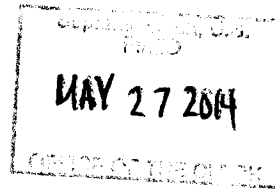


No. 13-1181



---

IN THE  
**Supreme Court of the United States**

---

GOOGLE INC.,  
*Petitioner,*  
v.

BENJAMIN JOFFE, ET AL.,  
*Respondents.*

---

**On Petition for a Writ of Certiorari  
to the United States Court of Appeals  
for the Ninth Circuit**

---

**BRIEF FOR RESPONDENTS IN OPPOSITION**

---

DANIEL A. SMALL  
DAVID A. YOUNG  
COHEN MILSTEIN SELLERS  
& TOLL, PLLC  
1100 New York Avenue, N.W.  
Suite 500 West  
Washington, D.C. 20005  
(202) 408-4600

JEFFREY L. KODROFF  
JOHN A. MACORETTA  
MARY ANN GEPPERT  
SPECTOR ROSEMAN  
KODROFF & WILLIS, P.C.  
1818 Market Street  
25th Floor  
Philadelphia, PA 19103  
(215) 496-0300

ELIZABETH J. CABRASER  
*Counsel of Record*  
MICHAEL W. SOBOL  
NICOLE D. SUGNET  
LIEFF, CABRASER, HEIMANN  
& BERNSTEIN, LLP  
275 Battery Street  
29th Floor  
San Francisco, CA 94111  
(415) 956-1000  
(ecabraser@lchb.com)

May 27, 2014

---

**BLANK PAGE**

### **QUESTION PRESENTED**

Whether the Ninth Circuit correctly rejected, on interlocutory review of a decision denying Google's motion to dismiss, Google's contention that 18 U.S.C. § 2511(2)(g)(i) categorically authorized its nationwide, surreptitious interception of data from unencrypted, private, in-home WiFi networks.

## TABLE OF CONTENTS

	Page
QUESTION PRESENTED .....	i
TABLE OF AUTHORITIES .....	iii
INTRODUCTION .....	1
STATEMENT.....	2
A. Google’s Street View Vehicles Surrepti- tiously Capture Personal Data .....	2
B. Proceedings Below .....	5
REASONS FOR DENYING THE PETITION .....	10
I. THIS COURT’S REVIEW IS NOT WARRANTED .....	10
A. There Is No Circuit Split for This Court To Resolve.....	10
B. The Petition Seeks Interlocutory Review of an Issue That Is Not Case Dispositive.....	12
C. The Ninth Circuit’s Decision Raises No Issues of National Importance.....	16
II. THE NINTH CIRCUIT’S JUDGMENT IS CORRECT.....	21
A. The Ninth Circuit Correctly Inter- preted the Phrase “Radio Communi- cation” in § 2510(16) .....	21
B. Alternative Grounds on Which To Affirm the Judgment Exist.....	25
CONCLUSION.....	26

## TABLE OF AUTHORITIES

	Page
CASES	
<i>Application of the United States for an Order Authorizing the Roving Interception of Oral Communications, In re</i> , 349 F.3d 1132 (9th Cir. 2003) .....	19
<i>Arizona v. Evans</i> , 514 U.S. 1 (1995).....	12
<i>Barnhart v. Sigmon Coal Co.</i> , 534 U.S. 438 (2002) .....	22
<i>Brotherhood of Locomotive Firemen &amp; Engine- men v. Bangor &amp; A.R.R. Co.</i> , 389 U.S. 327 (1967) .....	12
<i>Bunting v. Mellen</i> , 541 U.S. 1019 (2004) .....	12
<i>Camreta v. Greene</i> , 131 S. Ct. 2020 (2011) .....	16
<i>Environmental Def. v. Duke Energy Corp.</i> , 549 U.S. 561 (2007) .....	25
<i>FDIC v. Meyer</i> , 510 U.S. 471 (1994).....	21
<i>Innovatio IP Ventures, LLC Patent Litig., In re</i> , 886 F. Supp. 2d 888 (N.D. Ill. 2012) .....	20
<i>Martin v. Blessing</i> , 134 S. Ct. 402 (2013) .....	12
<i>Mohamad v. Palestinian Auth.</i> , 132 S. Ct. 1702 (2012) .....	2
<i>Mount Soledad Mem'l Ass'n v. Trunk</i> , 132 S. Ct. 2535 (2012).....	12, 13
<i>Reno v. Bossier Parish Sch. Bd.</i> , 528 U.S. 320 (2000) .....	25

*United States v. Ahrndt:*

No. 08-cr-468-KI, 2010 WL 373994 (D. Or. Jan. 28, 2010), <i>rev'd and remanded</i> , 475 F. App'x 656 (9th Cir. 2012) .....	20, 21
No. 08-cr-468-KI, 2013 WL 179326 (D. Or. Jan. 17, 2013) .....	21

## ADMINISTRATIVE DECISIONS

Notice of Apparent Liability for Forfeiture, <i>Google Inc.</i> , 27 FCC Rcd 4012 (Enf. Bur. 2012).....	3, 5
---	------

## CONSTITUTION, STATUTES, AND RULES

U.S. Const. art. III .....	14
Communications Act of 1934, 47 U.S.C. § 151 <i>et seq.</i> .....	9, 10, 23, 24
47 U.S.C. § 153(40) .....	24
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 .....	6, 22
§ 101(a)(6), 100 Stat. 1849 .....	6
§ 101(b)(4), 100 Stat. 1850 .....	6
Wiretap Act, 18 U.S.C. § 2510 <i>et seq.</i> .....	<i>passim</i>
§ 2510(1).....	15, 18, 24
§ 2510(2).....	15, 18
§ 2510(12).....	26

§ 2510(12)(A).....	15, 18
§ 2510(16).....	5, 6, 7, 11, 12, 13, 21, 25
§ 2510(16)(A).....	6
§ 2511(1)(a) .....	5, 17
§ 2511(2)(d) .....	16, 19
§ 2511(2)(g)(i).....	5, 6, 11, 15, 16, 19, 25, 26
§ 2511(2)(g)(ii).....	25
§ 2511(2)(g)(ii)(II) .....	6
§ 2520(a).....	5
§ 2520(c)(1).....	24
28 U.S.C. § 1292(b) .....	7
Sup. Ct. R. 10(a).....	12

## LEGISLATIVE MATERIALS

S. Rep. No. 99-541 (1986), <i>reprinted in</i> 1986 U.S.C.C.A.N. 3555 .....	23
--	----

## ADMINISTRATIVE MATERIALS

Administrative Office of the U.S. Courts, Pri- vacy Notice, <a href="http://www.uscourts.gov/Common/PrivacyPolicy.aspx">http://www.uscourts.gov/ Common/PrivacyPolicy.aspx</a> .....	17
Federal Communications Comm'n, <i>Consumer Guide: Voice over Internet Protocol (VoIP)</i> , <a href="http://transition.fcc.gov/cgb/consumerfacts/voip.pdf">http://transition.fcc.gov/cgb/consumerfacts/ voip.pdf</a> .....	15-16

## OTHER MATERIALS

- Assurance of Voluntary Compliance, [http://www.ct.gov/ag/lib/ag/press\\_releases/2013/20130312\\_google\\_avc.pdf](http://www.ct.gov/ag/lib/ag/press_releases/2013/20130312_google_avc.pdf) ..... 4
- Kim Young-won, *Google fined W210m for data gathering*, The Korea Herald (Jan. 28, 2014), *available at* <http://www.koreaherald.com/view.php?ud=20140128001166>..... 4
- Stephanie Bodoni, *Google Faces Norway Fine on Street View Data Collection*, Bloomberg News (Aug. 10, 2012), *available at* <http://www.bloomberg.com/news/2012-08-10/google-faces-norway-fine-on-street-view-data-collection.html>..... 4



## INTRODUCTION

As Google's Street View cars drove across the country — and around the world — from 2007 to 2010, Google, like a 21st century Peeping Tom, surreptitiously intercepted and recorded private communications from inside people's homes as the data traveled between people's computers, smartphones, and tablets, and their WiFi routers. When caught, Google initially denied that it had intercepted and recorded those private data. Once forced to admit this intrusion, Google acknowledged that what it did was wrong — it had “screwed up,” in its terms — and regulators domestic and foreign have rightly sanctioned Google for this privacy transgression.

Google claims that the U.S. citizens whose data it secretly captured cannot bring an action against Google for statutory damages under the Wiretap Act. Google claims that Congress — in seeking to expand the privacy protections of ordinary citizens in the face of increasingly intrusive technology — actually authorized its massive and secret interception of private communications for the brief moment they traveled over the plaintiffs' home WiFi networks.

Google's petition asks this Court to step out of its traditional role and instead to serve as a court of error correction, so that it may decide, on interlocutory review, a question of statutory interpretation, even though no state or federal appellate court has ruled differently from the Ninth Circuit.

Moreover, Google's entire claim amounts to the deeply counterintuitive proposition that, in protecting ham radio hobbyists, Congress authorized a massive intrusion of private wireless communications within the home because the last few feet — or inches — of transmission used unencrypted radio waves.

However the boundaries of privacy protections under new technology may ultimately be defined, this case does not come close to the border. The conduct Google wishes Congress had condoned is simply the modern version of a voyeur who lurks, unobserved, within view of the window of a home hoping to steal a glimpse of a private moment. The district court and the Ninth Circuit correctly rejected Google's argument.

The Court should deny Google's petition.

## STATEMENT

### A. Google's Street View Vehicles Surreptitiously Capture Personal Data

For the publicly stated purpose of adding Street View images to its Maps product, Google outfitted a fleet of vehicles with multi-directional cameras, wireless network antennae, and other customized hardware to create a sophisticated mobile data-collection system. *See* Consol. Class Action Compl. ¶¶ 55-59.<sup>1</sup>

Beyond this publicly announced purpose, Google had an additional, secret purpose. *See id.* ¶¶ 1-3. Google deliberately equipped its fleet of vehicles with devices and custom programming (for which it sought a patent), and dispatched them across the United States (and the world) to connect automatically to any WiFi network within range of the streets that the vehicles traveled. *See id.* ¶¶ 60-65, 72-73. Once connected to a WiFi network, Google's proprietary technology surreptitiously captured, parsed, and recorded data sent across the WiFi networks from

---

<sup>1</sup> Because this petition arises from a ruling on a motion to dismiss, the factual allegations in the complaint must be accepted as true. *See, e.g., Mohamad v. Palestinian Auth.*, 132 S. Ct. 1702, 1705 (2012).

connected devices (such as a smartphone, laptop computer, or tablet), known as the “payload data.” *See id.* ¶¶ 4, 60-65, 72-73. The payload data Google collected comprise user content including whole emails, usernames, passwords, web addresses, video and audio files, and even voice communications sent across the Internet using the Voice over Internet Protocol (“VoIP”). *See id.* ¶¶ 4, 66, 77.

From 2007 to 2010, Google intercepted and stored at least 600 gigabytes of data — approximately 200 gigabytes in the United States alone<sup>2</sup> — from WiFi networks to which its Street View vehicles connected. *See id.* ¶¶ 55, 73.

Google’s collection of WiFi payload data occurred in secret until 2010, when German regulators requested information about Google’s data collection practices. *See id.* ¶ 69. At first, Google falsely claimed that its vehicles collected only the names of WiFi networks and the identification number (known as a MAC address) assigned to the WiFi hardware, and not payload data. *See id.* ¶¶ 69-70. But when German regulators pressed to verify these claims, Google admitted that it had programmed its fleet of Street View vehicles to intercept and store payload data, though Google continued to conceal the extent of its collection by claiming that it had collected only “fragmentary” sampling data that did not include complete emails and other files. *See id.* ¶¶ 70-73, 75-77. Google later was forced to admit that this claim, too, was false. *See id.* ¶ 77.

---

<sup>2</sup> *See* Notice of Apparent Liability for Forfeiture, *Google Inc.*, 27 FCC Rcd 4012, ¶ 24 (Enf. Bur. 2012) (“*Google NAL*”), largely unredacted version available at <http://goo.gl/KfMJ31>.

In several public statements following these revelations, senior officers and directors of Google, including co-founder Sergey Brin and then-CEO Eric Schmidt, admitted that Google's Street View fleet had intercepted a wide range of sensitive personal information that Google should not have collected. *See id.* ¶¶ 75-77. Eric Schmidt candidly admitted, "We screwed up. Let's be clear about that." *Id.* ¶ 75. Sergey Brin likewise admitted, "In short, let me just say that we screwed up." *Id.*

A slew of criminal and regulatory investigations followed. *See id.* ¶¶ 81-109. In March 2013, Google entered into a voluntary settlement agreement with a group of 38 state attorneys general, in which Google did not admit liability but nonetheless agreed to pay a \$7 million fine.<sup>3</sup> In January 2014, the Korea Communication Commission fined Google 210 million Won (about \$200,000).<sup>4</sup> The Norwegian Data Protection Authority fined Google 250,000 Kroner (about \$50,000) in August 2012.<sup>5</sup> Norway's data-protection commissioner described that fine as "one of the biggest fines [it had] imposed."<sup>6</sup>

In 2012, the Federal Communications Commission's Enforcement Bureau also fined Google \$25,000 for "deliberately impeded[ing] and delay[ing]" its "in-

---

<sup>3</sup> *See* Assurance of Voluntary Compliance, [http://www.ct.gov/ag/lib/ag/press\\_releases/2013/20130312\\_google\\_avc.pdf](http://www.ct.gov/ag/lib/ag/press_releases/2013/20130312_google_avc.pdf).

<sup>4</sup> Kim Young-won, *Google fined W210m for data gathering*, The Korea Herald (Jan. 28, 2014), *available at* <http://www.koreaherald.com/view.php?ud=20140128001166>.

<sup>5</sup> Stephanie Bodoni, *Google Faces Norway Fine on Street View Data Collection*, Bloomberg News (Aug. 10, 2012), *available at* <http://www.bloomberg.com/news/2012-08-10/google-faces-norway-fine-on-street-view-data-collection.html>.

<sup>6</sup> *See id.*

vestigation by failing to respond to requests for material information,” and “willfully and repeatedly violat[ing] Commission orders to produce certain information and documents that the Commission required for its investigation.”<sup>7</sup> Despite Google’s lack of cooperation, the Bureau found that the engineer who designed the Street View collection software had “intended to collect, store, and analyze payload data from unencrypted Wi-Fi networks,” and that “other members of the Street View project” were aware of this capability.<sup>8</sup>

## **B. Proceedings Below**

1. Respondents, on behalf of themselves and proposed classes that include in-home WiFi network users, asserted civil claims against Google in various locations around the United States. The Judicial Panel on Multidistrict Litigation consolidated respondents’ actions in the United States District Court for the Northern District of California, and respondents filed the Consolidated Class Action Complaint alleging, among other things, that Google’s interception of WiFi payload data violated the Wiretap Act, which makes it unlawful to “intentionally intercept[] . . . any wire, oral, or electronic communication.” Consol. Class Action Compl. ¶¶ 128-132; 18 U.S.C. §§ 2511(1)(a), 2520(a).

2. Google moved to dismiss the Wiretap Act claims, asserting, as relevant here, that its mass interception of communications over unencrypted WiFi

---

<sup>7</sup> Google NAL ¶ 4.

<sup>8</sup> *Id.* ¶¶ 22, 51; *see id.* ¶¶ 30, 36-39. The engineer “invoked his Fifth Amendment right against self-incrimination and declined to testify” to the Bureau. *Id.* ¶ 3.

networks is categorically exempt from liability under 18 U.S.C. § 2511(2)(g)(i). That section states that

[i]t shall not be unlawful under this chapter or chapter 121 of this title for any person to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.

Congress defined the phrase “readily accessible to the general public” in 18 U.S.C. § 2510(16), but solely “with respect to a radio communication.”<sup>9</sup> Congress did not define the phrase with respect to any other type of communication.

Google argued, as it does here, that the definition in § 2510(16) identifies those electronic communications transmitted by radio that are readily accessible to the general public and, therefore, can be intercepted without liability under § 2511(2)(g)(i). Google argued further that, because WiFi communications occur on the radio frequency portion of the electromagnetic spectrum, when such communications are not “scrambled or encrypted” — such as through the use of WiFi Protected Access (“WPA”) — they are readily accessible to the general public. 18 U.S.C. §§ 2510(16)(A), 2511(2)(g)(i).<sup>10</sup>

---

<sup>9</sup> At the same time Congress enacted § 2510(16) and § 2511(2)(g)(i), it also enacted § 2511(2)(g)(ii)(II), which used the phrase “readily accessible to the general public” in the specific context of the “intercept[ion] [of] any radio communication.” See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(a)(6), (b)(4), 100 Stat. 1848, 1849-50 (“ECPA”).

<sup>10</sup> WPA is one of a number of protocols for the encryption of data routed over WiFi networks; networks using such protocols

The district court rejected Google’s argument and denied the portion of its motion to dismiss at issue here. Based on its thorough review of the statutory text (corroborated by legislative history), the district court concluded that Congress intended the term “radio communication” in § 2510(16) to refer not to all “communications by radio” — that is, all transmissions on the radio frequency portion of the electromagnetic spectrum — as Google had argued, but instead to “‘traditional radio services,’ such that public-directed radio broadcast communication, as the technology was understood at the time, would be clearly excluded from liability under the Act.” Pet. App. 87a-88a.

3. On Google’s motion, the district court certified its order for interlocutory appeal under 28 U.S.C. § 1292(b), and the Ninth Circuit granted permission for Google to appeal. In seeking interlocutory review, Google emphasized to both courts that the issues presented were ones of “first impression.”<sup>11</sup> Indeed, in moving for certification, Google told the district court that it was “aware of no other cases analyzing whether communications sent over open, unencrypted Wi-Fi networks constitute ‘radio communications’ under the Wiretap Act.”<sup>12</sup>

In a unanimous opinion authored by Judge Bybee, the Ninth Circuit reached the same conclusion as the district court, holding “that the phrase ‘radio communication’ in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi-Fi network.” Pet. App.

---

typically appear with a “lock” icon in a list of nearby WiFi networks.

<sup>11</sup> Mot. for Certification at 1; see Pet. for Permission to Appeal at 1 (“first-impression issue”).

<sup>12</sup> Mot. for Certification at 4.

11a. The court began by holding that, because Congress had not defined the term “radio communication” in the Wiretap Act, the court was required to give the phrase its ordinary meaning. *See id.*

Applying that principle of statutory interpretation, the court rejected Google’s “technical definition” of radio communication, which would encompass any information transmitted over the “radio frequency portion of the electromagnetic spectrum.” *Id.* at 12a (quoting Appellant’s Br. 28). The court found that Google’s definition did not comport with how Congress had chosen to use the term in the Wiretap Act itself and that it conflicted with how the term is understood in common parlance. *See id.* at 12a-14a. The court further observed that, in several places in the Wiretap Act, Congress had chosen to give technical definitions to other similar terms — including “wire communication,” “electronic communication service,” and “electronic communication” — but had not chosen to give a technical definition to “radio communication.” *Id.* at 14a.

The court then compared different methods of communication to discern the essential characteristics of a “radio communication” in everyday parlance. “AM/FM, Citizens Band (CB), ‘walkie-talkie,’ and shortwave transmissions are predominantly auditory, are broadcast, and are, not coincidentally, typically referred to as ‘radio’ in everyday parlance.” *Id.* at 15a. Accordingly, the Ninth Circuit concluded that the “commonly understood” meaning of “radio communication” was as a “predominantly audio broadcast.” *Id.* at 14a-15a.

The court then looked to the text of the Wiretap Act for indications whether this definition was consistent with the way in which Congress had used the



term “radio communication.” The court observed that, where Congress intended “to refer more broadly to any communication transmitted by radio wave,” it used the phrase “communication by radio” in the Wiretap Act. *Id.* at 17a. By contrast, Congress used the phrase “radio communication” in the Wiretap Act in contexts indicating an intent “to refer more narrowly” to “traditional audio broadcasts.” *Id.* at 16a-17a. Therefore, the court reasoned that Congress’s choice to use different phrases in different contexts signaled congressional intent to give the two phrases distinct meanings. *See id.* at 18a.

The Ninth Circuit found further support for its position because giving “radio communication” its ordinary meaning as “a predominantly audio broadcast” would avoid the absurd result — required by Google’s technical definition — that the Wiretap Act’s protection for a sensitive personal email sent from a secure WiFi network or a wired network would turn on whether the recipient had chosen to receive the email on an unsecured WiFi network. *See id.* at 19a-20a. Recognizing that Congress’s purpose in protecting electronic communications in the Wiretap Act was to “protect against the unauthorized interception of [those] communications,” *id.* at 20a (internal quotation marks omitted), the court reasoned that “Congress’s decision to carve out ‘radio communication’ for less protection . . . makes sense if ‘radio communication’ is given its ordinary meaning,” and not the broad, technical definition proposed by Google, *id.* at 20a-21a.

The court then disposed of Google’s arguments that the panel should look to the definition of “radio communication” in the Communications Act of 1934, finding that Congress had borrowed definitions from the

Communications Act when it wanted to, so its decision not to do so with “radio communication” signaled a contrary intent. *Id.* at 23a-24a. Furthermore, importing the Communications Act’s definition would have rendered text in the Wiretap Act superfluous. *Id.* at 24a.

4. Google petitioned for rehearing. The panel granted the petition in part, amending its opinion to delete Part III.B of its original opinion. In that part, the panel had held that payload data transmitted over unencrypted WiFi networks are not “readily accessible to the general public” within the ordinary meaning of that phrase. *See* Pet. App. 60a-63a. The panel otherwise denied Google’s petition for panel rehearing, and the full court denied Google’s petition for rehearing en banc, with no judge requesting a vote. *Id.* at 2a.

5. On remand from the Ninth Circuit, the district court restarted proceedings, which had been stayed during the interlocutory appeal. On January 31, 2014, the parties filed a joint case management statement in which Google asserted that a dozen legal and factual questions remain to be decided by that court. *See* Jt. Case Mgmt. Stmt. at 4-6. Google also requested that the court continue to stay proceedings pending the outcome of its petition for certiorari. *See id.* at 14.

Following a case management conference, the district court lifted the stay to permit discovery on one of the legal issues Google identified — respondents’ standing to sue. That discovery has been referred to a Magistrate Judge and is ongoing in the district court.

**REASONS FOR DENYING THE PETITION****I. THIS COURT’S REVIEW IS NOT WARRANTED****A. There Is No Circuit Split for This Court To Resolve**

Google seeks review of the Ninth Circuit’s holding that the Wiretap Act’s exemption from liability for the interception of an “electronic communication . . . readily accessible to the general public,” 18 U.S.C. § 2511(2)(g)(i), does not categorically permit Google to intercept unencrypted “payload data transmitted over a Wi-Fi network” because transmissions of payload data are not “radio communication[s]” within the meaning of 18 U.S.C. § 2510(16). Pet. App. 11a.

Google does not, and cannot, argue that any court has decided this question differently from the Ninth Circuit, because *no* other court — federal or state — has decided the question presented. Indeed, Google explicitly acknowledged the novelty of the question presented when it sought permission from the Ninth Circuit for interlocutory review of what Google repeatedly described as a “first-impression issue.”<sup>13</sup> Google similarly told the district court that it was “aware of no other cases analyzing whether communications sent over open, unencrypted Wi-Fi networks constitute ‘radio communications’ under the Wiretap Act.”<sup>14</sup> Nothing has changed since Google made these representations. Today, the Ninth Circuit and the district court in this case are the only two courts to have addressed this issue.

Unable to identify any authority arguably in tension, much less in actual conflict, with the Ninth Cir-

---

<sup>13</sup> Pet. for Permission to Appeal at 1.

<sup>14</sup> Mot. for Certification at 4.

cuit's judgment in this case, Google asks this Court to abandon its primary role of resolving "direct conflict[s] among the Circuits,"<sup>15</sup> to reach out and decide an issue of first impression as a "court of error correction."<sup>16</sup> This Court has "in many instances recognized that when frontier legal problems are presented, periods of 'percolation' in, and diverse opinions from, state and federal appellate courts may yield a better informed and more enduring final pronouncement by this Court." *Arizona v. Evans*, 514 U.S. 1, 23 & n.1 (1995) (Ginsburg, J., dissenting). Assuming the issue will ever arise again, the Court should allow the issue to percolate in the lower courts to see if they interpret § 2510(16) differently from the Ninth Circuit and to wait until the Court is presented with a case that is a better vehicle to decide the issue than this one.

#### **B. The Petition Seeks Interlocutory Review of an Issue That Is Not Case Dispositive**

1. The petition is also unsuited for this Court's review because Google brings it to this Court "in an interlocutory posture" before a final judgment has been entered. *Mount Soledad Mem'l Ass'n v. Trunk*, 132 S. Ct. 2535, 2536 (2012) (Alito, J., respecting denial of petitions for writs of certiorari); *see also Brotherhood of Locomotive Firemen & Enginemen v. Bangor & A.R.R. Co.*, 389 U.S. 327, 328 (1967) (per curiam) ("[B]ecause the Court of Appeals remanded the case, it is not yet ripe for review by this Court. The petition for a writ of certiorari is denied."). The

---

<sup>15</sup> *Bunting v. Mellen*, 541 U.S. 1019, 1021 (2004) (Stevens, J., respecting denial of petition for writ of certiorari); *cf.* Sup. Ct. R. 10(a).

<sup>16</sup> *Martin v. Blessing*, 134 S. Ct. 402, 405 (2013) (Alito, J., respecting denial of petition for writ of certiorari).

case has been remanded to the district court, and discovery is proceeding. Google identifies no pressing need to short circuit the ordinary process of litigation. If the case is not resolved on other grounds, Google would be “free to raise the same issue in a later petition following entry of a final judgment.” *Mount Soledad Mem’l Ass’n*, 132 S. Ct. at 2536.

As an initial matter, the Ninth Circuit’s holding in its amended decision does not foreclose Google from establishing, as a matter of fact, that unencrypted WiFi payload data were readily accessible to the general public at the time Google intercepted the data. The panel’s original opinion had reached the latter issue, holding that “payload data transmitted over an unencrypted Wi-Fi network is not ‘readily accessible to the general public’ and, consequently, that Google cannot avail itself of the § 2511(2)(g)(i) exemption.” Pet. App. 61a. However, in its amended opinion, the Ninth Circuit removed this aspect of its holding — at Google’s request, *see* Pet. for Reh’g at 12-18 — to make clear that the factual issue is to be resolved on remand to the district court. Pet. App. 2a. Google can attempt to prove in the district court that the WiFi communications it intercepted were in fact “readily accessible to the general public,” within the ordinary meaning of that phrase even though § 2510(16) does not make those WiFi communications readily accessible by definition.<sup>17</sup>

---

<sup>17</sup> Google’s *amicus* argues that — *today, in 2014* — communications over an unencrypted WiFi network are readily accessible to the general public because software and hardware to intercept those communications are commercially available. *See* ITIF Br. 11-13. Of course, these factual arguments cannot be resolved on a motion to dismiss and, in all events, the availability of such software and hardware today has no bearing on the

Furthermore, Google itself has claimed that there are at least a dozen additional grounds on which this case may ultimately be resolved in the lower courts without the need for this Court's intervention. Those grounds include, according to Google: (1) whether plaintiffs have Article III standing to sue, (2) whether Google "intercepted" the "contents" of communications within the meaning of the Wiretap Act, (3) whether any interception was "intentional" within the meaning of the Act, (4) whether Google intentionally intercepted communications sent over the named plaintiffs' wireless networks, (5) whether any payload data intercepted from a named plaintiff's wireless network constitute the plaintiff's own communication, (6) whether any payload data that Google acquired revealed to Google the substance, meaning, or import of a communication by a named plaintiff, (7) whether Google intended to acquire the contents of any plaintiff's WiFi Communications, (8) whether Google was a party to any WiFi communications that were intercepted, and (9) whether any plaintiff suffered harm or Google earned any benefit as a result of the alleged interception of their WiFi transmissions. *See* Jt. Case Mgmt. Stmt. at 4-6.

2. This Court should also deny the petition because, even if the Court were to grant review and to afford Google all the relief it seeks, the case would not end. Among the types of payload data that respondents have alleged that Google intercepted are VoIP calls, which are voice communications sent over

---

accessibility of communications over an unencrypted WiFi network between 2007 and 2010. In the rapidly advancing world of computer technology, four to seven years is a very long time. Whether WiFi communications were readily accessible in 2007-2010 is hardly an issue of critical importance today.

the Internet to another person, who may also be using a VoIP service, or may be using a regular telephone or a cellular phone. *See* Consol. Class Action Compl. ¶ 4. Google has never made an argument that the Wiretap Act permits it to intercept a VoIP call while the data packets comprising the call travel over an unencrypted wireless network.<sup>18</sup> Nor could it.

The exemption in § 2511(2)(g)(i) does not authorize such interceptions — even on Google’s view of the law — because VoIP calls are not “electronic communications” and § 2511(2)(g)(i) applies only to the interception of electronic communications. Congress defined that term to exclude both “oral communications” and “wire communications.” *See* 18 U.S.C. § 2510(12)(A). VoIP calls are “oral communications” — and, therefore, not electronic communications — because they are “uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.” *Id.* § 2510(2). VoIP communications are also “wire communications” — and, again, not electronic communications — because they are an “aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, . . . between the point of origin and the point of reception.” *Id.* § 2510(1).<sup>19</sup>

---

<sup>18</sup> *See* Pet. App. 8a (“Google only argues, as it did before the district court, that it is exempt from liability under the Act . . . under § 2511(2)(g)(i).”).

<sup>19</sup> VoIP calls that travel over a WiFi network are transmitted at least in part “by the aid of wire,” including those used to carry broadband data packets from a premises to the broadband provider’s network or those used to route the packets over the Internet backbone. *See generally* FCC, *Consumer Guide: Voice*

Because VoIP calls are not “electronic communications,” the § 2511(2)(g)(i) exemption cannot authorize the interception of VoIP calls traveling over WiFi networks. Nor does any other provision of the Wiretap Act authorize such interceptions.

Therefore, even if this Court granted the petition and reversed the Ninth Circuit, respondents still would have stated a claim against Google for violating the Wiretap Act.

### **C. The Ninth Circuit’s Decision Raises No Issues of National Importance**

“[T]his Court reviews judgments, not statements in opinions.” *Camreta v. Greene*, 131 S. Ct. 2020, 2030 (2011) (internal quotation marks omitted). The judgment here is that “‘radio communication’ in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi-Fi network.” Pet. App. 11a. Google barely addresses the holding in its hurry to condemn various statements in Judge Bybee’s opinion. Where it does address the holding, *see* Pet. 22-24, Google makes no claim that it affects any of the activities it discusses.

1. Google frets that, if the Ninth Circuit’s judgment stands, Information Technology professionals who use packet sniffers for security monitoring may be subject to criminal liability. Pet. 22-24. But Google’s singular focus on the Wiretap Act’s limited exemption for electronic communications readily accessible to the general public, § 2511(2)(g)(i), ignores other statutory exemptions in the Wiretap Act that permit such monitoring. For example, § 2511(2)(d) provides explicit protection for interceptions “where

---

over *Internet Protocol (VoIP)*, <http://transition.fcc.gov/cgb/consumerfacts/voip.pdf> (last visited May 15, 2014).



one of the parties to the communication has given prior consent to such interception.” Organizations routinely inform their employees and others that their permission to use the organization’s network is subject to the user’s consent to such monitoring.<sup>20</sup> There is thus no reason for concern that the Ninth Circuit’s decision will compel a change in industry security practices.<sup>21</sup>

In any event, Google’s concern that “the ubiquity of Wi-Fi and the availability of packet-analysis technology” will cause disputes like this one “to arise and with increasing frequency,” Pet. 25, ignores a more important trend — that WiFi router owners increasingly are aware of — and increasingly are using — the encryption features of their WiFi routers. The question whether the Wiretap Act protects payload

---

<sup>20</sup> See, e.g., Administrative Office of the U.S. Courts, Privacy Notice, <http://www.uscourts.gov/Common/PrivacyPolicy.aspx> (last visited May 15, 2014) (“For site security purposes and to ensure that this service remains available to all users, this Government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, such evidence may be provided to appropriate law enforcement officials.”).

<sup>21</sup> Google’s *amicus* similarly asserts that the Ninth Circuit’s decision will cause uncertainty regarding the legality of network security strategies employed by professionals to detect threats to WiFi networks. See ITIF Br. 11-14. However, none of the examples provided would require a security professional to intercept data transmitted over an unencrypted network without authorization. To the extent that network security professionals might inadvertently capture packets from other networks, see *id.* at 13-14, § 2511(1)(a) imposes liability only on a person who “intentionally intercepts” electronic communications.

data sent over unencrypted WiFi networks is unlikely to recur because news stories about conduct like Google's — conduct that Google's then-CEO and co-founder each admitted was a "screw[] up," Consol. Class Action Compl. ¶ 75 — have served to educate the public regarding their ability to secure their WiFi networks against intrusions. Thus, mass interception of unencrypted data of the kind perpetrated by Google will be *less* likely to occur as time goes on, and the question presented will become *less*, not more, important.

2. The rest of Google's parade of horrors flows not from the Ninth Circuit's judgment, but from Google's speculation about what statements in Judge Bybee's opinion might mean in future cases. Specifically, Google takes issue with Judge Bybee's reasoning that "[a] radio communication is commonly understood to be (1) predominantly auditory, and (2) broadcast," Pet. App. 14a-15a, asserting that this "distinction between 'auditory' and 'non-auditory' transmissions . . . has effectively disappeared with the evolution of modern communications technology." Pet. 18.

Google's policy complaint is not with the Ninth Circuit, but with the Wiretap Act itself. As explained above, the Wiretap Act excludes all wire communications and oral communications — both of which are auditory communications ("aural" or "oral") — from the category of electronic communications. See 18 U.S.C. § 2510(1), (2), (12)(A). Therefore, the Wiretap Act treats data packets that carry the human voice, such as VoIP calls, differently from data packets that carry text or images, such as emails and webpages. In "the world of Internet protocol communications, a bit of data [may well be] simply a bit of data," but

any interpretation of the Wiretap Act built on that view is at war with the text and structure of the Act, no matter how unintelligible Google finds Congress's "rationale for distinguishing 'auditory' bits from 'non-auditory' ones." Pet. 19.

Next, Google contends that the Ninth Circuit's distinction, if applied in hypothetical future cases, could eliminate protections for cellular phone communications and broadcast television viewing. Pet. 19-22. These concerns, too, are unfounded.

First, as Judge Bybee recognized, the Ninth Circuit long ago held that cellular phone calls are protected under the Wiretap Act as *wire* communications, because the calls are "aural" communications that travel, in part, over wires. See *In re Application of the United States for an Order Authorizing the Roving Interception of Oral Communications*, 349 F.3d 1132, 1138 n.12 (9th Cir. 2003), cited in Pet. App. 23a n.6. Because the exclusion in § 2511(2)(g)(i) that permits the interception of some electronic communications is inapplicable to wire communications, the Ninth Circuit's decision in this case augurs no reduction in the protection for cellular phone calls.

Second, the decision here also poses no risks to those who watch broadcast television. Viewers are the intended recipients of television programming. Indeed, broadcasters *want* consumers to "intercept" their programs. Watching television is thus fully exempt from Wiretap Act liability. See 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful under this chapter for a person . . . to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . ."). In all events, the court

looked to television as one of many reasons for rejecting Google’s claim that “radio communication,” in the Wiretap Act, includes all communications that use radio waves. *See* Pet. App. 14a-15a.

3. Finally, Google is wrong to suggest that the Ninth Circuit’s interpretation of § 2510(16) is at odds with the decisions of various district courts that have confronted this issue. *See* Pet. 24-25. The only two examples that Google gives — *In re Innovatio IP Ventures, LLC Patent Litigation*<sup>22</sup> and *United States v. Ahrndt*<sup>23</sup> — are flatly inapposite and reflect no uncertainty in the lower courts about the protection the Wiretap Act affords to users of WiFi technology.

The *Innovatio* court undertook the very fact-based analysis that will occur in the district court in this case. There, the court accepted *Innovatio*’s contention that, in light of the state of this rapidly evolving technology in 2012 — *two years* after Google publicly admitted to systematically intercepting data transmitted over unencrypted WiFi networks using custom-built software and hardware — WiFi networks without encryption were “readily accessible to the general public” within the ordinary meaning of that phrase. *See* 886 F. Supp. 2d at 893-94; *see also id.* at 894 (recognizing that, at earlier times, “sniffing technology might have been more difficult to obtain, and the court’s conclusion might have been different”). Notably, *Innovatio* did not join Google in relying on § 2510(16) to justify its interception of data traveling over unencrypted WiFi networks. *See id.* at 893 n.5.

---

<sup>22</sup> 886 F. Supp. 2d 888 (N.D. Ill. 2012).

<sup>23</sup> No. 08-cr-468-KI, 2010 WL 373994, at \*1 (D. Or. Jan. 28, 2010), *rev’d and remanded*, 475 F. App’x 656 (9th Cir. 2012).

*Ahrndt* did not involve the interception of data traveling over a WiFi router at all. Instead, a neighbor found child pornography in Ahrndt's iTunes media library contained on his hard drive, which was configured to be shared with any iTunes user joining Ahrndt's wireless network. See 2010 WL 373994, at \*1, \*6-8. On remand from the Ninth Circuit, the district court suppressed the evidence against Ahrndt without any mention of the Wiretap Act. See *United States v. Ahrndt*, No. 08-cr-468-KI, 2013 WL 179326 (D. Or. Jan. 17, 2013).

## II. THE NINTH CIRCUIT'S JUDGMENT IS CORRECT

### A. The Ninth Circuit Correctly Interpreted the Phrase "Radio Communication" in § 2510(16)

For all the reasons set forth in Judge Bybee's opinion, "radio communication" in § 2510(16) is not synonymous with "communication by radio" and does not "refer[] to any information transmitted using radio waves, *i.e.*, the radio frequency portion of the electromagnetic spectrum." Pet. App. 12a (quoting Appellant's Br. 28). Indeed, as the court correctly held, Google's technical definition is not only inconsistent with the text and structure of the Wiretap Act, "it is in tension with how Congress — and virtually everyone else — uses the phrase." *Id.* at 13a.

In several places in the Wiretap Act, Congress chose to give technical definitions to other, similar compound terms, including "wire communication," "oral communication," and "electronic communication," but did not choose to give a technical definition to "radio communication." *Id.* at 14a; see *FDIC v. Meyer*, 510 U.S. 471, 476 (1994) ("In the absence of [an applicable statutory] definition, we construe a statutory term in accordance with its ordinary or

natural meaning.”). The ordinary, non-technical meaning of “radio communication” is a predominantly audio broadcast. *See* Pet. App. 14a-15a.

Moreover, where Congress intended “to refer more broadly to any communication transmitted by radio wave,” it used the phrase “communication by radio.” Pet. App. 17a. By contrast, Congress used the phrase “radio communication” in the Wiretap Act in contexts indicating an intent “to refer more narrowly” to “traditional audio broadcasts.” *Id.* at 16a-17a. Therefore, the court correctly reasoned that Congress’s choice to use different phrases in different contexts in the Wiretap Act signaled congressional intent to give the two phrases distinct meanings. *Id.* at 18a; *see, e.g., Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 452-53 (2002).

In addition, finding that the ordinary meaning of “radio communication” excludes WiFi transmissions avoids the absurd result — required by Google’s position — that the Wiretap Act’s protection for a sensitive personal email turns on whether the recipient chose to receive the email on an unsecured network — for example, while sitting at Starbucks connected to the coffee shop’s WiFi network. *See* Pet. App. 19a-20a. The court correctly found that such a result is squarely at odds with the Wiretap Act’s overarching purpose to “protect against the unauthorized interception of electronic communications.” *Id.* at 20a (internal quotation marks omitted).

Indeed, the legislative history amply supports Judge Bybee’s conclusion that the purpose of ECPA is to ensure that privacy protections keep pace in a world of rapidly changing technology. The Senate Judiciary Committee explained in its report recommending passage of ECPA that “the law must ad-

vance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.” S. Rep. No. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

But even as Congress sought to protect privacy in an era of rapidly changing technology, “Congress was concerned that radio hobbyists not face liability for intercepting readily accessible broadcasts.” Pet. App. 10a (quoting 132 Cong. Rec. S7987-04 (1986) (“In order to address radio hobbyists’ concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful.”)). There is no evidence, however, that the congressional concern for amateur radio hobbyists animating the statutory exemption on which Google relies extends to countenancing the mass interception of unencrypted WiFi data. As Judge Bybee’s opinion recognized, “‘radio hobbyists’ do not mistakenly use packet sniffers to intercept payload data transmitted on WiFi networks. Lending ‘radio communication’ a broad definition that encompasses data transmitted on WiFi networks would obliterate Congress’s compromise.” *Id.* at 21a. The Ninth Circuit’s interpretation of statutory text is thus consistent with Congress’s purpose to protect the public’s privacy interests while protecting 20th century radio hobbyists who could “easily and mistakenly” intercept “traditional radio services.” *Id.*

Google argues that the Ninth Circuit erred in refusing to give the term “radio communication” in the Wiretap Act the same definition assigned to it by the Communications Act, which treats the term as a synonym of the phrase “communication by radio.”

Pet. 10-13; *see* 47 U.S.C. § 153(40) (“The term ‘radio communication’ or ‘communication by radio’ means the transmission by radio . . .”). But Google fails to acknowledge that, in the Wiretap Act, Congress expressly borrowed some definitions from the Communications Act, but did not borrow this one. *See* Pet. App. 24a (citing 18 U.S.C. § 2510(1)). Thus, the fact that Congress chose *not* to import the statutory definition of “radio communication” from the Communications Act, if anything, signals congressional intent that the Communications Act definition does *not* apply to the Wiretap Act.

Google also complains that the Ninth Circuit’s interpretation is in tension with provisions of the Wiretap Act that apply to communications that are not predominantly auditory broadcasts but are nonetheless “radio communication[s]” under the Wiretap Act. Pet. 13-18. Google’s primary example is television. But Google has no answer to the fact that the Wiretap Act refers to both radio and television separately, indicating that “[t]he Wiretap Act itself does not assume that the phrase ‘radio communication’ encompasses technologies like . . . television that are outside the scope of the phrase as it is ordinarily defined.” Pet. App. 13a (citing 18 U.S.C. § 2520(c)(1)). The Wiretap Act is thus similar to other statutes in which “Congress has not typically assumed that the term ‘radio’ encompasses the term ‘television.’” *Id.* at 12a. All of these provisions confirm the court’s conclusion that the ordinary meaning of the term “radio communication” excludes the transmission of data packets between a WiFi router and a smartphone, laptop computer, or tablet.



## **B. Alternative Grounds on Which To Affirm the Judgment Exist**

The Ninth Circuit’s judgment can also be affirmed on the alternative ground that the definition of “readily accessible to the general public” in § 2510(16) applies only to the exception in § 2511(2)(g)(ii), which authorizes the interception of some “radio communication,” and not to § 2511(2)(g)(i), which applies only to “electronic communication.” This is the most natural interpretation of Congress’s decision in 1986 to add two provisions that use the phrase “readily accessible to the general public” — one with respect to electronic communication and the other with respect to radio communication — but to define the phrase only “with respect to a radio communication.” 18 U.S.C. § 2510(16); *see supra* note 9.

This interpretation — which Judge Bybee recognized “has some force,” Pet. App. 8a — is consistent with the canon of statutory interpretation that “refuse[s] to adopt a construction that would attribute different meanings to the same phrase in the same sentence.” *Reno v. Bossier Parish Sch. Bd.*, 528 U.S. 320, 329-30 (2000).<sup>24</sup> On Google’s view, the phrase “readily accessible to the general public” in

---

<sup>24</sup> By contrast, the “natural presumption that identical words used in different parts of the same act are intended to have the same meaning” “readily yields” where — as in the case of the special definition of the term “readily accessible to the general public” in § 2510(16) — there is reason to “conclu[de] that they were employed in different parts of the act with different intent.” *Environmental Def. v. Duke Energy Corp.*, 549 U.S. 561, 574 (2007) (internal quotation marks omitted). Congress’s express statement that its definition in § 2510(16) applies only “with respect to a radio communication” supplies the necessary reason to conclude that the phrase carries a different meaning in the two exemptions.

§ 2511(2)(g)(i) means different things depending on how the electronic communication at issue was carried. If carried over a “radio . . . system,” § 2510(16) would define that phrase; but, if carried instead “by a wire . . . electromagnetic, photoelectronic or photooptical system,” courts would apply the ordinary meaning of the phrase. *See* 18 U.S.C. § 2510(12) (defining “electronic communication”). The panel’s decision to allow this result was erroneous, *see* Pet. App. 9a, and, if certiorari were granted, respondents would seek to affirm the Ninth Circuit’s judgment on this alternative ground.

### CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted,

DANIEL A. SMALL  
DAVID A. YOUNG  
COHEN MILSTEIN SELLERS  
& TOLL, PLLC  
1100 New York Avenue, N.W.  
Suite 500 West  
Washington, D.C. 20005  
(202) 408-4600

JEFFREY L. KODROFF  
JOHN A. MACORETTA  
MARY ANN GEPPERT  
SPECTOR ROSEMAN  
KODROFF & WILLIS, P.C.  
1818 Market Street  
25th Floor  
Philadelphia, PA 19103  
(215) 496-0300

ELIZABETH J. CABRASER  
*Counsel of Record*  
MICHAEL W. SOBOL  
NICOLE D. SUGNET  
LIEFF, CABRASER, HEIMANN  
& BERNSTEIN, LLP  
275 Battery Street  
29th Floor  
San Francisco, CA 94111  
(415) 956-1000  
(ecabraser@lchb.com)

May 27, 2014