

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 3:10-MD-2184-CRB
The Honorable James Ware, U.S. District Court Judge

**Plaintiffs-Appellees' Opposition to Google's Petition
for Rehearing and Rehearing En Banc**

SPECTOR ROSEMAN KODROFF
& WILLS, PC
Jeffrey L. Kodroff
John A. Macoretta
Mary Ann Giorno
1818 Market St., Ste. 2500
Philadelphia, PA 19103
Telephone: (215) 496-0300

COHEN MILSTEIN SELLERS
& TOLL PLLC
Daniel A. Small
David A. Young
1100 New York Avenue NW
Suite 500 West
Washington, DC 20005
Telephone: (202) 408-4600

Interim Co-Lead Counsel

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

LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP
Kathryn E. Barnett
150 Fourth Avenue North
One Nashville Place, Suite 1650
Nashville, Tennessee 37219
Telephone: (615) 313-9000

Interim Liaison Counsel

TABLE OF CONTENTS

	<u>Page</u>
I. BACKGROUND.....	2
II. GOOGLE DOES NOT MEET THE STANDARD FOR A PANEL REHEARING OR AN EN BANC HEARING.	6
III. THE PANEL PROPERLY HELD THAT WI-FI COMMUNICATIONS ARE NOT “RADIO COMMUNICATIONS” UNDER THE WIRETAP ACT.....	7
IV. GOOGLE’S POSITION WOULD UNDERMINE THE PARAMOUNT PRIVACY OBJECTIVES OF THE WIRETAP ACT...	12
V. THE PANEL’S DECISION DOES NOT JEOPARDIZE THE LEGALITY OF EVERYDAY ACTIVITIES INVOLVING WI-FI NETWORKS.	14
VI. THE PANEL PROPERLY AFFIRMED THE SUFFICIENCY OF PLAINTIFFS’ ALLEGATIONS THAT UNENCRYPTED WI-FI COMMUNICATIONS ARE NOT READILY ACCESSIBLE TO THE GENERAL PUBLIC, AND THE PANEL IGNORED NO “CRITICAL FACTS” RELEVANT TO THAT CONCLUSION.	16
VII. CONCLUSION.....	20

TABLE OF AUTHORITIES

CASES

Boardman v. Estelle,
957 F.2d 1523 (9th Cir. 1992) 11

Crowley v. Holmes
107 F.3d 15 (9th Cir. 1997) 19

Florida v. Jardines,
133 S. Ct. 1409 (2013)..... 14

Free Speech Coal. v. Reno,
220 F.3d 1113 (9th Cir. 2000) 7

*In re Application of the United States, for an Order Authorizing the
Roving Interception of Oral Commc’ns*,
349 F.3d 1132 (9th Cir. 2003) 8

In re Google Inc. Street View Elec. Commc’n Litig.,
794 F. Supp. 2d 10674 (N.D. Cal. 2011)..... 3

In re Innovatio IP Ventures, LLC Patent Litig.,
886 F. Supp. 2d 888 (N.D. Ill. 2012)..... 20

In re Pharmatrak, Inc. Privacy Litig.,
329 F.3d 9 (1st Cir. 2003)..... 12

Kyllo v. United States,
533 U.S. 27 (2001)..... 14

SEC v. McCarthy,
322 F.3d 650 (9th Cir.2003) 8

Smith v. Marsh,
194 F.3d 1045 (9th Cir. 1999) 11

United States v. Ahrndt,
475 F. App’x 656 (9th Cir. 2012)..... 16

United States v. Hall,
488 F.2d 193 (9th Cir. 1973) 19

STATUTES

18 U.S.C. § 2510(2)(g)(ii) 10
18 U.S.C. § 2510(16) 3, 6, 9, 16
18 U.S.C. § 2510(16)(D) 9
18 U.S.C. § 2511 2
18 U.S.C. § 2511(2)(a)(i) 15
18 U.S.C. § 2511(2)(g)(i) 3, 5
18 U.S.C. § 2511(2)(g)(ii) 9, 10
28 U.S.C. § 1292(b) 4
Electronic Communications Privacy Act (“ECPA”) 13

LEGISLATIVE HISTORY

H.R. Rep. 99-647 10
H.R. Rep. No. 99-647 (1986) 13
S. Rep. 99-541 10

MISCELLANEOUS

Fed. R. App. P. 40(a)(2) 7
Fed. R. App. Proc. 35(b)(1) 7
2A Sutherland Statutory Construction § 47:29 11
Ryan Spangler, *Packet Sniffer Detection with AntiSniff* (2003),
<http://www.linux-security.net/Sniffer.Detectors/snifferdetection.pdf> 15, 16

This case arises out of Google Inc.’s (“Google’s”) intentional and systematic interception of Plaintiffs-Appellees’ and proposed class members’ personal electronic data, including e-mails, passwords, and other confidential information, from Wi-Fi networks in their private homes. Four judges, including a unanimous Panel of this Court, have rejected Google’s argument that it should be categorically exempt from liability under the Wiretap Act based on its reading of the “radio communication” exemption to apply to every communication that travels on the radio frequency portion of the electromagnetic spectrum.

As the Panel pointed out, Google’s proposed interpretation of the term “radio communications” lumps together communications via such disparate devices as television, Bluetooth devices, cordless and cellular telephones, garage door openers, avalanche beacons, and wildlife tracking collars. The parties agree that the term “radio communication” should be given its ordinary meaning, but no one but Google would refer in ordinary speech to garage door openers as sending radio communications. Every judge who has interpreted the term has rejected Google’s counter-intuitive proposal to define “radio communications” to cover email correspondence traveling a few feet through the air in homes as frustrating the stated purpose and policies of the Wiretap Act. Both the District Court and this Court

instead concluded that the term's ordinary meaning is limited to traditional radio broadcasts.

Google also fails to come to grips with the fact that the Wiretap Act uses both "radio communication" and "communication by radio," and uses them differently. As the Panel correctly found, the latter term consistently is used broadly, to include all communications via radio waves, while the former is not. Google has no answer.

I. BACKGROUND.

From 2007 to 2010, Google equipped its Street View vehicles with antennas, hardware, and specially-designed software that allowed it to surreptitiously collect, decode, analyze, and store Wi-Fi data from nearby homes and businesses, including emails, passwords, and other private electronic communications that were being transmitted over those Wi-Fi networks. Google collected 600 gigabytes of private Wi-Fi data.

Benjamin Joffe and others filed class actions against Google under federal and state law, including the federal Wiretap Act, 18 U.S.C. § 2511. In an effort to avoid answering the allegations, Google moved to dismiss, arguing that its actions were categorically permitted under the Wiretap Act. Specifically, Google argued that payload data transmitted over unencrypted Wi-Fi networks falls under 18 U.S.C. § 2511(2)(g)(i) of the

Wiretap Act, which permits interception of ‘electronic communications’ that are ‘readily accessible to the general public.’” Panel Op. (Dkt. 53) (“Op.”) at 6. Google’s argument was wholly premised on its assertion that Wi-Fi transmissions are “radio communications,” and that under Section 2510(16), “radio communications” that are not “scrambled or encrypted” are deemed “readily accessible to the general public. Op. at 7.

The District Court rejected Google’s argument that all communications transmitted via the radio portion of the electromagnetic spectrum are “radio communications” under the Act. Instead, the District Court concluded that the term “radio communications” includes only “traditional radio services,” and not other technologies, such as Wi-Fi networks, that also transmit data using radio waves. *Id.* (citing *In re Google Inc. Street View Elec. Commc’n Litig.*, 794 F. Supp. 2d 1067, 1084 (N.D. Cal. 2011)). The District Court also held that Plaintiffs pled facts sufficient to show that Plaintiffs’ Wi-Fi data was not “readily accessible to the general public” “as the phrase is ordinarily understood.” Op. at 8; 794 F. Supp. 2d at 1082-83. The District Court certified the decision for interlocutory appeal under 28 U.S.C. § 1292(b), and this Court accepted the appeal. ER 2- ER 5; Op. at 6.

A unanimous Panel of this Court affirmed the District Court and found Google’s technical definition of “radio communication” to be “in tension with how Congress—and virtually everyone else—uses the phrase.” Op. at 15. The Panel held that the contemporaneous common understanding of “radio communication” did not include transmissions by every device that used radio waves, such as Wi-Fi networks, television broadcasts, Bluetooth devices, cordless and cellular telephones, garage door openers, avalanche beacons, and wildlife tracking collars. Op. at 14. Instead, the Panel found that the term “radio communications” in the Act should carry its ordinary meaning: “traditional radio technologies.” Op. at 15.

The Panel meticulously considered each of Google’s arguments in favor of a broad definition of “radio communications” that would include Plaintiffs’ Wi-Fi communications. The Panel emphasized that the Wiretap Act used two distinct phrases -- “radio communication” and “communication by radio” -- multiple times, and consistently used the former narrowly to refer to traditional radio broadcasts and consistently used the latter broadly to refer to all communications transmitted by radio waves. Noting that Congress specifically allowed interception of a few specific types of communications through exemptions in the Act, the Panel concluded that it would make little sense for Congress to have fashioned this

specific, limited list if, as Google argues, interception of virtually all communications by radio were exempt under 18 U.S.C. § 2511(2)(g)(i). Op. at 18-21.

The Panel also found that defining “radio communications” as traditional radio technologies avoids “absurd results that are inconsistent with the statutory scheme.” For instance, under Google’s overbroad proposed definition of “radio communications,” the protections of the Act would “turn on whether the *recipient* of communication decided to secure her wireless network,” no matter how sensitive or private the communication. Op. at 21-22 (emphasis in original). Google’s definition would also “obliterate” the compromise Congress struck between protecting privacy and exempting radio hobbyists from liability for inadvertent interceptions of traditional radio services. The Panel concluded that there is nothing inadvertent about using a packet sniffer to intercept payload data transmitted on Wi-Fi networks. Op. at 22-23.

The Panel also rejected Google’s argument that the Wiretap Act and its legislative history establish that cell phones and paging systems are a form of radio communication, concluding that, at the time of enactment (1986), cell phones were similar to two-way forms of traditional radio broadcasts. Op. at 23-24. Nor was the Panel persuaded by Google’s citation

to the Communication Act’s broad definition of radio communication, because Congress did not incorporate that definition into the Wiretap Act, but explicitly did borrow other definitions from the Communications Act. *Id.* at 25-26. Further, the Panel disagreed with Google that a series of amendments to Section 2510(16) implicitly supports Google’s broad interpretation of “radio communication.” *Id.* at 26-31. The Panel also rejected Google’s contention that the rule of lenity required it to accept Google’s interpretation. *Id.* at 31.

Finally, having found that Plaintiffs’ Wi-Fi communications are not “radio communications,” and thus not subject to the statutory definition of “readily accessible to the general public” in Section 2510(16), the Panel turned to the question of whether the communications are “readily accessible to the general public” under the ordinary meaning of that term. Finding that Plaintiffs pled that they are not, the Panel affirmed the District Court’s holding that Plaintiffs pled a violation of the Wiretap Act. *Op.* at 32-35.

II. GOOGLE DOES NOT MEET THE STANDARD FOR A PANEL REHEARING OR AN EN BANC HEARING.

A petition for Panel rehearing is only justified where a court “overlooked or misapprehended” a “point of law or fact.” Fed. R. App. P. 40(a)(2). An en banc hearing is “not favored” and only warranted for decisions in conflict with Supreme Court precedent or involving one or more

questions of “exceptional importance” (such as a conflict with decisions of other Courts of Appeal). *See* Fed. R. App. Proc. 35(b)(1).

Here, the Panel’s decision is in conflict with no other ruling and a denial of a motion to dismiss under the Wiretap Act merely means that Google must answer the allegations and does not raise questions of the type of exceptional importance necessary to justify en banc review. *Cf. Free Speech Coal. v. Reno*, 220 F.3d 1113 (9th Cir. 2000) (no exceptional importance re panel decision striking down provisions of Child Pornography Prevention Act of 1996 even where two other circuits found provisions constitutional).

III. THE PANEL PROPERLY HELD THAT WI-FI COMMUNICATIONS ARE NOT “RADIO COMMUNICATIONS” UNDER THE WIRETAP ACT.

After a careful and full analysis of each of Google’s arguments, the Panel properly defined “radio communications” based on the language, structure and purposes of the Wiretap Act, and consistent with Congressional intent to protect private communications within the home and with Congress’s and the public’s use of the term.

As the Panel found, Google’s proposed broad definition is contrary to how “radio communication” is commonly understood (and was at the time the statute was enacted), and would substitute a technical

definition for the term despite the fact that Congress chose *not* to provide a technical definition. Op. at 13-16. Moreover, the Panel’s definition is supported by Congress’ decision to use two distinct terms, “radio communications” and “communications by radio,” and to use them differently, with only the latter term used to refer to all communications transmitted by radio waves. Op. at 18-21, *see SEC v. McCarthy*, 322 F.3d 650, 656 (9th Cir.2003). Additionally, the Panel’s definition, unlike Google’s proposal, avoids results both absurd and inconsistent with the legislative purpose, such as protection for a communication turning on the manner in which the recipient receives it, and allowing limitless interception of unencrypted police and government agency communications. *See id.* at 21-23.¹

Google’s petition does not grapple with the vast majority of the Panel’s analysis, and does not provide a basis for rehearing. Instead, against the Panel’s solid reasoning, Google makes three failing arguments. First, Google contends the Panel erred because sections 2510(16) and

¹ Google is incorrect that the narrower definition of radio communication creates legal uncertainty regarding cell phone calls. Pet. at 11. Whether considered radio communications or not, cell phone calls are protected as wire communications. *See In re Application of the United States, for an Order Authorizing the Roving Interception of Oral Commc’ns*, 349 F.3d 1132, 1138 n.12 (9th Cir. 2003).

2511(2)(g)(ii) list types of radio communications that “are clearly not ‘predominantly auditory.’” *See* Pet. at 5-8.² Google mistakenly assumes that these sections of the Act list communications that can only be radio communications or that the statutory sections define them as radio communications.

To the contrary. Section 2510(16) simply specifies ways that radio communications cease to be “readily accessible to the general public.” It does not state or suggest that, for example, all “scrambled or encrypted” communications are radio communications. Nor is that true as a factual matter: a secure online banking session, conducted entirely over a wired internet connection, is encrypted but is not, even under Google’s definition, a radio communication because none of the information is transmitted by radio waves.

Similarly, Section 2511(2)(g)(ii) simply identifies certain radio communications that may be intercepted lawfully. It does not state or suggest – nor would it be factually accurate to do so – that the listed communications systems only transmit radio communications. For example,

² Far from being arguments Google did not previously have the opportunity to make, as Google contends, Pet. at 5, its prior submissions already “lean[ed] heavily on § 2510(16)(D) and the accompanying legislative history,” Op. at 23, and the Panel rejected those arguments.

a government website is a “governmental . . . communications system, . . . readily accessible to the general public,” but can be accessed without utilizing radio waves. As the Panel properly found, these provisions—and section 2510(2)(g)(ii) in particular—are relevant for defining “radio communication” because they list categories that *include* radio communications. Op. at 20-21. But that does not support Google’s logical leap that the categories include *only* radio communications.

Moreover, the Panel found that “radio communication[s]” are “*predominantly* auditory broadcast[s].” Op. at 17 (emphasis added). Almost all of Google’s examples of non-auditory communications are drawn from the legislative history—not the statute itself—and are incidental to or substantially similar to an auditory broadcast. *See, e.g.*, S. Rep. 99-541, at 15 (protection of radio communications sent over a system provided by a common carrier encompasses alphanumeric pagers); H.R. Rep. 99-647, at 38 (protecting audio as well as video transmissions from news teams in the field). Such examples are encompassed within “*predominantly* auditory broadcast[s]” and thus present no challenge to the Panel’s conclusion, which was based on the language and structure of the statute itself. Moreover, these examples merely quibble with the precise contours of the meaning of “radio communication,” which the Panel was not called upon to, and did not,

decide. What matters here is not whether alphanumeric pagers send radio communications, but whether home Wi-Fi networks do.

Second, Google asserts that the Panel’s interpretation conflicts with the settled meaning of “radio communication” in communications law and in what Google contends is everyday parlance. *See* Pet. at 7-8.³

However, the Panel was correct to interpret an undefined statutory term based on its “common meaning,” not technical meaning, especially when the technical meaning pertains to a different area of the law (here, communications law) than does the statute at issue (here, a privacy statute). 2A Sutherland Statutory Construction § 47:29 (7th ed.). Furthermore, Google’s other examples—packet radio and RFID—are themselves technical and industry terms, not examples of common usage of “radio communication.”

Third, Google argues that the Panel’s conclusion that Wi-Fi communications are not “radio communications” was dependent on its conclusion that television broadcasts are not “radio communications.” *See* Pet. at 8-9. This argument also fails because, as the Panel pointed out, the

³ Google did not raise this argument before the panel and has waived it. This Court’s longstanding rule that it “will not consider arguments that are raised for the first time on appeal,” *Smith v. Marsh*, 194 F.3d 1045, 1052 (9th Cir. 1999), “applies to arguments raised for the first time in a petition for rehearing.” *Boardman v. Estelle*, 957 F.2d 1523, 1535 (9th Cir. 1992).

Wiretap Act itself distinguishes radio and television communications, and other statutes do the same. Op. at 14- 15. Moreover, even if a traditional television transmission is a radio communication, it does not follow that *all* communications by radio are radio communications. Notably, references to “radio communication” in the statute and its history have much more in common than just, as Google suggests, the use of radio waves to transmit information. Pet. at 6. Every instance of “radio communication” in the Act denotes forms of radio broadcasts that are directed to the public or whose content is easily accessed. *See* Pls.’ Br. at 17-20. This interpretation is also consistent with the pro-privacy history and purposes of the statute. *See id.* at 21-26, 33-36; *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”). These are all sound reasons for concluding that Wi-Fi transmissions are not radio communications, and the reasons are in no way undermined if one concludes that television broadcasts are a type of radio communication.

IV. GOOGLE’S POSITION WOULD UNDERMINE THE PARAMOUNT PRIVACY OBJECTIVES OF THE WIRETAP ACT.

The District Court’s and the Panel’s rejection of Google’s arguments should not be disturbed because, if adopted, Google’s

interpretation of the Wiretap Act would threaten the very privacy rights that the Act was enacted to protect. *See* H.R. Rep. No. 99-647, at 16-19 (1986) (stating that one of Congress' goals in passing the Electronic Communications Privacy Act ("ECPA") and updating the Wiretap Act was to keep privacy protection of electronic communication consistent with expectations arising from the Fourth Amendment). Specifically, Google contends that the content of an e-mail loses protection under the Wiretap Act simply because it travels a short distance in the home from a laptop to a router. As the District Court explained in rejecting Google's proposition,

Interpreting the ECPA such that the statute provides obscure limitations on the protection of emails and other computer-to-computer communications based on the particular medium that transmitted the electronic communication would render the Wiretap Act, and the efforts of the 99th Congress to provide such protections, absurd. Under such an interpretation, the Act would provide a private civil right of action, and even impose criminal liability, for the interception of emails transmitted over an ethernet cable through a wired network, but would stop short at protecting those very same emails should they pass momentarily over radio waves through a Wi-Fi network established to transmit data within a home.

ER 24-ER 25.

Moreover, Google's interpretation of the Act would undermine privacy within the home, which has received substantial protection under the Fourth Amendment. *See, e.g., Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013)("[W]hen it comes to the Fourth Amendment, the home is first among

equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable government intrusion.' This important right would be of little practical value if the State's agents could stand in a home's porch or side garden and trawl for evidence with impunity" (citations omitted)); *see also Kyllo v. United States*, 533 U.S. 27 (2001) (holding that Fourth Amendment requires a warrant for police to use a thermal imaging device outside a home to detect heat sources emanating from inside).

Here, unlike the searchers in Fourth Amendment cases, Google can invoke no law enforcement authority or national security interest to justify its intrusion; it collected private data solely for its own commercial use. The right reaffirmed in *Jardines* should be doubly secure against such breach. The Panel's interpretation is consistent with common usage, promotes the statutory purpose, and protects the reasonable expectation of privacy in the home.

V. THE PANEL'S DECISION DOES NOT JEOPARDIZE THE LEGALITY OF EVERYDAY ACTIVITIES INVOLVING WI-FI NETWORKS.

Google's argument that the ruling casts doubt about whether packet-sniffing used for enterprise security will violate the Wiretap Act is unfounded. *See* Pet. at 16-17. Packet-sniffing as used by computer network

IT personnel does not violate the Wiretap Act because the IT personnel have permission to intercept and decode payload data being transferred on the Wi-Fi network. *See* 18 U.S.C. § 2511(2)(a)(i) (permitting providers of electronic communication service to intercept to extent necessary to maintain service), (2)(c) (permitting interception with consent); *see also* Ryan Spangler, *Packet Sniffer Detection with AntiSniff*, (2003), <http://www.linux-security.net/Sniffer.Detectors/snifferdetection.pdf> (“Commercial packet sniffers are used to help maintain networks...”). Likewise, a homeowner may engage in packet-sniffing if she wants to monitor the efficiency of her own Wi-Fi network. *See id.* However, if an unauthorized party were to engage in packet sniffing on a homeowner’s network, as did Google, this is hacking and a violation of the Wiretap Act. *See id.* (“[U]nderground packet sniffers are used by attackers to gain *unauthorized access to remote hosts.*”) (Emphasis added).

Likewise, contrary to Google’s assertions, the ruling does not make the ordinary operation of Wi-Fi-enabled devices illegal, *see* Pet. at 17-18. Such devices do not – as Google did here – intercept, process and store the transmission of every Wi-Fi network in reach.

Nor does Google’s citation (Pet. at 17) to *United States v. Ahrndt*, 475 F. App’x 656 (9th Cir. 2012) support its position. *Ahrndt* does

not involve the interception and decoding of Wi-Fi transmissions, but rather deals with undeveloped facts pertaining to whether the plaintiff intentionally enabled the file sharing feature on his network, which ultimately resulted in the Ninth Circuit remanding the case for “further factfinding.” *Id.* at 658.

VI. THE PANEL PROPERLY AFFIRMED THE SUFFICIENCY OF PLAINTIFFS’ ALLEGATIONS THAT UNENCRYPTED WI-FI COMMUNICATIONS ARE NOT READILY ACCESSIBLE TO THE GENERAL PUBLIC, AND THE PANEL IGNORED NO “CRITICAL FACTS” RELEVANT TO THAT CONCLUSION.

Because Wi-Fi transmissions are not radio communications, 18 U.S.C. § 2510(16)’s definition of radio communications that are “readily accessible to the general public” does not apply. And because the Wiretap Act defines “readily accessible to the general public” only with respect to radio communications, the Panel correctly looked to the ordinary meaning of the phrase “readily accessible to the general public” to evaluate Plaintiffs’ allegations regarding Wi-Fi transmissions. *Op.* at 32 n.7. Based on that ordinary meaning, the Panel affirmed the District Court’s conclusion that Plaintiffs sufficiently pled that the unencrypted Wi-Fi transmissions intercepted by Google were not “readily accessible to the general public.” *Op.* at 32-35; ER 23-ER 26.⁴

⁴ Google’s mischaracterization of the Panel’s affirmance of the sufficiency of Plaintiffs pleadings as a factual finding is not supported by the language [footnote continued on next page]

The Panel affirmed the District Court's holding on two grounds: Wi-Fi transmissions' geographical limits and the sophisticated hardware and software needed to intercept them. Op. at 33-34. This was not beyond the scope of the District Court's holding, or this appeal, as Google argues. Pet. at 12. In holding that Wi-Fi networks are not readily accessible to the general public, the District Court specifically noted Plaintiffs' allegations concerning the need to use "technology allegedly outside the purview of the general public." ER 25. In their appellate brief, Plaintiffs directly defended the sufficiency of their allegations that Wi-Fi communications are not readily accessible to the general public, again pointing to the need for sophisticated software and hardware to intercept these communications and the short distances that Wi-Fi transmissions travel. Appellees' Br. at 37-38, 43-44. In its reply brief, Google responded by comparing cellular and Wi-Fi communications and through factual material from several websites concerning both the distance Wi-Fi transmissions travel and the relative difficulty of intercepting Wi-Fi communications. See Reply Br. at 24-26 and n.9.

of the Panel's decision, especially when it is clear that the Panel was reviewing a ruling on a Rule 12(b)(6) motion to dismiss.

Considering this whole record, the Panel properly affirmed the District Court's conclusion that Plaintiffs' allegations are sufficient to state a claim under the Wiretap Act. Thus, the Panel's conclusions on this issue were not the result of "ad hoc fact finding," as Google asserts (Pet. at 12-13), but came directly from issues that the parties and the District Court directly addressed. There is no basis for Google's request to strike this part of the Panel's decision, and Google provides no authority for it.

Moreover, Google's arguments do not challenge the sufficiency of Plaintiffs' allegations under this ordinary meaning of "readily accessible to the general public." Rather, Google offers "critical facts" that it contends undercut the veracity of Plaintiffs' allegations. As such, they are wholly misplaced at this stage of the litigation and irrelevant to a request for rehearing. And even if they were relevant, they provide no basis for granting Google's petition.

First, Google is wrong that "everyone agrees" that Wi-Fi transmissions "are broadcast by radio." *See* Pet. at 15. Plaintiffs argued, and both the District Court and the Panel agreed, that these Wi-Fi transmissions are not publicly broadcast by radio. *See* Op. at 15, 17; ER 24.

Next, Google cites an outdated case to argue that "broadcasting communications into the air by radio waves is more analogous to carrying

on an oral communication in a loud voice or with a megaphone then it is to the privacy afforded by wire.” Pet. at 15 (citing *United States v. Hall*, 488 F.2d 193, 198 (9th Cir. 1973); *superseded by statute as stated in Crowley v. Holmes*, 107 F.3d 15 (9th Cir. 1997)). *Hall*, however, dealt with the interception of oral conversations over radio-telephones, which are similar to walkie-talkies and akin to traditional radio broadcasts. *See Hall*, 488 F.2d at 194-195. *Hall* has nothing to do with electronic Wi-Fi communications containing payload data that travel within the home via radio waves.

Additionally, Google seeks to convince this Court that its surreptitious collection of 600 gigabytes of Wi-Fi data was no more invasive than “free-riding” a neighbor’s Wi-Fi network to access the Internet. *See* Pet. at 15-16. To the contrary, however, Google intentionally went far beyond identifying home-based wireless networks or even surfing the Internet over them. Rather, Google intercepted, decoded, and stored personal information in Wi-Fi transmissions traveling a very short distance from a computer to a router within the home. *See Op.* at 33. Thus, Google’s argument does not provide any reason to grant its Petition.

Finally, Google contends that the Panel ignored the “critical fact” that hardware and software used to intercept and decode payload data

may be purchased or downloaded from the Internet. Pet. at 16. To the contrary, the Panel directly acknowledged and then squarely rejected

Google's argument:

The availability of the technology necessary to intercept the communication cannot be the sole determinant of whether it is "readily accessible to the general public" as the phrase is ordinarily understood. A device that surreptitiously logs a computer user's keystrokes can be purchased online and easily installed, but that hardly means that every keystroke—whether over wires or a wireless connection—is "readily accessible to the general public."

Op. at 34 fn. 8.⁵

VII. CONCLUSION.

For the foregoing reasons, Google's petition for rehearing and rehearing en banc should be denied.

⁵ Also, the Panel considered and rejected the conclusion of the district court in *In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 893 (N.D. Ill. 2012), the only case cited by Google in support of its position.

Dated: October 30, 2013

Respectfully submitted,

By: /s/ Jeffrey L. Kodroff

Jeffrey L. Kodroff
John A. Macoretta
Mary Ann Giorno
SPECTOR ROSEMAN KODROFF &
WILLIS, P.C.
1818 Market Street, 25th Floor
Philadelphia, PA 19103
Telephone: (215) 496-0300

By: /s/ Daniel A. Small

Daniel A. Small
David A. Young
COHEN MILSTEIN SELLERS &
TOLL, PLLC
1100 New York Ave., NW
Suite 500 West
Washington, DC 20005
Telephone: (202) 408-4600

Interim Co-Lead Counsel

Dated: October 30, 2013

By: /s/ Elizabeth J. Cabraser

Elizabeth J. Cabraser
LIEFF, CABRASER, HEIMANN
& BERNSTEIN, LLP
275 Battery St., 29th Floor
San Francisco, CA 94111
Telephone: (415) 956-1000

Kathryn E. Barnett
LIEFF, CABRASER, HEIMANN
& BERNSTEIN, LLP
150 Fourth Avenue, North, Suite 1650
Nashville, TN 37219
Telephone: (615) 313-9000

Interim Liaison Counsel

CERTIFICATE OF SERVICE

I hereby certify that on October 30, 2013, 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. 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.

Dated: October 30, 2013

LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP

By: /s/ Elizabeth J. Cabraser

Elizabeth J. Cabraser
LIEFF CABRASER HEIMANN &
BERNSTEIN, LLP
275 Battery St., 29th Floor
San Francisco, CA 94111
(415) 956-1000

CERTIFICATE OF COMPLIANCE

I, Jeffrey L. Kodroff, hereby certify that this brief complies with the type face requirements of Fed. R. App. P. 32(a)(5) and the type style requirement of Fed. R. App. P. 32(a)(6) because it has been prepared in proportionally spaced type-face using Microsoft Word in 14-point Times New Roman font.

This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 4,165 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

Dated: October 30, 2013

/s/ Jeffrey L. Kodroff

Jeffrey L. Kodroff
SPECTOR ROSEMAN KODROFF &
WILLIS, P.C.
1818 Market Street, 25th Floor
Philadelphia, PA 19103
Telephone: (215) 496-0300