

13-1181
No. 13-1

Supreme Court, U.S.
FILED

MAR 27 2014

OFFICE OF THE CLERK

IN THE
Supreme Court of the United States

GOOGLE INC.,

Petitioner,

v.

JOFFE, *et al.*,

Respondents.

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

PETITION FOR A WRIT OF CERTIORARI

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

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

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

QUESTION PRESENTED

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

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

PARTIES TO THE PROCEEDINGS

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

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

CORPORATE DISCLOSURE STATEMENT

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

TABLE OF CONTENTS

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

TABLE OF CONTENTS—Continued

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

TABLE OF CONTENTS—Continued

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

TABLE OF AUTHORITIES

CASES

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

TABLE OF AUTHORITIES—Continued

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

STATUTES AND REGULATIONS

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

TABLE OF AUTHORITIES—Continued

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

LEGISLATIVE MATERIALS

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

OTHER AUTHORITIES

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

TABLE OF AUTHORITIES—Continued

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

TABLE OF AUTHORITIES—Continued

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

IN THE
Supreme Court of the United States

No. 13-

GOOGLE INC.,

Petitioner,

v.

JOFFE, *et al.*,

Respondents.

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

PETITION FOR WRIT OF CERTIORARI

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

OPINIONS BELOW

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

JURISDICTION

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

STATUTORY PROVISIONS INVOLVED

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

INTRODUCTION AND STATEMENT

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

1. The Wiretap Act broadly prohibits the interception of wire and electronic communications, but allows interception of “an electronic communication made through an electronic communication system that is

configured so that such electronic communication is readily accessible to the general public.” 18 U.S.C. § 2511(2)(g)(i). The Act expressly provides that “radio communications” are “readily accessible to the general public”—and thus exempt from the prohibition on interception—if they are not “scrambled or encrypted” (or transmitted in another restricted manner specified in the Act). *Id.* § 2510(16)(A). The question at issue in this case is whether unencrypted Wi-Fi communications, which are undisputedly carried over radio waves, are “radio communications” and thus not subject to the Wiretap Act’s ban on interception.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The court of appeals denied Google's request for rehearing en banc on December 27, 2013.²

REASONS FOR GRANTING THE PETITION

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

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

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

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

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

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

A. The Ninth Circuit's Interpretation Is Inconsistent With The Established Meaning Of "Radio Communication" In The Telecommunications Field And Under Federal Law

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

basic modern technologies such as television and cell phone communications.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

* * *

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

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

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

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

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

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

MARCH 2014