loud voice or with a megaphone than it is to the privacy afforded by a wire." *United States v. Hall*, 488 F.2d 193, 198 (9th Cir. 1973).

The panel's efforts to distinguish unencrypted Wi-Fi from other kinds of radio-based transmissions ignore critical facts. For example, the suggestion that Wi-Fi transmissions are "geographically limited" (Op. 33), overlooks that for years "people have been beaming the Wi-Fi standard—typically used for 'hotspots' and wireless home networks—

over dozens of miles." Charles Waltner, *Long-Range Wifi: Filling the Gaps in the Broadband Map*, The Network: Cisco's Technology News Site (Oct. 18, 2010) http://newsroom.cisco.com/dlls/2010/hd_101810.html (Addendum B, Tab 2). Nor is it accurate that "intercepting and decoding payload data communicated on a Wi-Fi network requires sophisticated hardware" (Op. 34). Network-analysis tools that do precisely that (colloquially referred to as "packet-sniffers") are ubiquitous. They are sold by Cisco and other mainstream commercial providers, and indeed are included as a standard feature of Apple's desktop operating system and offered by Microsoft as a free download for Windows. Addendum B, Tabs 3-5. The tools needed to receive, store, and monitor data transmitted on nearby Wi-Fi networks thus are available to virtually anyone with a personal computer. At a minimum, Google had a right to develop these issues through discovery and briefing on the relevant law and facts.[8] The panel's ruling violates due process by arbitrarily depriving Google of that opportunity.

The panel's error will also put everyday activities involving Wi-Fi networks at legal risk. Packet-sniffers, for instance, are essential for enterprise security; their use is a common part of network manage-

[8] The only other decision to have ruled on this question concluded, based on a detailed factual record, that "the proposition that Wi-Fi communications are accessible only with sophisticated technology breaks down." *In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 892-94 (N.D. Ill. 2012).

ment and security research, and is taught in respected universities. Addendum B, Tabs 3-5.[9] The panel's ruling that unencrypted Wi-Fi broadcasts are not "readily accessible" casts significant doubt about whether those tools can now be used—for laudable purposes—without violating the Wiretap Act.

The panel's holding also raises concerns about the ordinary operation of Wi-Fi-enabled devices. In the course of receiving transmissions on a given network, Wi-Fi devices by design continually receive and decode all nearby packets to determine which ones are intended for that device. Kak, *supra*, https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf. Likewise, those connecting to an open Wi-Fi network will often receive material that is being transmitted by other computers connected to that network. Common examples include the file names and directories for materials being shared on the network via iTunes or other programs. *Cf. United States v. Ahrndt*, 475 F. App'x 656 (9th Cir. 2012) (user connected to unsecured Wi-Fi network was able to view file names in her neighbor's file library). These examples simply reflect the regular operation of Wi-Fi—the fact that unencrypted Wi-Fi transmissions are just radio signals that, by design, can be acquired

[9] *See also* Avinash Kak, Purdue University College of Engineering, *Lecture 23: Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing* (Apr. 2, 2013), https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf.

and decoded with ease. Here too, the sweeping language in the panel's decision creates uncertainty about whether these everyday occurrences now violate the Wiretap Act.

* * *

The panel prematurely adjudicated Google's defense under the (g)(i) exemption and thereby deprived it of the opportunity to develop a factual and legal record showing that the defense applied here. Rehearing is needed to undo the panel's mistake and alleviate the serious legal and practical uncertainties it creates.

CONCLUSION

Google's petition for rehearing and rehearing en banc should be granted.

DATED: September 24, 2013

Respectfully submitted,

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

s/ *Seth P. Waxman*
Seth P. Waxman
WILMER CUTLER PICKERING HALE
AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, D.C. 20006
(202) 663-6800

Counsel for Petitioner/Appellant Google Inc.

CERTIFICATE OF COMPLIANCE

I certify that pursuant to Circuit Rule 35-1 and 40-1(a), the attached petition for panel rehearing and rehearing en banc is proportionally spaced, has a typeface of 14 points or more, and contains 4,197 words.

s/ *Michael H. Rubin*
Michael H. Rubin
WILSON SONSINI GOODRICH & ROSATI
PROFESSIONAL CORPORATION
650 Page Mill Road
Palo Alto, CA 94304
(650) 493-9300

Counsel for Google Inc.

ADDENDUM A

ADDENDUM A: TABLE OF CONTENTS

Definitions of "Radio Communication" and "Radiocommunication(s)":

Dictionary	Definition	Tab
Nelson M. Cooke & John Markus, Electronics Dictionary 303 (1st Ed. McGraw-Hill 1945)	"The transmission by radio of writing, signs, signals, pictures, and sounds of all kinds."	1
Frederic Swing Crispin, Dictionary of Technical Terms 322 (8th Ed. Bruce Publ'g Co. 1948)	"The transmission of voice or a coded message by means of radio energy."	2
Dennis Longley & Michael Shain, Dictionary of Information Technology 284 (John Wiley & Sons 1982)	"Telecommunication by means of electromagnetic waves at radio frequencies."	3
A.J. Meadows *et al.*, Dictionary of New Information Technology 151 (Kogan Page 1982)	"Any communication using radio waves."	4

Dictionary	Definition	Tab
Cambridge Dictionary of Science and Technology 737 (Cambridge University Press 1988)	"Any form of communication involving the transmission and reception of electromagnetic waves, from a frequency of 10 kHz up to more than 10 GHz. Information is conveyed by modulation of the information it is desired to impart onto a carrier. The information may be letters represented by code (e.g. Morse), speech, telemetry, pictures (either facsimile or television), digital signals or computer data. In broadcasting, radio communication is a one way process serving many listeners or viewers, or it may be two-way as in telecommunication systems. In the latter, communication may be between two mobile users in different vehicles or from a mobile vehicle and a fixed station, from one microwave tower to another in terrestrial communication (see radio link) or from one Earth station to another via a communication satellite."	5
McGraw-Hill Dictionary of Scientific and Technical Terms 1552 (Sybil P. Parker Ed., 4th Ed. McGraw-Hill 1989)	"Communication by means of radio waves, such as by radio facsimile, radiotelegraph, radiotelephone, and radioteletypewriter."	6
Newton's Telecom Dictionary 458 (2d Ed. Telecom Library 1989)	"Any telecommunication by means of radio waves."	7

Dictionary	Definition	Tab
Gilbert Held, Dictionary of Communications Technology 437 (3d Ed. John Wiley & Sons 1998)	"Communications by means of radio waves."	8
Rudolf F. Graf, Modern Dictionary of Electronics 616 (7th Ed. Newnes 1999)	"An overall term for transmission by radio of writing, signs, signals, pictures, and sounds of all kinds."	9
The Focal Illustrated Dictionary of Telecommunications 510 (Focal Press 1999)	"Generic term used to cover any form of communications which occurs using radio waves and operating within the radio frequency spectrum."	10
Newton's Telecom Dictionary 948 (26th Ed. Flatiron Publishing 2011)	"Any telecommunication by means of radio waves."	11

Electronics Dictionary

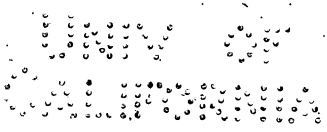
An illustrated glossary of over 6,000 terms used in radio, television, industrial electronics, communications, facsimile, sound recording, etc.

by NELSON M. COOKE, Lt. Com., U.S.N.
Executive Officer, Radio Matériel School, Naval Research Laboratory, Washington, D.C.

and

JOHN MARKUS
Associate Editor, Electronics

FIRST EDITION



McGRAW-HILL BOOK COMPANY, INC.
NEW YORK 1945 LONDON

ELECTRONICS DICTIONARY

The opinions or assertions contained herein are not be be construed as official or reflecting the views of the Navy Department or of the naval service at large.

THE MAPLE PRESS COMPANY, YORK, PA.

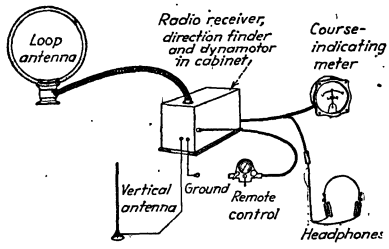
time in either direction between two points. 2. An arrangement of parts and connecting wires for radio purposes.

radio communication The transmission by radio of writing, signs, signals, pictures, and sounds of all kinds.

radio compass A radio direction finder used for navigational purposes (AIEE definition). Strictly speaking, it is not a compass because it gives direction with respect to a radio station rather than to the north magnetic pole.

radio control Control of stationary equipment or of unmanned moving objects such as ships, aircraft, or automobiles by means of signals transmitted through space by radio.

radiode A container for radium.



Radio direction finder for small planes.

radio direction finder A radio receiving device that can be used to determine the line of propagation of radio waves.

radio direction-finding station A station equipped with special apparatus for determining the direction of the emissions of other stations.

radio engineering That field of engineering dealing with the generation, transmission, and reception of radio waves and with the design, manufacture, and testing of associated equipment. This definition includes television, which is simply radio engineering extended to handle picture signals.

radio fadeout Complete or near-complete absorption of radio waves by those parts of the ionosphere which are affected by a sudden ionospheric disturbance.

radio field intensity The effective value of the electric or magnetic field intensity at a point due to the passage of radio waves of a specified frequency. Usually expressed as the electric field intensity in microvolts or millivolts per meter. Unless otherwise stated, it is measured in the direction of maximum field intensity.

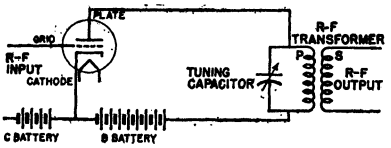
radio field-to-noise ratio The ratio, at a given location, of the radio field intensity of the desired wave to the noise field intensity.

radio fix 1. Determination of the position of the source of radio signals by obtaining cross bearings on the transmitter with two or more radio direction finders in different locations, then computing the position by triangulation. 2. Determination of the position of a vessel or aircraft equipped with direction-finding equipment by obtaining radio bearings on two or more transmitting stations of known location and then computing the position by triangulation.

radio frequency A frequency usually higher than those corresponding to normally audible sound waves and lower than the frequencies corresponding to heat and light waves.

radio-frequency alternator A rotating-type generator for providing high power at radio frequencies generally lower than 100,000 cycles. Used at one time for radio transmitters, but the chief use today is for high-frequency heating.

radio-frequency amplifier A vacuum-tube amplifier stage or section used to increase the voltage or power of radio-frequency signals. In a tuned-radio-frequency receiver, all stages ahead of the detector are radio-frequency amplifier stages (often called simply radio-frequency stages). In a super-



Simplified circuit diagram of a radio-frequency amplifier stage.

DICTIONARY
OF TECHNICAL TERMS

Containing Definitions of Commonly Used Expressions in Aeronautics, Architecture, Woodworking and Building Trades, Electrical and Metalworking Trades, Printing, Chemistry, etc.

FREDERIC SWING CRISPIN, C.E.
Head of Department of Industrial Arts
Gratz High School, Philadelphia, Pa.

(*Eighth Edition — Revised*)

THE BRUCE PUBLISHING COMPANY
MILWAUKEE

square feet of effective heating area of a radiator.

ra'di-a'tion (*Mech. Engin.*) The act of radiating, as of heat. The amount or area of radiating surface in a building is spoken of as so many feet of radiation.

ra'di-a'tor (*Mech. Engin.*) A heating unit.

ra'di-a'tor hose (*Auto.*) The hose which connects radiator and engine.

ra'di-a'tor shut'ter (*Auto.*) Used for controlling the amount of air entering the radiator. Most shutters consist essentially of a series of metal slats operated as a unit either mechanically or thermostatically.

rad'i-cal (*Algebra*) Relating to the root or roots of numbers; being or containing a root. (*Chem.*) A group of atoms which retain the action of single atoms.

ra'di-o (*Elec.*) A preferred name for wireless. Often incorrectly used where a compound word would be more proper, as radiotelephone, radiotelegraph, etc.

ra'di-o-ac'tive (*Elec.*) Giving off positive and negative charged particles.

ra'di-o broad'cast'ing. The changing of auditory energy to radio energy to be transmitted in the form of radio waves.

ra'di-o chan'nel (*Tel.*) The "space" in the radio-frequency spectrum allocated to each station or service. In present television standards a channel is 6 megacycles wide.

ra'di-o com-mu'ni-ca'tion. The transmission of voice or a coded message by means of radio energy.

ra'di-o com'pass (*Aero.*) A compass which receives its directions from the radiation principles of the loop antenna. It does not point north but toward the radio broadcasting station on which it is set.

ra'di-o-fre'quen-cy (*Elec.*) The frequency of the electric waves used in the transmission of radio signals which are just beyond audible frequencies, approximately between 40,000 and 30,000,000 vibrations per second.

ra'di-o-gram'. A message transmitted through the medium of radio and relayed by some means to the addressee.

ra'di-o–marker bea'con (*Aero.*) A radio transmitter of low power emitting a characteristic aural signal to indicate course positions with respect to a landing field or an airway.

ra'di-o net'work. The grouping of a number of radio broadcasting stations for the purpose of transmitting a common program, usually originating at one of the affiliated stations.

ra'di-o op'er-a'tor. The individual who is charged with the responsibility of operating a radio transmitter and receiver for the purpose of carrying on communication either in code or voice.

ra'di-o-phone'. The apparatus necessary to carry on voice communication by means of radio, from either a fixed or movable location.

ra'di-o–range bea'con (*Aero.*) A radio transmitter supplying directive radio waves that provide a means of keeping an aircraft on its proper course.

ra'di-o re-ceiv'er. The equipment necessary to change radio energy, being received, into auditory energy.

ra'di-o sta'tion. The location of the apparatus used in the transmitting

DICTIONARY OF INFORMATION TECHNOLOGY

Dennis Longley
and
Michael Shain

A WILEY-INTERSCIENCE PUBLICATION

JOHN WILEY & SONS
New York

Published in the USA
A Wiley Interscience Publication
John Wiley & Sons, Inc., New York

Library of Congress Cataloging in Process Number: 82–51103

ISBN 0 471–89574–1

Typeset by Leaper & Gard Ltd, Bristol
Printed in Great Britain

R

race In electronics, an undesirable state, produced by poor design of digital circuits, in which the output can vary with minor changes in the relative time of arrival of input pulses. Compare hazard.

rack (1) In electronics, a metal frame or chassis for the mounting of items of equipment. (2) In photography, to focus a lens.

rack and pinion focusing In filming, a method of converting the rotation of a knob into a linear movement of the lens: a toothed bar (rack) engages into a gear wheel (pinion).

rack focus In filming, to change the focus during a shot.

rack focus shot In filming, a shot in which the depth of field and focus are changed in order to move the emphasis to the action at a different distance from the camera. See depth of field.

rack over In filming, a camera arrangement that enables a viewfinder to be moved into the position normally occupied by the film, thus enabling the cameraman to see through the lens. See reflex.

radar In radiodetermination, (RAdio Detection And Ranging), a technique using a comparison between transmitted signals and those reflected by, or retransmitted from, a distant object, to determine the position of the object.

radial transfer In computing, the transmission of data between a peripheral unit and another device that is closer to the center than the peripheral unit.

radiant energy The energy of a sinusoidal wave is proportional to the square of the amplitude of oscillation. See photon.

radiating element In radiocommunications, a basic unit of an antenna designed to produce electromagnetic radiation. See antenna.

radio In communications, (1) a service for the transmission of speech and music by electromagnetic radiation, (2) electromagnetic radiation in the frequency range 10kHz – 3000GHz. See radiodetermination, radiocommunication, radio waves, radio astronomy, electromagnetic radiation, GHz, kHz.

radio astronomy Gathering of information of astronomical bodies and objects by the reception of cosmic origin radio waves. See radio waves.

radio beacon In radionavigation, an automatic radio transmitter whose emissions enable a ship or aircraft to determine its direction or bearing relative to the beacon location.

radiocommunication Telecommunication by means of electromagnetic waves at radio frequencies. See radio waves.

radiodetermination The determination of the velocity, position and other characteristics of an object by means of the propagation properties of radio waves. See radio waves.

radiolocation Radiodetermination used for purposes other than those of radio navigation. See radionavigation, radiodetermination.

radio microphone A microphone combined with a low range radio transmitter, thus requiring no connecting wires to an amplifier, used for studio or location work. See amplifier, transmitter.

radionavigation The use of radiodetermination for navigation purposes,

dictionary of new INFORMATION TECHNOLOGY

A.J.Meadows M.Gordon A.Singleton

Kogan Page, London
Nichols Publishing Company, New York

First published in Great Britain in 1982 by
Kogan Page Ltd, 120 Pentonville Road, London N1 9JN

British Library Cataloguing in Publication Data
Meadows, A. J.
Dictionary of new information technology.
1. Information science – Dictionaries
I. Title II. Gordon, M.
III. Singleton, A.
020'.0321 Z1006

ISBN 0-85038-531-8

First published in the United States of America
in 1982 by Nichols Publishing Company,
Post Office Box 96, New York, NY 10024

Library of Congress Cataloging in Publication Data
Main entry under title:
Dictionary of new information technology.
1. Electronic data processing – Dictionaries.
2. Telecommunication – Dictionaries. 3. Office practice – Automation – Dictionaries. I. Meadows, A. J. (Arthur Jack)
QA76.15.D527 1982 001.5'03'21 82-3532
ISBN 0-89397-135-9 AACR2

Printed and bound in Great Britain by
T J Press (Padstow) Ltd

RACE random access computer equipment (see *random access*).

RAD rapid access disc (see *magnetic disc* and *access time*).

RADA random access discrete address. A location in a *RAM* (see *address*).

radio communication any communication using radio waves (see *spectrum*).

Radio Suisse a Swiss *host* system.

RADIR random access document indexing and retrieval (see *random access*, *RAM*, and *information retrieval system*).

ragged right an uneven right-hand margin (see *justify*).

RAM *random access memory*.

RAMIS Random Access Management Information System. An *information retrieval system* which stores management information in *RAM*.

RAMPI Raw Material Price Index. An *online databank*.

R&D research and development. Designates technical and applied scientific activity, particularly directed towards the development of new products, processes, services or systems.

random access memory (RAM) *memory* where any location can be read from, or written to, in a *random access* fashion.

random access (storage) *access* to *storage* where the next *location* from which information is to be obtained is unrelated to the previous location. Normally implies that the *access time* to any location is the same.

ranged left text which is justified at the left-hand margin only. Used as a synonym for *ragged right* (see *justify*).

RAPID random access personnel information system (see *RAMIS*, *RAM* and *information retrieval system*).

RASTAC random access storage and control (see *RAM*).

RASTAD random access storage and display (see *RAM* and *display*).

raster a grid on a *terminal* screen which divides the *display* area into discrete elements (like a map reference system).

raster count the number of positions on a *display* screen which can be defined using its *raster* (ie the product of the number of horizontal and vertical divisions).

raster graphics a form of *computer graphics* which, unlike *vector graphics*, utilizes a full matrix of *pixels*. Each pixel has its own code, and is switched on, or off, according to a guiding *program* (see *raster*).

raster plotter a *plotter* which draws a complete picture on a *CRT*, including an image both of the object of interest and its background. It is used in *computer graphics*. (See also *calligraphic plotter* and *raster*.)

raster scan the sweeping of the display area of a device, line-by-line, to generate, or read, an image.

raw data *data* which have not been processed.

RAX *remote access*.

RCA Selectavision see *Selectavision*.

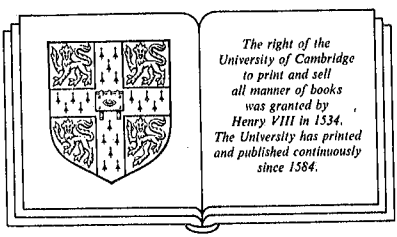
reactive mode when each entry at a *terminal* causes some action to be taken by a *central processor*, but the processor does not necessarily return an immediate response to the *terminal*. It is to be contrasted with *conversational mode*.

read 1. to copy, usually from one *storage* area to another. 2. to sense information from some form of recorded medium, eg from a *card* or *magnetic tape*.

READ 1. real-time electronic access and display (see *real time*, *access* and *display*). 2. remote electrical alphanumeric display (see *remote access*, *alphanumeric* and *display*).

Cambridge Dictionary of Science and Technology

General Editor
PETER M. B. WALKER, CBE, FRSE



CAMBRIDGE UNIVERSITY PRESS
CAMBRIDGE
NEW YORK PORT CHESTER MELBOURNE SYDNEY

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York NY 10011 USA
10 Stamford Road, Oakleigh, Melbourne 3166 Australia

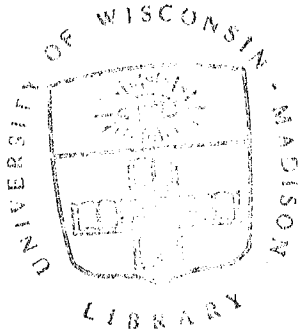
Previously published under the title
Chambers Science and Technology Dictionary
Published in the UK by W & R Chambers under the title
Chambers Science and Technology Dictionary
Published in North America by agreement under the title
Cambridge Dictionary of Science and Technology
Reprinted 1990

Printed in the United States of America

Library of Congress Cataloging-in-Publication Data

Chambers science and technology dictionary.
Cambridge dictionary of science and technology/general editor Peter M. B. Walker.
p. cm.
"First published in 1988 under the title: Chambers science and technology dictionary" – T.p. verso.
ISBN 0-521-39441-4
1. Science – Dictionaries. 2. Technology – Dictionaries.
I. Walker, Peter M. B. II. Title. III. Title: Dictionary of science and technology.
Q123.C482 1990
503 – dc20

ISBN 0-521-39441-4 hardback



formation (quantitative) equals rate of decay. Particularly important between radium and radon.

radioactive isotope *(Phys.)*. Naturally occurring or artificially produced isotope exhibiting radioactivity; used as a source for medical or industrial purposes. Also *radioisotope*.

radioactive series *(Phys.)*. Most naturally occurring radioactive isotopes belong to one of three series that show how they are related through radiation and decay. Each series involves the emission of an α-particle, which decreases the *mass number* by 4, and β- and γ-decay which do not change the mass number. The natural series have members having mass number: (a) $4n$ (thorium series); (b) $4n + 2$ (*uranium-radium series*); (c) $4n + 3$ (*actinium series*). Members of the $4n + 1$ (*plutonium series*) can be produced artificially. Also called *radioactive chain*.

radioactive standard *(Phys.)*. A radiation source for calibrating radiation measurement equipment. The source has usually a long half-life and during its decay the number and type of radioactive atoms at a given reference time is known.

radioactive tracer *(Phys.)*. Small quantity of radioactive preparation added to corresponding nonactive material to *label* or *tag* it so that its movements can be followed by tracing the activity. (The chemical behaviour of radioactive elements and their nonactive isotopes is identical.)

radioactivity *(Phys.)*. Spontaneous disintegration of certain natural heavy elements (e.g. radium, actinium, uranium, thorium) accompanied by the emission of α-rays, which are positively charged helium nuclei; β-rays, which are fast electrons; and γ-rays, which are short X-rays. The ultimate end-product of radioactive disintegration is an isotope of lead. See also **artificial radioactivity, induced radioactivity**.

radio-allergosorbent test *(Immun.)*. *RAST*. Method for measuring extremely small amounts of IgE antibody specific for various allergens. Blood serum is reacted with allergen-coated particles which are then washed to remove non-reacting proteins. Radiolabelled anti-human IgE is then added and this binds to the IgE antibody, bound to the particles via the allergen. Provided that the amount of allergen supplied and the anti-IgE are present in excess, the radioactivity on the particles after washing is proportional to the amount of allergen-specific antibody in the serum sample.

radio altimeter *(Aero.)*. Device for determining height, particularly of aircraft in flight, by electronic means, generally by detecting the delay in reception of reflected signals, or change in frequency; also called *radar altimeter*.

radio astronomy *(Astron.)*. The exploration of the universe by detecting radio emission from a variety of celestial objects. The frequency spans a vast range from 10 MHz to 300 GHz. A variety of antennas are used, from single dishes to elaborate networks of telescopes forming intercontinental radio **interferometers**. The principle sources of radio emission are: the Sun, Jupiter, interstellar hydrogen, emission nebulae, pulsars, supernova remnants, radio galaxies, quasars, and the cosmic background radiation of the universe itself.

radio beacon *(Telecomm.)*. Stationary radio transmitter which transmits steady beams of radiation along certain directions for guidance of ships or aircraft, or one which transmits from an omnidirectional antenna and is used for the taking of bearings, using an identifying code. Also *aerophare*.

radio beam *(Telecomm.)*. Concentration of electromagnetic radiation within narrow angular limits, such as is emitted from a highly directional antenna.

radio bearing *(Telecomm.)*. Direction of arrival of a radio signal, as indicated by a loop, goniometer, interferometer or any directional receiving system as used for navigational purposes.

radiobiology *(Biol.)*. Branch of science involving study of effect of radiation and radioactive materials on living matter.

radio broadcasting *(Telecomm.)*. The transmission by means of radio waves, of a programme of sound or picture for general reception. The separation of the frequency channels is decided by international agreement.

radiocaesium *(Chem.)*. ^{137}Cs, a radioactive isotope recovered from the waste of nuclear reactors in nuclear power plants. Useful for mass-radiation and sterilization of foodstuffs. Also for high-intensity X-ray radiation of surface tumours in place of much more expensive radium. Half-life 37 years.

radiocarbon *(Chem.)*. ^{14}C, a weakly radioactive isotope undergoing beta-decay with a half-life of 5770 years. It is present in the atmosphere in roughly constant amount, as it is produced from ^{14}N by cosmic rays. It is used in some tracer studies. It can also be used to date the time of death of once-living material (and hence the likely time of manufacture of an artifact). This is because living material has the same ratio of ^{14}C to ^{12}C as the atmosphere. After death, however, the ^{14}C decays and is not replaced.

radiocarbon dating *(Geol.)*. A method of determining the age in years of fossil organic material or water bicarbonate, based on the known decay rate of ^{14}C to ^{14}N. See **radiocarbon**.

radiochemical purity *(Chem.)*. The proportion of a given radioactive compound in the stated chemical form. Cf. **radioisotopic purity**.

radiochemistry *(Chem.)*. Study of science and techniques of producing and using radioactive isotopes or their compounds to study chemical compounds. Cf. **radiation chemistry**.

radio circuit *(Telecomm.)*. Communication system including a radio link, comprising a transmitter and antenna, the radio transmission path, with possible reflections or scatter from ionized regions, and a receiving antenna and receiver.

radiocolloids *(Phys.)*. Radioactive atoms in colloidal aggregates.

radio communication *(Telecomm.)*. Any form of communication involving the transmission and reception of electromagnetic waves, from a frequency of 10 kHz up to more than 10 GHz. Information is conveyed by **modulation** of the information it is desired to impart onto a **carrier**. The information may be letters represented by code (e.g. Morse), speech, telemetry, pictures (either facsimile or television), digital signals or computer data. In broadcasting, radio communication is a one way process serving many listeners or viewers, or it may be two-way as in telecommunication systems. In the latter, communication may be between two mobile users in different vehicles or from a mobile vehicle and a fixed station, from one microwave tower to another in terrestrial communication (see **radio link**) or from one *Earth* station to another via a **communication satellite**.

radio compass *(Telecomm.)*. Originally a rotating loop, later rendered more sensitive by a goniometer system and by display on a cathode-ray tube. Any device, depending on radio, which gives a bearing. See **Adcock antenna**.

radio direction-finding *(Telecomm.)*. Passive reception of direction-finding signals from radio beacons or navigational transmitters, as distinct from active radar. Abbrev. *RDF*.

radioelement *(Phys.)*. An element exhibiting natural radioactivity.

radio frequency *(Telecomm.)*. One suitable for radio transmission, above 10^4 Hz and below 3×10^{12} Hz approx. Abbrev. *RF*. Also *radio spectrum*.

radio-frequency heating *(Elec.Eng.)*. See **dielectric heating, induction heating**.

radio-frequency spectrometer *(Nuc.Eng.)*. Type of **mass spectrometer** used in the study of ions in plasmas.

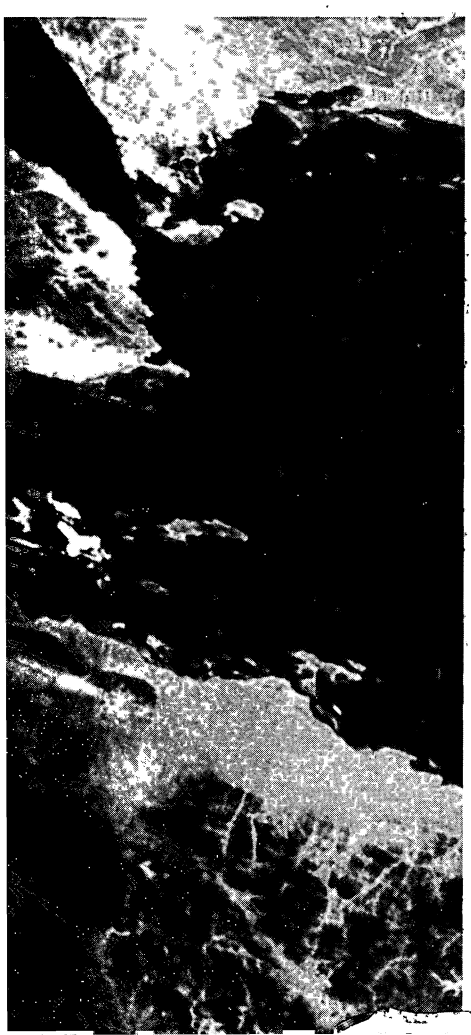
radio-frequency spectroscopy *(Phys.)*. See **nuclear magnetic resonance, electron spin resonance**.

radio galaxy *(Astron.)*. About one galaxy in a million is an intense source of cosmic radio waves, caused by synchrotron emission of relativistic electrons.

radiogenic *(Phys.)*. Said of stable or radioactive products arising from radioactive disintegration.

McGraw-Hill DICTIONARY OF SCIENTIFIC AND TECHNICAL TERMS

Fourth Edition



Sybil P. Parker
EDITOR IN CHIEF

McGRAW-HILL BOOK COMPANY

New York
St. Louis
San Francisco

Auckland Bogotá
Caracas Colorado Springs
Hamburg Lisbon
London Madrid
Mexico Milan
Montreal New Delhi
Oklahoma City Panama
Paris San Juan
São Paulo Singapore
Sydney Tokyo
Toronto

On the cover: Pattern produced from white light by a computer-generated diffraction plate containing 529 square apertures arranged in a 23 × 23 array. (R. B. Hoover, Marshall Space Flight Center)

On the title pages: Aerial photograph of the Sinai Peninsula made by Gemini spacecraft. (NASA)

Included in this Dictionary are definitions which have been published previously in the following works: P. B. Jordain, *Condensed Computer Encyclopedia*, Copyright © 1969 by McGraw-Hill, Inc. All rights reserved. J. Markus, *Electronics and Nucleonics Dictionary*, 4th ed., Copyright © 1960, 1966, 1978 by McGraw-Hill, Inc. All rights reserved. J. Quick, *Artists' and Illustrators' Encyclopedia*, Copyright © 1969 by McGraw-Hill, Inc. All rights reserved. *Blakiston's Gould Medical Dictionary*, 3d ed., Copyright © 1956, 1972 by McGraw-Hill, Inc. All rights reserved. T. Baumeister and L. S. Marks, eds., *Standard Handbook for Mechanical Engineers*, 7th ed., Copyright © 1958, 1967 by McGraw-Hill, Inc. All rights reserved.

In addition, material has been drawn from the following references: R. E. Huschke, *Glossary of Meteorology*, American Meteorological Society, 1959; *U.S. Air Force Glossary of Standardized Terms*, AF Manual 11-1, vol. 1, 1972; *Communications-Electronics Terminology*, AF Manual 11-1, vol. 3, 1970; W. H. Allen, ed., *Dictionary of Technical Terms for Aerospace Use*, 1st ed., National Aeronautics and Space Administration, 1965; J. M. Gilliland, *Solar-Terrestrial Physics: A Glossary of Terms and Abbreviations*, Royal Aircraft Establishment Technical Report 67158, 1967; *Glossary of Air Traffic Control Terms*, Federal Aviation Agency; *A Glossary of Range Terminology, White Sands Missile Range, New Mexico*, National Bureau of Standards, AD 467-424; *A DOD Glossary of Mapping, Charting and Geodetic Terms*, 1st ed.; Department of Defense, 1967; P. W. Thrush, comp. and ed., *A Dictionary of Mining, Mineral, and Related Terms*, Bureau of Mines, 1968; *Nuclear Terms: A Glossary*, 2d ed., Atomic Energy Commission; F. Casey, ed., *Compilation of Terms in Information Sciences Technology*, Federal Council for Science and Technology, 1970; *Glossary of Stinfo Terminology*, Office of Aerospace Research, U.S. Air Force, 1963; *Naval Dictionary of Electronic, Technical, and Imperative Terms*, Bureau of Naval Personnel, 1962; *ADP Glossary*, Department of the Navy, NAVSO P-3097.

McGRAW-HILL DICTIONARY OF SCIENTIFIC AND TECHNICAL TERMS, Fourth Edition

2 3 4 5 6 7 8 9 0 DOW/DOW 8 9 5 4 3 2 1 0 9

ISBN 0-07-045270-9

Library of Congress Cataloging-in-Publication Data

McGraw-Hill dictionary of scientific and technical terms.

1. Science—Dictionaries. 2. Technology—Dictionaries.
I. Parker, Sybil P.
Q123.M34 1989 503'/21 88-13490
ISBN 0-07-045270-9

radioactive tracer [NUCLEO] A radioactive isotope which, when attached to a chemically similar substance or injected into a biological or physical system, can be traced by radiation detection devices, permitting determination of the distribution or location of the substance to which it is attached. Also known as radiotracer. { ˌrād·ē·ō'ak·tiv 'trā·sər }

radioactive transformation *See* radioactive decay. { ˌrād·ē·ō'ak·tiv ˌtranz·fər'mā·shən }

radioactive waste [NUCLEO] Liquid, solid, or gaseous waste resulting from mining of radioactive ore, production of reactor fuel materials, reactor operation, processing of irradiated reactor fuels, and related operations; and from use of radioactive materials in research, industry, and medicine. { ˌrād·ē·ō'ak·tiv 'wāst }

radioactive-waste disposal [NUCLEO] The disposal of waste radioactive materials and of equipment contaminated by radiation; the two basic disposal methods are concentration for burial underground or in the sea, and dilution for controlled dispersion; reprocessing of reactor fuel is a major source of radioactive waste. { ˌrād·ē·ō'ak·tiv ˌwāst di'spō·zəl }

radioactive well logging [ENG] The recording of the differences in radioactive content (natural or neutron-induced) of the various rock layers found down an oil well borehole; types include γ-ray, neutron, and photon logging. Also known as radiation well logging; radioactivity prospecting. { ˌrād·ē·ō'ak·tiv 'wel ˌläg·iŋ }

radioactivity [NUC PHYS] **1.** A particular type of radiation emitted by a radioactive substance, such as alpha radioactivity. **2.** *See* radioactive decay. **3.** *See* activity. { ˌrād·ē·ō·ak'tiv·əd·ē }

radioactivity analysis *See* activation analysis. { ˌrād·ē·ō·ak'tiv·əd·ē ə'nal·ə·səs }

radioactivity concentration guide [NUCLEO] The concentration of radioactive material in an environment which would result in doses equal, over a period of time, to those in the radiation protection guide; this Federal Radiation Council term replaces the former maximum permissible concentration. { ˌrād·ē·ō·ak'tiv·əd·ē ˌkänsˌən'trā·shən ˌgīd }

radioactivity equilibrium [NUC PHYS] A condition which may arise in the decay of a radioactive parent with short-lived descendants, in which the ratio of the activity of a parent to that of a descendant remains constant. { ˌrād·ē·ō·ak'tiv·əd·ē ˌē·kwə'lib·rē·əm }

radioactivity log [ENG] Record of radioactive well logging. { ˌrād·ē·ō·ak'tiv·əd·ē ˌläg }

radioactivity prospecting *See* radioactive well logging. { ˌrād·ē·ō·ak'tiv·əd·ē 'präˌspek·tiŋ }

radio aid to navigation [ELECTR] An aid to navigation which utilizes the propagation characteristics of radio waves to furnish navigation information. { 'rād·ē·ō ˌād tə ˌnav·ə'gā·shən }

radio altimeter [ENG] An absolute altimeter that depends on the reflection of radio waves from the earth for the determination of altitude, as in a frequency-modulated radio altimeter and a radar altimeter. Also known as electronic altimeter; reflection altimeter. { 'rād·ē·ō al'tim·əd·ər }

radio altitude *See* radar altitude. { 'rād·ē·ō 'al·təˌtüd }

radio and wire integration [COMMUN] The combining of wire circuits with radio facilities. { 'rād·ē·ō ən 'wīr ˌint·ə'grā·shən }

radio antenna *See* antenna. { 'rād·ē·ō an'ten·ə }

radio approach aids [NAV] Equipment that uses radio or radar to furnish guidance to an aircraft with required accuracy from the time it is in the vicinity of an airfield until it reaches a position from which a landing can be made. { 'rād·ē·ō ə'prōchˌādz }

radioassay [ANALY CHEM] An assay procedure involving the measurement of the radiation intensity of a radioactive sample. { ˌrād·ē·ō'aˌsā }

radio astronomy [ASTRON] The study of celestial objects by measurement and analysis of their emitted electromagnetic radiation in the wavelength range from roughly 1 millimeter to 30 millimeters. { 'rād·ē·ō·ə'strän·ə·mē }

radio atmometer [ENG] An instrument designed to measure the effect of sunlight upon evaporation from plant foliage; consists of a porous-clay atmometer whose surface has been blackened so that it absorbs radiant energy. { 'rād·ē·ō·at'mäm·əd·ər }

radio attenuation [ELECTROMAG] 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. { 'rād·ē·ō əˌten·yə'wā·shən }

radio aurora *See* artificial radio aurora. { 'rād·ē·ō ə'ror·ə }

radioautography *See* autoradiography. { ˌrād·ē·ō,ȯ'täg·rə·fē }

radio autopilot coupler [ENG] Equipment providing means by which an electrical navigational signal operates an automatic pilot. { 'rād·ē·ō 'ȯd·ōˌpī·lət 'kəp·lər }

radio B battery [ELEC] A B-type battery used in a radio set, usually consisting of 15 to 30 permanently connected cells. { 'rād·ē·ō 'bē ˌbad·ə·rē }

radio beacon [NAV] A nondirectional radio transmitting station in a fixed geographic location, emitting a characteristic signal from which bearing information can be obtained by a radio direction finder on a ship or aircraft. Also known as aerophare; radiophare. { 'rād·ē·ō 'bē·kən }

radio-beacon buoy [NAV] A buoy equipped with a marker radio beacon; such a buoy is usually used to mark an important entrance to a channel; the beacon is of low power and provides a signal for a short range. { 'rād·ē·ō ˌbē·kən ˌbȯi }

radio-beacon monitor station [COMMUN] A station which monitors the signal from one or more remotely located marine radio beacons. { 'rād·ē·ō ˌbē·kən 'man·ə·tərˌstā·shən }

radio beam [ELECTROMAG] A concentrated stream of radio-frequency energy as used in radio ranges, microwave relays, and radar. { 'rād·ē·ōˌbēm }

radio bearing [NAV] The bearing of a radio transmitter from a receiver as determined by a radio direction finder. { ˌrād·ē·ōˌber·iŋ }

radiobiology [BIOL] Study of the scientific principles, mechanisms, and effects of the interaction of ionizing radiation with living matter. Also known as radiation biology. { ˌrād·ē·ō·bī'äl·ə·jē }

radio blackout [COMMUN] A fadeout that may last several hours or more at a particular frequency. Also known as blackout. { 'rād·ē·ō 'blakˌau̇t }

radio broadcasting [COMMUN] Radio transmission intended for general reception. { 'rād·ē·ō 'brȯdˌkast·iŋ }

radiocarbon *See* carbon-14. { ˌrad·ē·ō'kär·bən }

radiocarbon dating *See* carbon-14 dating. { ˌrad·ē·ō'kär·bən 'dād·iŋ }

radiocardiogram [MED] An x-ray recording of the variation with time of the concentration of a radioisotope in a heart chamber; usually the radioactive material is injected intravenously. { ˌrad·ē·ō'kärd·ē·əˌgram }

radiocesium *See* cesium-137. { ˌrad·ē·ō'sē·zē·əm }

radiochemical laboratory [CHEM] A specially equipped and shielded chemical laboratory designed for conducting radiochemical studies without danger to the laboratory personnel. { ˌrad·ē·ō'kem·ə·kəl 'lab·rəˌtȯr·ē }

radiochemistry [CHEM] That area of chemistry concerned with the study of radioactive substances. { ˌrad·ē·ō'kem·ə·strē }

radiochronology [GEOL] An absolute-age dating method based on the existing ratio between radioactive parent elements (such as uranium-238) and their radiogenic daughter isotopes (such as lead-206). { ˌrad·ē·ō·krə'näl·ə·jē }

radio climatology [CLIMATOL] The study of regional and seasonal variations in the manner of propagation of radio energy through the atmosphere. { 'rād·ē·ō 'klī·mə'täl·ə·jē }

radio command [ELECTR] A radio control signal to which a guided missile or other remote-controlled vehicle or device responds. { 'rād·ē·ō kəˌmand }

radio communication [COMMUN] Communication by means of radio waves, such as by radio facsimile, radiotelegraph, radiotelephone, and radioteletypewriter. { 'rād·ē·ō kəˌmyü·nə'kā·shən }

radio communications guard *See* radio guard. { 'rād·ē·ō kəˌmyü·nə'kā·shənz ˌgärd }

radio compass *See* automatic direction finder. { 'rād·ē·ō 'kəm·pəs }

radio control [ELECTR] The control of stationary or moving objects by means of signals transmitted through space by radio. { 'rād·ē·ō kən'trōl }

radio countermeasures [ELECTR] Electrical or other techniques depriving the enemy of the benefits which would ordinarily accrue to him through the use of any technique employing

#1 SELLING TELECOMMUNICATIONS DICTIONARY

Newton's TELECOM dictionary

THE OFFICIAL GLOSSARY OF TELECOMMUNICATIONS
ACRONYMS, TERMS AND JARGON

by Harry Newton

NEWTON'S TELECOM DICTIONARY

THE OFFICIAL GLOSSARY OF TELECOMMUNICATIONS ACRONYMS, TERMS AND JARGON

Books by Telecom Library:

The TELECONNECT Dictionary
Newton's Telecom Dictionary
The TELECONNECT Guide to:
- Automatic Call Distributors
- The Business of Interconnect
- How to Sell Call Accounting Systems
- Professional Selling

The TELECOM LIBRARY Guide to:
- T-1 Networking
- Negotiating Telecommunications Contracts
- Long Distance For Less
- Buying Short Haul Microwave
- The Perfect RFP
- The Inbound Telephone Call Center
- The Perfect Proposal
- ISDN Made Understandable
- OS/2 LANs
- ZEdit: The Software Rose

and . . .

- 101 Money-Saving Secrets Your Phone Company Won't Tell You
- Profit and Control Through Call Accounting
- Telecommunications Management for Business and Government
- Which Phone System Should I Buy?

Magazines by Telecom Library

The Telecom Library publishes two monthly magazines: **TELECONNECT**, the Telecom Industry's Favorite Magazine and **INBOUND/OUTBOUND**, which talks about using Technology to Sell, Service and Keep Your Customers. Call **1-800-999-0345** for subscription information.

FREE Catalog of Telecom Books

Telecom Library publishes books itself, and also distributes the books of every other telecommunications publisher. You may receive a FREE copy of our latest catalog by calling **212-691-8215** or **212-206-6660,** or by dropping a line to Kim Huy at the address below. You may order your Telecom Library books by calling **1-800-LIBRARY.**

Quantity Purchases

If you wish to purchase this book, or any others, in quantity, please contact:

Kim Huy, Manager
Telecom Library Inc.
12 West 21 Street
New York, NY 10010

1-800-LIBRARY or **212-691-8215** or **212-206-6660**
Facsimile orders: **212-691-1191**

Printed in USA by Bookcrafters, Chelsea MI

THIS DICTIONARY

SECOND EDITION

Most technical dictionaries define terms tersely. They leave you more confused than ever. This dictionary is different from any other. My definitions tell you what the term is, how it works, how you use it, what its benefits are, and how it fits into the greater scheme of things.

This is a **working** dictionary. The idea is to use it every day. You can give it to your users, to your customers, to your boss. You can even give it to your kids to let them understand what you do.

A big **Thank You** to the dozens of people and dozens of companies who helped. I'd love to name them all. If I do, I'll leave someone out. So thank you all. I do, however, want to especially thank the consultant liaison people from our industry's major long distance carriers, MCI and AT&T. MCI's dial-up consultant liaison bulletin board is just fabulous. Among the manufacturers, special thanks to Amdahl, Aspect Telecommunications, NEC, Newbridge Networks, Northern Telecom, Ricoh and Teknekron Infoswitch. They'll recognize some of their words in this dictionary. Special thank yous also to Jim Ross of Ross Engineering, Adamstown, MD, John Perri and Karen Miller of call accounting company SoftCom, NYC and to Jane Laino of Corporate Communications Consultants, NYC.

I've included all the relevant definitions I could find. If I've left any definitions out, or some of my definitions are unclear, drop me a line. In an earlier, much shorter version, this dictionary was called *The TELECONNECT Dictionary.* It's now much improved, much expanded and much updated. As I worked through this one, I became increasingly amazed at just how much our industry has progressed in fewer than two years. Writing this dictionary has been one of the most stimulating (and most time-consuming) tasks I've ever undertaken. However, there will be another improved and expanded edition. Please let me have your suggestions, additions, amendments and comments.

Harry Newton
12 West 21 Street
New York, NY 10010

July 4, 1989

Two hints on using this dictionary: Every definition is in alphabetical order. I ignore spaces, e.g. AD HOC comes after ADHOA. Mostly I include the acronym (e.g. ISUP) and the spelled-out-words (ISDN User Part). Sometimes the main explanation is under the acronym and sometimes under the spelled-out-words. Depends on which is more common. I explain some concepts in multiple definitions, like ISDN, which is an immensely complex idea. You'll find ISDN definitions leading to other ISDN definitions, like a puzzle.

A word of style: The plural of PBX is PBXs, not PBX's. T-1 is T-1, not T1, although in most circles T1 is the same as T-1. In this dictionary, it's T-1.

R

RACE: An association in the European Economic Community, Research and development for Advanced Communications in Europe.

RACEWAYS: A metal or plastic channel used for loosely holding electrical and telephone wires in buildings. A raceway is usually located in the floor and is usually encased on three or four sides by concrete. A raceway is used for interior wiring. A raceway performs the same job as a conduit, but it's typically larger.

RACK: A structure on which equipment is mounted. What a rack is to equipment, so a frame is to wiring. See also DISTRIBUTION FRAME.

RADAR: RAdio Detection And Ranging.

RADIO: The science of communicating over a distance by converting sounds or signals to electromagnetic waves and radiating them through the air or through space. Also called Wireless by the British and the Australians.

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 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 PAGING ACCESS: Provides attendant and phone user dial access to customer-owned radio paging equipment to selectively tone-alert, or voice-page individuals carrying pocket radio receivers. The paged party can answer by dialing an answering code from a phone within the PBX.

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*

Baffins Lane, Chichester
West Sussex, PO 19 IUD, 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

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.

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.

A member of the Reed Elsevier Group.

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)
1. 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

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 electrocardiograph signal from the subject to a remote receiver. It

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-Heineman
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

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

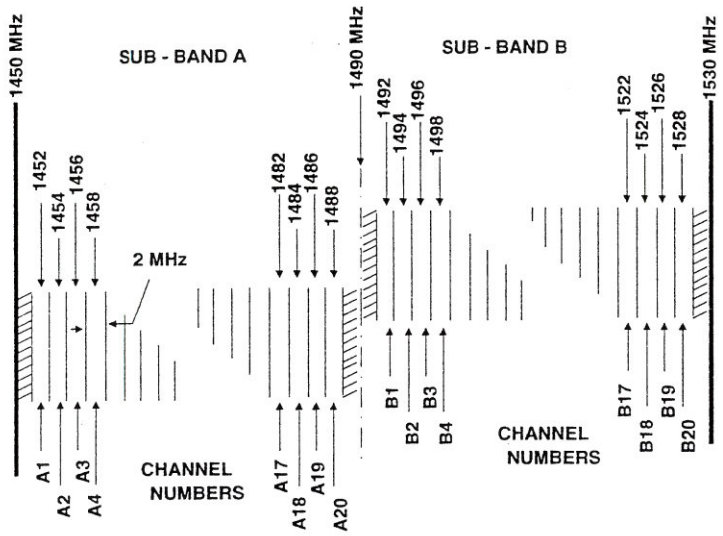


Figure R.2 Radio channelling plan

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

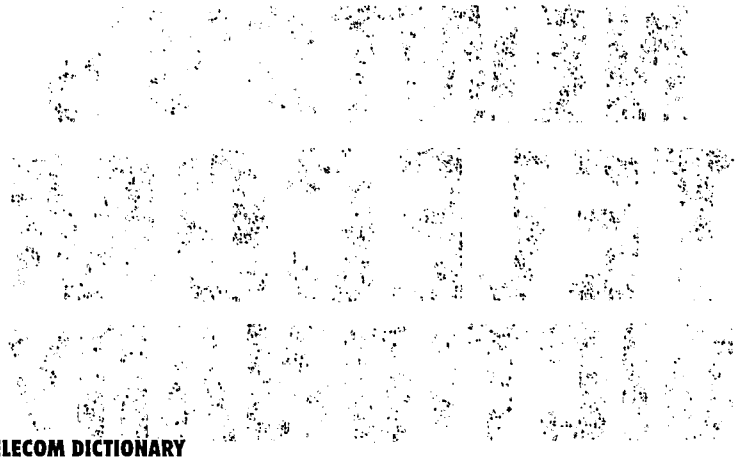
NEWTON's TELECOM DICTIONARY

26th Expanded and Updated Edition

Harry Newton

Steve Schoen, Contributing Editor

New York



NEWTON's TELECOM DICTIONARY
26th Expanded and Updated Edition

email: Harry@HarryNewton.com
book site: www.NewtonsTelecomDictionary.com
personal web site: www.HarryNewton.com
investment web site: www.InSearchOfThePerfectInvestment.com

Published in the United States by Flatiron Publishing
50 Central Park West, Suite 5C
New York, NY 10023
www.FlatironBooks.com

Printed by United Book Press
1807 White Head Road
Baltimore, MD 212074104
800-726-0120 410-944-4044 Cell phone 410-340-7878
Represented by Larry Davis

Steve Schoen, Contributing Editor
Gail Saari, Artist, Layout, Production and Cover Design

ISBN 13 digit Number 978-0-9793873-5-7

radio communication Any telecommunication by means of radio waves.

radio conformance testing A set of tests performed on a radio to ensure spectrum compatibility and conformance to design and manufacturing criteria. Radio conformance testing includes, but is not limited to, testing of channel allocation, modulation accuracy, transmitter power level adjustment accuracy, and adjacent channel interference.

radio control radio service Radio Control (R/C) is a one-way, short distance, non-voice radio service for on/off operation of devices at places distant from the operator. The FCC authorizes your R/C unit to transmit any non-voice emission type for the purpose of (1) the operator turning on and/or off a device at a remote location, or (2) an indicating device for the operator being turned on and/or off by a sensor at a remote location. You cannot communicate voice or data in the R/C. See Personal Radio Services.

radio day RADAY. 0000 ZULU through 2359 ZULU. By using ZULU time, a radio day is the exact same time period for users all around the world, irrespective of differences in their local time. See ZULU time.

radio discipline A military term for the use of proper radio techniques and operating procedures; proper equipment use; the maintenance of message security and integrity; the strict adherence to authorized radio frequencies; the keeping of messages brief; the taking of proper remedial action when communications are disrupted; and the maintenance of radio silence when ordered to do so. See circuit discipline.

Radio France Internationale France's government-funded international radio service, whose mission is to contribute to the spread of French culture worldwide. Radio France Internationale (RFI) broadcasts in French and nineteen other languages via FM radio, short-wave radio, radio relay, satellite radio, and now also by Internet radio to over 200 countries. RFI began service in 1931, and was initially called le Poste Colonial. Over the years it went through several name changes. In 1975 the service was renamed Radio France Internationale, a name which has stuck longer than any of its predecessors.

Radio Free Asia Created by Congress in 1994 and incorporated in 1996, Radio Free Asia (RFA) broadcasts news and information in Burmese, Cantonese, Khmer, Korean, Lao, Mandarin, Tibetan, Uyghur, Vietnamese, and Wu to listeners in countries where these languages are spoken. RFA also streams its radio broadcasts on the Web. Per its web site (www.rfa.org), Radio Free Asia's mission is to provide accurate and timely news and information to Asian countries whose governments prohibit access to a free press. RFA also provides information on how government firewalls can be circumvented so that blocked web sites, such as RFA's, can be accessed. See Radio Free Europe, Voice of America.

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 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 RFID. A method of identifying unique items using radio waves. Typically, a reader communicates with a tag, which holds digital information in a microchip. But there are chipless forms of RFID tags that use material to reflect back a portion of the radio waves beamed at them. For a fuller explanation, 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 interference.

radio frequency over glass See RF over glass.

Radio Hill The official or unofficial name given to hills in various places around the world, so named because their being well-situated high ground made them good locations for radio antennas. Seven states in the U.S. have a Radio Hill. There even is one in Antarctica. In countries where other languages prevail, the naming convention still exists. For example, there is a Radiokop in South Africa. The word "kop" is "hill" in Afrikaans.

radio interface unit RIU. The interface between a wireless link and a wired link, for example, between the wireless local loop and the local phone company's wired network, or between a cordless phone's base station and premises wiring, or between an air-to-ground or ship-to-shore radio link and the PSTN.

radio link budget The amount of power that must be supplied to a radio transmitter, for example, a transmitter in a cellular base station, so that the radio signals it emits reach the transmitter's specified maximum service distance with sufficient strength and quality for a receiver at that distance. The calculation of the radio link budget takes into account many variables, including, for example, transmitter frequency, distance to the receiver, receiver sensitivity limit, and the minimum signal-to-noise requirement. Radio link budget calculators are available on the Web.

radio modem A modem that transmits and receives data via radio waves. The radio modem does this by transforming bits into modulations of radio waves, and vice-versa. Also called a wireless modem.

radio-on-demand Archived radio content available on an on-demand basis. This is a slowly emerging service whose best days are ahead.

radio over IP RoIP. The use of an Internet Protocol (IP) network to interconnect disparate and/or geographically dispersed radio systems. The IP network's transport media can be anything over which IP will run, including, for example, optical fiber, coaxial cable, or twisted pair. A gateway device connects the radio system to the IP network. See also RoIP for another explanation.

radio paging access Provides attendant and phone user dial access to customer-owned radio paging equipment to selectively tone-alert, or voice-page individuals carrying pocket radio receivers. The paged party can answer by dialing an answering code from a phone within the PBX.

radio paging access with answer back Allows access to customer-provided paging systems and provides the capability in the PBX to connect the paged party when the former answers the radio page by dialing a special code from any PBX.

radio rally 1. A special broadcast by a radio station, and which may last hours or even days, whose purpose is to have listeners respond to a call to action, such as phoning in a pledge for a promoted cause. Sometimes called a radio-telethon:

2. Another term for hamfest, especially in the UK. See hamfest.

radio regulations The internationally-accepted rules governing radio communications, as issued by the ITU. The most recent edition was published in 2001.

radio resource management A management entity or subentity concerned with the operation of the radio resources management protocol. A cellular radio term.

radio resource management entity A management entity or subentity concerned with the operation of the radio resource management protocol. A cellular radio term.

radio shadow An area where radio signals weaken or disappear due to an environmental obstruction.

radio shot Industry jargon for a microwave radio link.

radio silence A period during which radios stop transmitting. It is most often associated with the military, where a radio transmission may give away a military unit's position or plans to the enemy.

radio watch A period of duty during which a radio operator maintains a vigil for radio transmissions. The term is mainly used in the military, which divides each 24-hour period into back-to-back watches. For example, the U.S.

ADDENDUM B

ADDENDUM B: TABLE OF CONTENTS

Citation	Tab
FCC, Consumer Guide, Interception & Divulgence of Radio Communications, http://www.fcc.gov/guides/interception-and-divulgence-radio-communications (last visited Sept. 24, 2013)	1
Charles Waltner, *Long Range Wifi: Filling the Gaps in the Broadband Map*, The Network: Cisco's Technology News Site (Oct. 18, 2010), http://newsroom.cisco.com/dlls/2010/hd_101810.html	2
Cisco IOS Embedded Packet Capture, http://www.cisco.com/en/US/products/ps9913/products_ios_protocol_group_home.html (last visited Sept. 24, 2013)	3
Apple, About Wireless Diagnostics, http://support.apple.com/kb/HT5606 (last visited Sept. 24, 2013)	4
Microsoft, How to Capture Network Traffic with Network Monitor, http://support.microsoft.com/kb/148942/EN-US (last visited Sept. 24, 2013).	5
Response to Defendant Google, Inc.'s Motion To Dismiss Consolidated Class Action Complaint (Jan. 25, 2011) ECF No. 64, at 8-9.	6

Federal Communications Commission

Federal Communications Commission

Guide

Interception and Divulgence of Radio Communications

Background

Interception and divulgence of radio communications is governed by many jurisdictions, including federal and state. Since September 11, 2001, many of the rules have changed. Some federal and state laws make intercepting and divulging radio communications unlawful and may subject the violator to severe criminal penalties. The Department of Justice has the authority to prosecute violators of these laws.

Unauthorized Publications of Communications

The FCC has the authority to interpret Section 705 of the Communications Act – "Unauthorized Publication of Communications." This section generally does not prohibit the mere interception of radio communications, although merely intercepting radio communications may violate other federal or state laws. This means that if you inadvertently happen to overhear your neighbor's cordless telephone conversation or listen to radio transmissions on your scanner, such as emergency service reports, you do not violate the Communications Act.

The Communications Act also allows the divulgence of certain types of radio transmissions. The law specifies that there are no restrictions on the divulgence or use of radio communications that have been transmitted for the use of the general public. Such radio communications include transmissions of a local radio or television broadcast station; announcements relating to ships, aircraft, vehicles or persons in distress; or transmissions by amateur or citizens band radio operators.

Section 705 prohibits a person from using an intercepted radio communication for his or her own benefit. One court held that, under this provision, a taxicab company may sue its competitor for wrongfully intercepting and using for its benefit radio communications between the company's dispatchers and drivers. A more recent Supreme Court decision, however, questions the ability of the government to regulate the disclosure of legally-obtained radio communications, and this area of the law remains unsettled.

In addition, the courts have determined that the act of viewing a transmission – such as a pay television signal – that the viewer was not authorized to receive is a "publication" and this violates Section 705. Section 705 also prohibits the interception of satellite cable programming for private home viewing if the programming is either encrypted (i.e., scrambled) or is not encrypted, but is sold through a marketing system. To legally intercept such a transmission, you must have authorization from the programming provider.

The Communications Act also contains provisions that affect the manufacture of equipment used for listening to or receiving radio transmissions, such as "scanners." The FCC cannot authorize scanning equipment that:

- can receive transmissions in the frequencies allocated to domestic cellular services;
- can readily be altered by the user to intercept cellular communications; or
- may be equipped with decoders that convert digital transmissions to analog voice audio.

In addition, these receivers may not be manufactured in the United States or imported for use in the United States. FCC regulations also prohibit the sale or lease of scanning equipment that is not authorized by the FCC.

Filing a Complaint

If you believe that a station has violated the contest, lottery or funds solicitation rules, you can file a complaint with the FCC. There is no charge for filing a complaint. You can file your complaint using an online complaint form. You can also file your complaint with the FCC's Consumer Center by calling 1-888-CALL-FCC (1-888-225-5322) voice or 1-888-TELL-FCC (1-888-835-5322) TTY; faxing 1-866-418-0232; or writing to:

Federal Communications Commission
Consumer and Governmental Affairs Bureau

Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, DC 20554

What to Include in Your Complaint

The best way to provide all the information the FCC needs to process your complaint is to complete fully the online complaint form. When you open the online complaint form, you will be asked a series of questions that will take you to the particular section of the form you need to complete. If you do not use the online complaint form, your complaint, at a minimum, should indicate:

- your name, address, email address and phone number where you can be reached;
- name and phone number of the company that you are complaining about and location (city and state) if the company is a cable or satellite operator;
- station call sign (KDIU-FM or WZUE TV), radio station frequency (1020 or 88.5) or TV channel (13), and station location (city and state);
- network, program name, and date and time of program if you are complaining about a particular program; and
- any additional details of your complaint, including time, date and nature of the conduct or activity you are complaining about and identifying information for any companies, organizations or individuals involved.

For More Information

For information about other communications issues, visit the FCC's Consumer and Governmental Affairs Bureau website, or contact the FCC's Consumer Center using the information provided for filing a complaint.

Print Out

Interception and Divulgence of Radio Communications Guide (pdf)

Federal Communications Commission
445 12th Street SW, Washington, DC 20554
Phone: 1-888-225-5322
TTY: 1-888-835-5322
Fax: 1-866-418-0232
Contact Us

FEATURE

Long-Range Wi-Fi: Filling the Gaps in the Broadband Map

Recent advances, open standards and economies of scale driving surprising adoption of Wi-Fi as last mile option for bringing broadband to rural areas worldwide

October 18, 2010

By Charles Waltner

A technology known as long-range Wi-Fi has become a surprising ally to the "social enterprise" Inveneo and other communications service providers worldwide that are extending the scope of affordable broadband communications.

Long-range Wi-Fi, however, is nothing new. For more than a decade, people have been beaming the Wi-Fi standard – typically used for "hotspots" and wireless home networks – over dozens of miles, says Andris Bjornson, a project engineer for Inveneo, a San Francisco-based non-profit that brings networks and computing resources to off-the-grid areas in the developing world.

More Info

Related Feature

Building Networks for Communities on the Digital Fringe

Related Links

Inveneo Website: www.inveneo.org

Ubiquiti website: www.ubnt.com

"It's all about the antenna and focusing the radio signal," he says. "You can make a decent antenna out of a Pringles can or a plastic water bottle."

But what has changed, he says, is the development of a much better selection of sophisticated gear that is far more durable and easier to manage than what comes with a snack food container.

"Long-range Wi-Fi networks have always been possible, but until recently you had to be a real geek to do it," says Kristin Peterson, the chief executive for Inveneo.

The Power of Standards

And critically, the most recent Wi-Fi standard, 802.11.n, has given long-range, or "outdoor," Wi-Fi far greater broadband capacity, signal quality and reliability than previous generations of the technology, says Ben Moore, the vice president of business development with Ubiquiti, the main supplier of Wi-Fi gear for Inveneo's networks.

"In the past three years, long-range Wi-Fi's bandwidth capabilities have increased five to 10 times," Moore says. "That definitely helps with the combination of voice, video and data now common on the Internet."

He says with such improvements long-range Wi-Fi now offers a high-quality and cost-effective alternative to fiber or other wired connections. "Installing fiber house-to-house, especially in less densely populated areas, requires years and years for a return on investment. Our products do that in only a month or two."

As they have done for Ethernet and Internet protocol (IP) technologies, economies of scale and the interoperability provided by an open standard are making Wi-Fi an increasingly attractive networking technology by driving down prices and fueling new products and advances.

For much of the early histories of Ethernet and IP, religious debates raged about the inadequacies of these technologies for taking on bigger tasks. But because of an already established base of users, vendors, and experts, Ethernet and IP continued to expand their scope of uses. Other new technologies, while theoretically better for certain tasks, simply could not match the profound advantages that came with such adoption momentum.

Now history seems to be repeating itself with Wi-Fi. Moore says Wi-Fi's popularity and improved standards have made it an attractive option for last mile Internet access and have put it "head-to-head" with a long-touted answer for wireless broadband buildouts: WiMax. "We believe our products deliver on the WiMax promise," he says.

Bjornson says alternatives like WiMax, satellites or proprietary wireless systems are either too expensive, too hard to use or just don't work as well as new long-range Wi-Fi gear. Also, because Wi-Fi is an open, unlicensed standard, Inveneo and other operators can easily set up and run mixed gear networks, such as using Cisco Linksys hotspot wireless routers with Ubiquiti's long-distance Wi-Fi equipment.

Making the Connection

Inveneo has most dramatically demonstrated the effectiveness of long-range Wi-Fi in its recent work in Haiti. There it has been able to quickly and cheaply set up a robust, ad hoc broadband network for a cadre of international relief agencies helping the country rebuild from its massive earthquake.

Crucial to the non-profit Inveneo, Ubiquiti's products are about 10 times less expensive than other options, Bjornson says. Ubiquiti's products also typically have relatively low-power demands, another plus for Inveneo's installations in areas with spotty electrical supplies, he says.

Moore says most of Ubiquiti's customers are larger telecommunications companies and "WISPs," or wireless Internet service providers. WISPs are usually small and serve 1,000 to 10,000 subscribers in rural communities where wired access from DSL, fiber optics or cable struggle to reach.

He says demand for outdoor Wi-Fi products is "accelerating" around the world, from Uruguay and Australia to Moldova and Mexico, where governments and entrepreneurs are turning to the familiar technology to speed broadband buildouts.

Moore says many of his customers are also in the United States, where Wi-Fi is helping address that country's own digital divide. According to the United States Federal Communications Commission, 14 to 24 million Americans (5 to 8 percent of the population) – typically living in poor or rural areas – don't have access to broadband connections.

While the new Wi-Fi standard has greatly improved most of the technology's previous shortcomings, some limitations remain. Most significantly, long-range Wi-Fi generally needs a clear line of sight from antenna to antenna. Also, environmental and electrical interference can degrade signals, though Moore says new techniques are successfully addressing these challenges.

And as Inveneo has discovered, the new generation of Wi-Fi gear is proving more than capable of expanding broadband to areas once thought out of its reach. "Our unofficial motto is: Get Stuff Done," Bjornson says. "We've found that long-range Wi-Fi lets us do just that."

Charles Waltner is a freelance writer in Piedmont, Calif.

Most Recent News

Cisco Delivers Network Convergence System to Power "Internet of Everything"
Today, 08:00 AM

In "Silicon Valley of the North," It Takes an Ecosystem
By Amy Cortese
9/23/2013

The Great Canadian Smartphone Race
By Kristi Essick
9/23/2013

All Featured News >>

Cisco IOS Embedded Packet Capture

HOME
PRODUCTS & SERVICES
CISCO IOS AND NX-OS SOFTWARE
CISCO IOS TECHNOLOGIES
MANAGEMENT INSTRUMENTATION
- **Cisco Embedded Automation Systems**
- **Cisco Generic Online Diagnostics (GOLD)**
- **Cisco IOS Diagnostic Tools for Commercial**
- **Cisco IOS Embedded Event Manager (EEM)**
- **Cisco IOS Embedded Packet Capture**
- **Cisco IOS IP Service Level Agreements (SLAs)**
- **Cisco IOS NetFlow**
- **Cisco IOS Service Diagnostics**
- **Data Sheets and Literature**

The Cisco IOS Embedded Packet Capture (EPC) delivers a powerful troubleshooting and tracing tool. The feature allows for network administrators to capture data packets flowing through, to, and from, a Cisco router.

EPC is a software feature consisting of infrastructure to allow for packet data to be captured at various points in the packet-processing path. The network administrator may define the capture buffer size and type (circular, or linear) and the maximum number of bytes of each packet to capture. The packet capture rate can be throttled using further administrative controls. For example, options allow for filtering the packets to be captured using an Access Control List and, optionally, further defined by specifying a maximum packet capture rate or by specifying a sampling interval.

Features and Benefits

Cisco IOS Embedded Packet Capture provides an additional level of embedded systems management not previously seen in Cisco IOS Software. The feature provides enhanced capabilities beyond those previously enabled in the Router IP Traffic Export feature. EPC includes:

- Ability to capture IPv4 and IPv6 packets in the Cisco Express Forwarding path
- A flexible method for specifying the capture buffer size and type
- EXEC-level commands to start and stop the capture
- Show commands to display packet contents on the device
- Facility to export the packet capture in PCAP format suitable for analysis using an external tool such as Wireshark

Cisco IOS Embedded Packet Capture extends the embedded management capabilities of Cisco IOS and provides another powerful tool to help resolve application and network problems. It can be particularly useful in situations where it is not practical or desirable to tap into the network using a stand-alone packet-sniffing tool or when the need arises to remotely debug or troubleshoot issues.

Technical Support and Documentation

Cisco Feature Navigator

- Product Support Information

Latest Cisco IOS Embedded Packet Capture Documentation

- Cisco IOS Embedded Packet Capture Datasheet

Data Sheets and Literature (2)

Data Sheets
White Papers

About Wireless Diagnostics

Languages English

Learn about Wireless Diagnostics, included with OS X Mountain Lion v10.8.4 and later.

Wireless Diagnostics can help you resolve wireless connectivity issues by analyzing the Wi-Fi network your Mac is connected to and providing solutions. Wireless Diagnostics is included with OS X Mountain Lion v10.8.4 and later.

If you can connect to your Wi-Fi router, but are having issues with webpages loading, sending or receiving email, music or video streaming, or downloading, use Wireless Diagnostics. After Wireless Diagnostics has completed an analysis of your Wi-Fi network, it will list any issues it finds and offer some solutions.

Wireless Diagnostics can collect detailed logs that could be provided to a network specialist, such as an IT person.

Collapse All | Expand All

How to use the Wireless Diagnostics Assistant

Can't join a Wi-Fi network?

Features and utilities

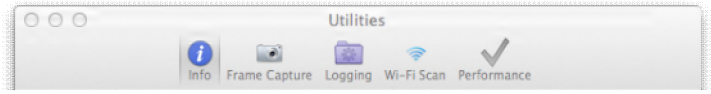
In addition to letting you quickly view extensive Wi-Fi and networking state information about your current connection (including the Wi-Fi Interface, the Wireless Environment, and your Network Configuration), Wireless Diagnostics includes:

- **The Wireless Diagnostics Assistant**
  When Wireless Diagnostics is launched it opens the Assistant, which will help identify Wi-Fi issues and provide recommendations. The Assistant is the main window of Wireless Diagnostics. Upon completion, a diagnostic report will be placed on your desktop which can be used for further analysis if an issue still exists. An option to use Monitor Mode will also be presented in the reporting window.

- **Monitor mode**
  Use Monitor mode for intermittent issues, such as unexpectedly dropped connections and auto-join issues. When an issue is detected, Monitor mode will automatically stop, indicate it's detected an issue, and collect information about what occurred. Information will be saved to the desktop as part of the Wireless Diagnostics report, so that you may share it with a network specialist.

  How to use Monitor mode

- **Utilities**
  Utilities includes additional functionality that can be helpful when resolving intermittent issues, or when working with a service provider. It consists of several tools: Info, Frame Capture, Logging, Wi-Fi Scanning, and Performance. In Wireless Diagnostics, choose **Window > Utilities**, or press Command-2. The Utilities window appears.

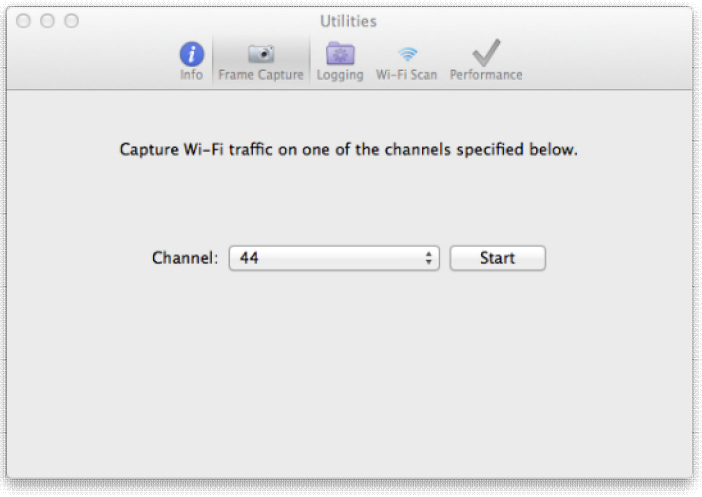


  - **Info**--Quickly view useful Wi-Fi and networking state information for your current connection in the Info window.

    What's in the Info window?

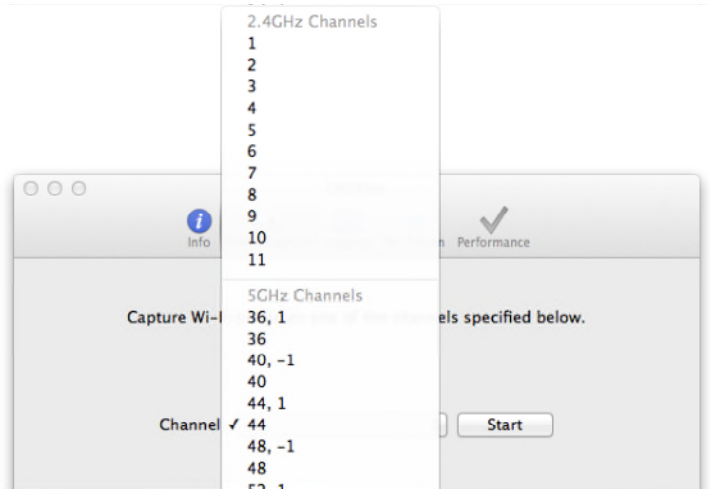
  - **Frame Capture**--This advanced utility lets you perform wireless packet captures, such as for for network and IT specialists. Use it if you want to capture Wi-Fi traffic around a reproducible issue.

    Using Frame Capture

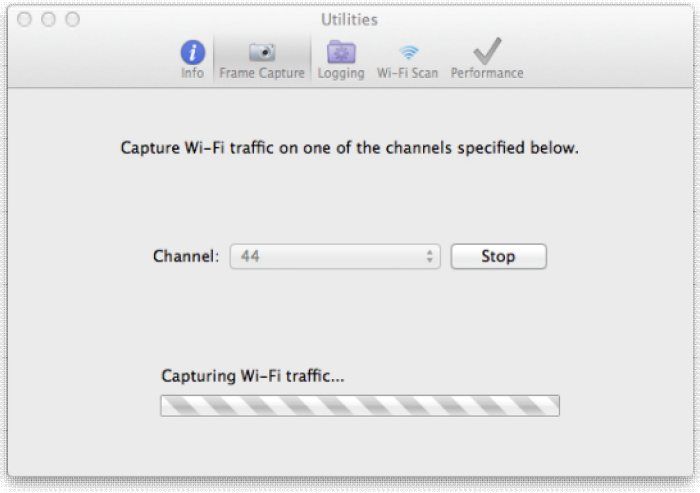


First select a channel. 5 GHz channels are denoted by 1 and -1 at the end.

- -1 indicates the channel *below* the primary channel
- 1 indicates the channel *above* the primary channel



Note: These channels are available in the United States. The list will vary by country.



Click on the Start button, and the Frame Capture will begin to capture Wi-Fi Traffic on the specified channel. Press stop if you wish to stop the capture.

A file ending in .wcap will be sent to the desktop.

130426_134358.wcap

You can use an application such as Wireshark to view the capture.

- **Logging**--Log additional important information for the Wi-Fi interface, the wireless environment, and the current network configuration, then include them in the final diagnostics report archive which will be saved to your desktop. You should enable and disable background logging for specific logs if requested by your IT network specialists.

  More information about logging

- **Wi-Fi Scanning**--Wi-Fi Scanning will examine the Wi-Fi environment around you, and let you know what Wi-Fi routers exist. It includes information on the Network name, Password Security type, Protocol, Signal Strength, and Noise, as well as Channel, Band, and Country the router is designed for.

  How to use Wi-Fi Scanning

- **Performance**--The Performance window shows information about your current connection, as well as two live signal graphs.

  Performance window details

Wi-Fi best practices

Additional Information

See Recommended settings for Wi-Fi routers and access points for recommended performance, security, and reliability settings.

Last Modified: Sep 13, 2013

Important notice for users of Windows XP: To continue receiving security updates for Windows, make sure that you're running Windows XP with Service Pack 3 (SP3). The support for Windows XP with Service Pack 3 ends April 8, 2014. If you're running Windows XP with Service Pack 3 (SP3) after support ends, to ensure that you will receive all important security updates for Windows, you need to upgrade to a later version, such as Windows 8.

For more information, see Support is ending for some versions of Windows.

How to capture network traffic with Network Monitor

Article ID: 148942 - View products that this article applies to.

System Tip

This article applies to a different version of Windows than the one you are using. Content in this article may not be relevant to you.
Visit the Windows 7 Solution Center

This article was previously published under Q148942

Notice

This article applies to Windows 2000. **Support for Windows 2000 ends on July 13, 2010.** The Windows 2000 End-of-Support Solution Center (http://support.microsoft.com/?scid=http%3a%2f%2fsupport.microsoft.com%2fwin2000) is a starting point for planning your migration strategy from Windows 2000. For more information see the Microsoft Support Lifecycle Policy (http://support.microsoft.com/lifecycle/) .

SUMMARY

The purpose of this article is to provide you with the information needed to capture network traffic from a local area network using Microsoft's Network Monitor. The text of this article comes directly from the Network Monitor's Help file and should be referenced for more detailed instructions.

MORE INFORMATION

Network Monitor is a network diagnostic tool that monitors local area networks and provides a graphical display of network statistics. Network administrators can use these statistics to perform routine trouble- shooting tasks, such as locating a server that is down, or that is receiving a disproportionate number of work requests. While collecting information from the network's data stream, Network Monitor displays the following types of information:

- The source address of the computer that sent a frame onto the network. (This address is a unique hexadecimal (or base-16) number that identifies that computer on the network.)
- The destination address of the computer that received the frame.
- The protocols used to send the frame.
- The data, or a portion of the message being sent.

The process by which Network Monitor collects this information is called capturing. By default, Network Monitor gathers statistics on all the frames it detects on the network into a capture buffer, which is a reserved storage area in memory. To capture statistics on only a specific subset of frames, you can single out these frames by designing a capture filter. When you have finished capturing information, you can design a display filter to specify how much of the information that you have captured will be displayed in Network Monitor's Frame Viewer window.

To use Network Monitor, your computer must have a network card that supports promiscuous mode. If you are using Network Monitor on a remote machine, the local workstation does not need a network adapter card that supports promiscuous mode, but the remote computer does.

To capture across networks, or to preserve local resources, use the Network Monitor Agent to capture information using a remote Windows NT computer. When you capture remotely, the Network Monitor Agent gathers statistics from a remote computer, and then sends these statistics to your local computer, where they are displayed in a local Network Monitor window.

Once data has been captured either locally or remotely, the data can be saved to a text or a capture file, and can be opened and examined at a later time.

Note The core functionality of Network Monitor, described in Help, is supported by Microsoft Product Support Services. Network-dependent tasks, such as interpreting data that you capture from your network, are not supported. The Network Monitor Agent is supported for Windows NT, but is unsupported on Windows 3.1 and Windows for Workgroups workstations.

Creating an address list

To use address pairs in a Capture filter, you should first build an address database. Once this database is built, you can use the addresses listed in the database to specify address pairs in a capture filter.

To create an address list, follow these steps:

1. From the **Capture** menu, select **Start**. Optionally, open a .cap file in the Frame Viewer window.
2. When you have finished capturing, select **Stop** and **View** from the **Capture** menu to display the Frame Viewer window.
3. From the **Display** menu, select **Find All Names**. Network Monitor processes the frames, then adds them to the address database.
4. Close the Frame Viewer window, and display the Capture window.
5. From the **Capture** menu, select **Filter** to display the **Capture filter** dialog box.
6. In the **Capture Filter** dialog box, double-click on the Address Pairs line. Or, choose **Address** in the **Add** groupbox.

Network Monitor displays the address database you have created. You can use the names in this database to specify address pairs in the Capture filter.

Capturing data between two computers

To monitor traffic between two computers, follow these steps:

1. From the **Capture** menu, choose **Filter** to display the **Capture Filter** dialog box.
2. Double-click on the ANY<->ANY line to display the **Address Expression** dialog box.
3. In the left window of the **Address Expression** dialog box, select the address of a computer.
4. In the right window of the **Address Expression** dialog box, select the address of a computer.

When you have done this, choose the **Next** button at the top of this window for more instructions.

1. In the Direction window, of the dialog box, choose one of the symbols:
    - Choose the **<-->** symbol to monitor the traffic that passes in either direction between the addresses that you have selected.
    - Choose the **-->** symbol to monitor only the traffic that passes from the address selected in the left window to the address selected in the right window.
2. Choose **OK**.
3. In the **Capture Filter** dialog box, choose **OK**.
4. From the **Capture** menu, choose **Start**.

Saving captured data

Use the Save As command to save capture statistics to a capture file or to save changes to capture files that you have modified. Later, to view frames saved to file, you can open this file and display the statistics in Network Monitor's Frame Viewer window.

To save the captured frames to a capture file or text file:

1. Do one of the following:
    - On the Toolbar, click the **File Save** button.
      -or-
    - From the **File** menu, choose **Save As**.
2. Do one the following:
    - To save the file to the current drive and directory, in the **File Name** box, specify a file name and an extension. If you are saving a file that you have modified, you cannot save it under its original name in the same directory.
    - To save the file to a network share to which you are not connected, choose the **Network** button, and then use the **Connect Network Drive** dialog box to establish the connection.
    - To save the file to a different drive or directory, do the following:
        a. In the **Drives** box, select a new drive.
        b. In the **Directories** box, select a new directory.
        c. Type the file name.
3. To save only those frame statistics that meet the specifications of the current display filter, choose **Filtered**.

   This option is available only if you are saving data from the Frame Viewer window.
4. To save a particular range of frames, type the beginning and ending frame numbers in the **From** and **To** boxes.
5. Choose **OK**.

Note When a range of frames is saved to a capture file, the numbers associated with the frames are changed; in a capture file, frame numbers always begin with 1, regardless of the number associated with the original frame. Similarly, if you apply a display filter, and then save the filtered frames, the frame numbers in the capture file begin with 1. If, however, you use the Print to File option in the Print dialog box, the original frame numbers associated with the frames are preserved.

Buffer size settings

The default buffer size is 1 megabyte (MB). To increase the buffer size so that you do not lose information, follow these steps:

1. Click **Capture**, and then click **Buffer Settings**.
2. Increase the value for the **Buffer Size (MB)** setting, and then click **OK**.

Tracing in a WAN Environment

Sometimes, you may be asked to make a capture of network traffic between two specific computers that are separated by one or more routers. In these cases, the support professional may want to analyze all network traffic between the first computer and its nearest router, and all network traffic between the second computer and its nearest router. Most of the time, this is done to check whether or not network packets are being lost or corrupted somewhere between the routers. To make these traces consistent and to be able to read these traces simultaneously, the system clocks must be synchronized between the two computers prior to making the trace. Use the following steps to synchronize time between two computers:

1. Choose the computer against which to synchronize the time.
2. From the other computer, type the command
   net time *ComputerName* /set /yes

   where *ComputerName* is the name of the computer from step 1.
3. Verify the computers have the same time by typing **TIME** at each one.
4. Proceed with the trace.

Finding Media Access Control Addresses

If the computer to be monitored is running:

- An MS-DOS-based network client, run MSD at that computer.
- Windows for Workgroups 3.11 (running TCP/IP), type **IPCONFIG /ALL** from the command line.
- Windows 95, run WINIPCFG from the command line at the local workstation.
- MacOS, Open Appletalk Control Panel. Select **User Mode** from **Edit** Menu, change mode to Advanced. Appletalk Control Panel now reveals **Info** button. Click this button to obtain the MAC address
- Windows NT, at the local console, use one of these options:
  - NET CONFIG SERVER from the command line
  - IPCONFIG /ALL from the command line
  - IPXROUTE config from the command line
  - arp -a from the command line
  - Getmac.exe from the Windows NT Resource Kit
  - WinMSD
- Windows NT, remotely, run Getmac.exe from the Windows NT Resource Kit

Properties

Article ID: 148942 - Last Review: December 11, 2005 - Revision: 7.3

APPLIES TO

- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Professional Edition
- Microsoft Windows 2000 Server
- Microsoft Windows NT Advanced Server 3.1
- Microsoft Windows NT Advanced Server 3.1
- Microsoft Windows NT Server 3.5
- Microsoft Windows NT Server 3.51
- Microsoft Windows NT Server 4.0 Standard Edition
- Microsoft Windows NT Workstation 3.1
- Microsoft Windows NT Workstation 3.5
- Microsoft Windows NT Workstation 3.51
- Microsoft Windows NT Workstation 4.0 Developer Edition
- Microsoft Windows 98 Standard Edition
- Microsoft Windows 95
- Microsoft SNA Server 2.1
- Microsoft SNA Server 3.0
- Microsoft LAN Manager to Windows NT Advanced Server Upgrade
- Microsoft Systems Management Server 1.0 Standard Edition
- Microsoft Systems Management Server 1.1 Standard Edition
- Microsoft Systems Management Server 1.2 Standard Edition
- Microsoft LAN Manager 2.2c
- Microsoft TCP/IP for Windows for Workgroups 3.11

- Microsoft TCP/IP for Windows for Workgroups 3.11a
- Microsoft TCP/IP for Windows for Workgroups 3.11b
- Microsoft Windows for Workgroups 3.11
- Microsoft Internet Information Server 1.0
- Microsoft Host Integration Server 2000 Standard Edition

Keywords: kbhowto KB148942

Give Feedback

Back to the top

SPECTOR ROSEMAN KODROFF & WILLS, PC
Jeffrey L. Kodroff, Esq.
1818 Market St., Ste. 2500
Philadelphia, PA 19103
Tel. 215-496-0300
Fax. 215-496-6611

COHEN MILSTEIN SELLERS & TOLL PLLC
Daniel A. Small, Esq.
1100 New York Avenue, NW, Suite 500W
Washington, DC 20005
Tel. 202-408-4600
Fax. 202-408-4699

Plaintiff Co-Lead Counsel

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Elizabeth J. Cabraser, Esq. (SBN: 083151)
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel. 415-956-1000
Fax. 415-956-1008

Plaintiffs' Liaison Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: GOOGLE, INC. STREET VIEW ELECTRONIC COMMUNICATIONS LITIGATION

Case No. 5:10-md-02184 JW (HRL)

PLAINTIFFS' RESPONSE TO DEFENDANT GOOGLE, INC.'S MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT

Hearing Date: March 21, 2011
Hearing Time: 9:00 a.m.
Before: Hon. James Ware

3. Whether Plaintiffs' Electronic Communications Are Readily Accessible to the General Public Is a Factual Determination That Cannot Be Resolved on a Motion to Dismiss

Google makes no argument that Plaintiffs' WiFi transmissions of electronic communications are "readily accessible to the general public" under the normal meaning of the words in that phrase. Nor could it; Plaintiffs have properly alleged that the communications Google intercepted from their WiFi networks were neither "*readily* accessible" nor readily accessible "to the general public." *See* Compl. ¶¶ 5, 18-38, 55, 60-64, 130, 142 (emphasis added). Any factual disputes Google might raise about the truth of those allegations are not properly resolved on a motion to dismiss.

First, the electronic communications transmitted between Plaintiffs' computers and their WiFi routers are not normally visible or apparent to anyone else who may be connected to their network or in the near vicinity.[8] Such communications can only be intercepted and viewed after using wireless sniffers and processing the intercepted data to make it readable. *See* Compl. ¶ 63-64. Accordingly, the communications are not readily accessible.

Second, the wireless sniffers and processing required to pluck Plaintiffs' data out of the air and to assemble it into readable content requires a level of technical sophistication not possessed by members of the general public. Thus, the sophisticated technology required to access the WiFi data is not available to the "general public," who would not know how to use such equipment even if they could obtain it. *See id.* Additionally, WiFi communications only have a range of approximately 120 feet to 600 feet (under optimal circumstances).[9] Communications sent over such a system therefore cannot be said to be "readily accessible to the general public" on any plain reading of that phrase, given the difficulty of acquiring and reassembling such communications, and when the range of the transmission system being accessed is so limited.

[8] The present situation is distinguishable from *United States v. Ahrndt*, No. 08-cr-468, 2010 WL 373994 (D. Or. Jan. 28, 2010). *See* MTD at 10. In that case, the defendant used the widely available iTunes software program and affirmatively configured it to permit any other person with the same program who connected to his WiFi network to have access to the files shared by iTunes. Affirmatively making files available for perusal and use by others connected to your network is far different than sending communications over a WiFi network that can only be accessed by others with sophisticated and complicated packet sniffing software.

[9] *See* Wi-Fi, https://secure.wikimedia.org/wikipedia/en/wiki/Wi-Fi#Reach (last visited Jan. 25, 2011).

Third, as discussed above, individuals use their home WiFi systems for e-mail, online banking, and other activities of a confidential nature. They are willing to conduct these sensitive activities because they understand the communications to be private. *See*, *e.g.*, *Warshak*, 2010 WL 5071766, at *10 ("Given the often sensitive and sometimes damning substance of his e-mails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view."); *Gonzales v. Google*, 234 F.R.D. 674, 687-88 (N.D. Cal. 2006) (noting the potentially sensitive nature of search queries). Such actions strongly demonstrate that individuals do not expect their online activities to be intercepted by others and do not understand them to be readily accessible.

Google briefly addresses these factual allegations in its motion, *see* MTD at 9 & n.5, but does not seriously contest them. Nor could it do so on a motion to dismiss, because whether the communications were "readily accessible to the general public," based on the ordinary meaning of those terms, raises factual questions that cannot be resolved on such a motion.

4. Google Intercepted Encrypted Communications

Furthermore, Google incorrectly assumes that this case only concerns unencrypted communications. To the contrary, Plaintiffs have alleged that Google's interception of "electronic communications sent or received on wireless internet connections" violates the Wiretap Act, and do not limit the Class or its allegations to unencrypted networks. *See* Compl. ¶¶ 1, 60-66, 119. Indeed, Google has stated that it intercepted encrypted communications, but contends it discarded the contents and did not record them to disk. *See* Rubin Decl. Ex. 3, at 2. Google's acknowledged interception of encrypted communications violate the Act.

5. The "Electronic Communications Systems" Were Not Configured Such that Communications are Readily Accessible to the Public.

Finally, the G1 electronic communications exception upon which Google relies applies to an electronic communication made (1) "through" an (2) "electronic communication system" that is (3) "configured" so that such (4) "electronic communication is readily accessible to the general public." "The term 'configure' is intended to establish an objective standard of design configuration for determining whether a system receives privacy protection." S. Rep. No. 541,

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BENJAMIN JOFFE; LILLA MARIGZA; RICK BENITTI; BERTHA DAVIS; JASON TAYLOR; ERIC MYHRE; JOHN E. REDSTONE; MATTHEW BERLAGE; PATRICK KEYES; KARL H. SCHULZ; JAMES FAIRBANKS; AARON LINSKY; DEAN M. BASTILLA; VICKI VAN VALIN; JEFFREY COLMAN; RUSSELL CARTER; STEPHANIE CARTER; JENNIFER LOCSIN, *Plaintiffs-Appellees*, v. GOOGLE, INC., *Defendant-Appellant*.	No. 11-17483 D.C. No. 5:10-md-02184-JW OPINION

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

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

Filed September 10, 2013

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

Opinion by Judge Bybee

SUMMARY**

Wiretap Act

The panel affirmed the district court's order denying a motion to dismiss claims that Google, Inc., violated the Wiretap Act when, in the course of capturing its Street View photographs, it collected data from unencrypted Wi-Fi networks.

The panel held that Google's data collection did not fall within a Wiretap exemption set forth in 18 U.S.C. § 2511(2)(g)(i) because data transmitted over a Wi-Fi network is not an "electronic communication" that is "readily accessible to the general public." Under 18 U.S.C. § 2510(16)(A), a "radio communication" is by definition "readily accessible to the general public" so long as it is not scrambled or encrypted. The panel held that the Wi-Fi network data collected by Google was not a radio communication, and thus was not by definition readily

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

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

accessible to the general public. The panel also held that data transmitted over a Wi-Fi network is not readily accessible to the general public under the ordinary meaning of the phrase as it is used in § 2511(2)(g)(i). Accordingly, the district court did not err in denying the motion to dismiss on the basis of the Wiretap Act exemption for electronic communication that is readily accessible to the general public.

COUNSEL

Michael H. Rubin (argued), David H. Kramer, Brian M. Willen, and Caroline E. Wilson, Wilson Sonsini Goodrich & Rosati Professional Corporation, Palo Alto, California, for Defendant-Appellant.

Elizabeth J. Cabraser (argued) and Jahan C. Sagafi, Lieff, Cabraser, Heimann & Bernstein, LLP, San Francisco, California; Kathryn E. Barnett, Lieff, Cabraser, Heimann & Bernstein, LLP, Nashville, Tennessee; Jeffrey L. Kodroff, John A. Macoretta, and Mary Ann Giorno, Spector Roseman Kodroff & Willis, P.C., Philadelphia, Pennsylvania; Daniel A. Small and David A. Young, Cohen Milstein Sellers & Toll, PLLC, Washington, D.C., for Plaintiffs-Appellees.

Marc Rotenberg, Alan Butler, and David Jacobs, Electronic Privacy Information Center, Washington, D.C., for Amicus Curiae Electronic Privacy Information Center.

OPINION

BYBEE, Circuit Judge:

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

I. BACKGROUND

A. *Facts and History*

Google launched its Street View feature in the United States in 2007 to complement its Google Maps service by providing users with panoramic, street-level photographs. Street View photographs are captured by cameras mounted on vehicles owned by Google that drive on public roads and photograph their surroundings. Between 2007 and 2010, Google also equipped its Street View cars with Wi-Fi antennas and software that collected data transmitted by Wi-Fi networks in nearby homes and businesses. The equipment attached to Google's Street View cars recorded basic information about these Wi-Fi networks, including the network's name (SSID), the unique number assigned to the router transmitting the wireless signal (MAC address), the signal strength, and whether the network was encrypted.

Gathering this basic data about the Wi-Fi networks used in homes and businesses enables companies such as Google to provide enhanced "location-based" services, such as those that allow mobile phone users to find nearby restaurants and attractions or receive driving directions.

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

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

Several putative class-action lawsuits were filed shortly after Google's announcement, and, in August 2010, the cases were transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California. In November, 2010, Plaintiffs-Appellees (collectively "Joffe") filed a consolidated complaint, asserting claims against

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

Google under the federal Wiretap Act, 18 U.S.C. § 2511; California Business and Professional Code § 17200; and various state wiretap statutes. Joffe seeks to represent a class comprised of all persons whose electronic communications were intercepted by Google Street View vehicles since May 25, 2007.

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

B. *District Court's Decision*

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

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

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

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

Finally, the court addressed whether data transmitted over unencrypted Wi-Fi networks is nevertheless an "electronic communication" that is "readily accessible to the general

[3] It is less clear whether the district court's definition also excludes television broadcasts. Joffe argued at oral argument that television broadcasts are "traditional radio services."

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

II. OVERVIEW OF THE WIRETAP ACT

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

governmental communication systems "readily accessible to the general public," including police, fire, and civil defense agencies; by a station operating on an authorized frequency for "amateur, citizens band, or general mobile radio services;" or by a marine or aeronautical communications system. 18 U.S.C. § 2511(2)(g)(ii)(I)–(IV).

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

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

As noted, § 2510(16) defines "readily accessible to the general public" solely with respect to a "radio

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

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

public," such as those transmitted by a law enforcement communications system. But this exemption is unnecessary when § 2511(2)(g)(i) already exempts all radio communications that are "readily accessible to the general public."

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

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

III. ANALYSIS

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

We reject both claims.[4] We hold that the phrase "radio communication" in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi-Fi network. As a consequence, the definition of "readily accessible to the general public [ ] with respect to a radio communication" set forth in § 2510(16) does not apply to the exemption for an "electronic communication" that is "readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i). We further hold that

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

payload data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public" under the ordinary meaning of the phrase as it is used in § 2511(2)(g)(i).

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

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

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

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

According to Google, radio communication "refers to any information transmitted using radio waves, *i.e.*, the radio frequency portion of the electromagnetic spectrum." Appellant's Br. at 28. The radio frequency portion of the spectrum is "the part of the spectrum where electromagnetic

waves have frequencies in the range of about 3 kilohertz to 300 gigahertz." *Id.* at 27.

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

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

Google's proposed definition is in tension with how Congress—and virtually everyone else—uses the phrase. In common parlance, watching a television show does not entail "radio communication." Nor does sending an email or viewing a bank statement while connected to a Wi-Fi network. There is no indication that the Wiretap Act carries a buried implication that the phrase ought to be given a broader definition than the one that is commonly understood. *See Mohamad v. Palestinian Auth.*, 132 S. Ct. 1702, 1707 (2012) (favoring a definition that matches "how we use the word in everyday parlance" and observing that "Congress remains free, as always, to give the word a broader or

different meaning. But before we will assume it has done so, there must be *some* indication Congress intended such a result").

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

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

There are two telltale indicia of a "radio communication." A radio communication is commonly understood to be (1) predominantly auditory, and (2) broadcast. Therefore, television—whether connected via an indoor antenna or a satellite dish—is not radio, by virtue of its visual component. A land line phone does not broadcast, and, for that reason, is not radio. On the other hand, AM/FM, Citizens Band (CB),

'walkie-talkie,' and shortwave transmissions are predominantly auditory, are broadcast, and are, not coincidentally, typically referred to as "radio" in everyday parlance. Thus, we conclude that "radio communication" should carry its ordinary meaning: a predominantly auditory broadcast.[5]

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

---

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

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

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

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

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

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

When read in context, the phrase "radio communication" tends to refer more narrowly to broadcast radio technologies rather than to the radio waves by which the communication

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

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

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

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

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

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

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

The definition of "readily accessible to the general public" in § 2510(16) is limited to "radio communication," and does not encompass all "electronic communication." Congress's decision to carve out "radio communication" for less protection than some other types of "electronic communication" makes sense if "radio communication" is given its ordinary meaning. Traditional radio services can be easily and mistakenly intercepted by hobbyists. *See* 132 Cong. Rec. S7987-04 (1986) ("In order to address radio hobbyists' concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services

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

Next, Google strenuously argues that the rest of the Wiretap Act supports its position that "radio communication" in 18 U.S.C. § 2510(16) means "any information transmitted using radio waves." Google leans heavily on § 2510(16)(D) and the accompanying legislative history, which together

suggest that cellular telephone and paging systems are a form of "radio communication." If cell phone and paging systems are a type of "radio communication," Google argues, it must be the case that Congress intended that the phrase include Wi-Fi networks and the rest of the radio spectrum because these technologies differ from paradigmatic radio communications like AM/FM, CB, and shortwave transmissions. But cell phone communications were not dissimilar from CB, shortwave, or other two-way forms of traditional radio broadcasts when § 2510(16)(D) was added to the Wiretap Act in 1986 as part of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848. When Congress enacted § 2510(16)(D), cell phones were still called "cellular radiotelephones." *See* H.R. Rep. No. 99-647, at 20 (1986). As with other audio broadcasts, cellular conversations were often inadvertently picked up by radio hobbyists "scanning radio frequencies in order to receive public communications." S. Rep. No. 99-541, at 3560 (1986); *see also* H.R. Rep. No. 99-647, at 20 ("Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls"). The fact that technology has evolved and cellular communications are no longer as similar to CB broadcasts as they once were does not require us to read "radio communication" to include all communications made using radio waves. Rather, the historical context surrounding Congress's protection of cellular conversations as a form of a "radio communication" is consistent with the commonsense definition of the term because, at the time of the enactment of the definition in 1986, cellular conversations could have reasonably been construed as analogous to a form of two-way

radio.[6] Assuming, *arguendo*, that the phrase "radio communication" covers cell phone transmissions as they existed in 1986 does not inevitably lead to the conclusion that it also encompasses transmissions that are plainly not predominantly auditory broadcasts, such as payload data transmitted over a Wi-Fi network.

Google also looks beyond the Wiretap Act in an effort to fit its expansive definition of "radio communication" into the statutory scheme. It points out that the Communications Act expressly defines the phrases "radio communication" and "communication by radio" broadly to include "the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds." 47 U.S.C. § 153(40). But when Congress wanted to borrow a definition from the Communications Act to apply to the Wiretap Act, it expressly said so. *See* 18 U.S.C. § 2510(1) (giving the phrase "communication common carrier" the meaning that it has "in section 3 of the Communications Act"). Here, Congress refrained from incorporating the definition of "radio

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

communication" used in the Communications Act. And, as previously discussed, the Wiretap Act uses the phrases "radio communication" and "communication by radio" differently, indicating that Congress did not intend to import the Communications Act's definition, which treats them as synonyms. *See* 47 U.S.C. § 153(40). Furthermore, the Communication Act's definition of "radio communication" encompasses technologies like television by including "the transmission by radio of . . . pictures . . . of all kinds," 47 U.S.C. § 153(40), while the Wiretap Act sometimes distinguishes them. *See, e.g.*, 18 U.S.C. § 2520(c)(1) (providing specified penalties when the "violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on [frequencies specified by regulation]"). Separate references to television-related communications would be redundant when paired with the phrase "radio communication" if we were to assume that the Communication Act's definition applied to the Wiretap Act. Importantly, the presumption that a definition set out in one part of the code is intended to govern another is hardly unyielding in the face of such contradictory evidence. *See, e.g.*, *General Dynamics Land Sys., Inc. v. Cline*, 540 U.S. 581, 595 (2004) (holding that the word "age" carries a different meaning in different sections of the ADEA); *Robinson v. Shell Oil*, 519 U.S. 337, 343 (1997) (holding that the term "employees" carries a different meaning in different sections of Title VII).

Google also leans heavily on a series of amendments to 18 U.S.C. § 2510(16) to argue that Congress impliedly gave the phrase "radio communication" a meaning other than the ordinary one that we adopt here. In 1990, Senator Patrick

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

In 1994, Congress amended § 2510(16) to add a new category of communication—which it called an "electronic communication"—that it deemed to be a "radio communication" that was not "readily accessible to the general public." In relevant part, the statute provided that "'readily accessible to the general public' means, with respect to a radio communication, that such communication is not . . . (F) an electronic communication." 18 U.S.C. § 2510(16) (1994). Google claims that Congress added § 2510(16)(F) in 1994 in order to protect from interception new technologies that transmitted data using radio frequencies, including the contemporary versions of wireless networks. There is some support for this proposition in the congressional record. *See*

H.R. Rep. No. 103-827, at 18 (1994) (explaining that the bill "[e]xtends privacy protections of the Electronic Communications Privacy Act to cordless phones and certain data communications transmitted by radio").

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

This evidence of congressional action and inaction is far more equivocal than Google acknowledges. First, the task force's report does not control what the phrase "radio communication" meant to Congress when it enacted § 2510(16) in 1986. The task force's report suggests that it thought that the "wireless data communication" technology that existed in 1991 entailed "radio communication" as the phrase is used in § 2510(16). But the task force's opinion on questions of statutory interpretation has no independent authority; it is not charged with divining congressional intent. The task force's recommendation informs us that in 1991 a

group of fifteen individuals thought that early versions of wireless networks involved "radio communication" under the statute. Their opinion is not indicative of what Congress intended when it included the phrase in the Wiretap Act. It may be considered evidence of the phrase's ordinary meaning. But it does not outweigh the more substantial evidence, discussed at length above, indicating that the ordinary meaning of "radio communication" excludes data transmitted over a Wi-Fi network.

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

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

protection for such communications offered by § 2510(16)(F) unnecessary.

Alternatively, Congress might have (correctly) determined that § 2510(16)(F) made the statute incoherent. Recall that the short-lived provision provided that "'readily accessible to the general public' means, with respect to a radio communication, that such communication is not . . . (F) an electronic communication." 18 U.S.C. § 2510(16)(F) (1994). The phrase "electronic communication" has been broadly defined since the Electronic Communications Privacy Act of 1986. In 1994, when § 2510(16)(F) was added, the Wiretap Act provided—as it still does today—that "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce." 18 U.S.C. § 2510(12). As Google stresses in its briefs, and the statute plainly states, "radio communication" is a subset of "electronic communication." Yet § 2510(16)(F) conveyed that a "radio communication" was not "readily accessible to the general public" if it was an "electronic communication," which incoherently implies that the latter was a subset of the former. The repeal of § 2510(16)(F) could, therefore, have been a housekeeping matter designed to resolve this internal tension without affecting the protection afforded "electronic communications, including data" that the 1994 Congress sought to protect.

Neither of these entirely plausible explanations for the amendment and repeal are consistent with Google's assumption that the pre-1994 conception of "radio communication" included data transmitted over a Wi-Fi

network and the 1996 repeal of § 2510(16)(F) sought to restore that conception. The point is that we do not know why the 1996 Congress deleted § 2510(16)(F). We choose to rely on the ordinary meaning of the phrase "radio communication" rather than follow a trail of enactment history that culminates in silence and then speculate as to Congress's unexpressed intent.

Finally, Google's fall back position is that the rule of lenity dictates that we accept its proposed definition of "radio communication." Although this is a civil suit, the Wiretap Act also carries criminal penalties so Google's reliance on the rule of lenity is not unfounded. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) ("Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."). But we do not resort to the rule of lenity every time a difficult question of statutory interpretation arises. Rather, "the rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a 'grievous ambiguity or uncertainty in the statute.'" *Barber v. Thomas*, 130 S. Ct. 2499, 2508 (2010) (citations omitted); *see also Smith v. United States*, 508 U.S. 223, 239 (1993) ("The mere possibility of articulating a narrower construction [ ] does not make the rule of lenity applicable. Instead, that venerable rule is reserved for cases where, '[a]fter "seizing every thing from which aid can be derived,"' the Court is 'left with an ambiguous statute.'") (citations omitted). Here, the traditional tools of statutory interpretation are sufficient. The ordinary meaning of "radio communication" is consistent with the structure of the Act and avoids absurd results without running afoul of any clearly expressed congressional intent. We need not resort to the rule of lenity where, as here, the ambiguity can be fairly resolved.

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

In the previous section, we concluded that payload data transmitted over a Wi-Fi network is not a "radio communication" under 18 U.S.C. § 2510(16). As a result, the definition of "readily accessible to the general public" in § 2510(16) does not apply to the exemption for intercepting an "electronic communication" that is "readily accessible to the general public" in § 2511(2)(g)(i). But that does not end the inquiry. Although payload data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public" *by definition* solely because it is an unencrypted "radio communication," it is still possible for a transmission that falls outside of the purview of the § 2510(16) definition to be considered "readily accessible to the general public" under the ordinary meaning of that phrase.[7] We now hold, in agreement with the district court, that payload data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public" and,

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

consequently, that Google cannot avail itself of the § 2511(2)(g)(i) exemption.

First, Wi-Fi transmissions are not "readily" available because they are geographically limited and fail to travel far beyond the walls of the home or office where the access point is located. Google was only able to intercept the plaintiffs' communications because its Street View vehicles passed by the street outside of each plaintiff's house. The FCC generally limits the peak output of Wi-Fi broadcasts to 1 watt. *See* 47 C.F.R. § 15.247(b). Meanwhile, AM, FM, and other traditional radio broadcasts typically range from 250 to 100,000 watts. *See* Fed. Commc'n Comm'n, *Encyclopedia – FM Broadcast Station Classes and Service Countours*, *available at* http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf (last visited Aug. 13, 2013); *see also* Fed. Commc'n Comm'n, *Encyclopedia – AM Broadcast Station Classes; Clear, Regional, and Local*, *available at* http://www.fcc.gov/encyclopedia/am-broadcast-station-classes-clear-regional-and-local-channels (last visited Aug. 13, 2013). As a result, AM radio stations have a service range of up to 100 miles, while individual Wi-Fi access points usually have a range of less than 330 feet. *See* Fed. Commc'n Comm'n, *Encyclopedia – Why AM Radio Stations Must Reduce Power, Change Operations, or Cease Broadcasting at Night*, http://www.fcc.gov/encyclopedia/why-am-radio-stations-must-reduce-power-change-operations-or-cease-broadcasting-night (last visited Aug. 13, 2013); Encyclopedia Brittanica Online, *Wi-Fi*, http://www.britannica.com/ EBchecked/topic/1473553/Wi-Fi (last visited Aug. 13, 2013).

Second, the payload data transmitted over unencrypted Wi-Fi networks is only "accessible" with some difficulty.

Unlike traditional radio broadcasts, a Wi-Fi access point cannot associate or communicate with a wireless device until it has been authenticated. *See* IEEE Computer Soc'y, *IEEE Standard for Information Technology — Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks — Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* 473, Fig. 11-6 (2007). Devices on Wi-Fi networks—even unencrypted networks—communicate via encoded messages sent to a specific destination over the wireless channel. *Id.* Therefore, intercepting and decoding payload data communicated on a Wi-Fi network requires sophisticated hardware and software. To capture this information, a wireless device must initiate a connection with the network and send encapsulated and coded data over the network to a specific destination. If the communications were intercepted by a traditional analog radio device they would sound indistinguishable from random noise. Wi-Fi transmissions are not "readily accessible" to the "general public" because most of the general public lacks the expertise to intercept and decode payload data transmitted over a Wi-Fi network.[8] Even if it is commonplace for

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

members of the general public to connect to a neighbor's unencrypted Wi-Fi network, members of the general public do not typically mistakenly intercept, store, and decode data transmitted by other devices on the network. Consequently, we conclude that Wi-Fi communications are sufficiently inaccessible that they do not constitute an "electronic communication . . . readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i) as the phrase is ordinarily understood.

IV. CONCLUSION

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

AFFIRMED.

---

hardly means that every keystroke—whether over a wired or a wireless connection—is "readily accessible to the general public."

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 September 24, 2013.

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/ Michael H. Rubin
Michael H. Rubin