

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

	<u>Page</u>
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

DirectTV, 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 Technol-
 ogy 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 (Cam-
 bridge 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 caselaw² 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); *DirectTV, 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.