Docket No. 11-17483

In the

United States Court Of Appeals

For the

Ninth Circuit

BENJAMIN JOFFE, *et al.*,

Plaintiffs-Appellees,

v.

GOOGLE INC.,

Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California,
Benjamin Joffe, et al. v. Google Inc.
Case No. 5:10-MD-2184-JW
Entered on June 29, 2011

BRIEF OF PLAINTIFFS-APPELLEES BENJAMIN JOFFE, *ET AL*.

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

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

Interim Co-Lead Counsel

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

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

Interim Liaison Counsel

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

OTHER AUTHORITIES

TABLE OF AUTHORITIES
(continued)

Page

REGULATIONS

JURISDICTION

Plaintiffs-Appellees agree with Google's statement of jurisdiction.

ISSUES PRESENTED FOR REVIEW

Does the Wiretap Act prohibit the unauthorized interception of personal data transmitted over unencrypted home Wi-Fi[1] networks?

STATEMENT OF THE CASE

Plaintiffs-Appellees' class action complaint seeks redress for Google's intentional and systematic interception of Plaintiffs-Appellees' and the proposed class members' personal electronic data—including e-mails, passwords, documents, and other confidential information—from their private home Wi-Fi networks. Although these home networks were not password protected, the communications transmitted over them were private and not broadcast for public consumption. Such communications are protected from prying eyes by the Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"). Google's interception of these data violates the Wiretap Act.

Google argues that all communications over non-password-protected Wi-Fi networks fall within an exception to the Wiretap Act, so that anyone may, with impunity, intercept such communications by reaching inside people's homes with surveillance equipment. The District Court, per Chief Judge Ware, correctly rejected that argument. The District Court found instead that the exception on

[1] Wi-Fi is a popular technology that allows an electronic device (such as a laptop, smart phone, etc.) to exchange data wirelessly over a computer network.

which Google relied applies only to traditional, broadcast radio communications; it does not encompass every electronic communication that travels, even just a few feet, by radio waves.

The District Court certified its order for interlocutory review, and this Court accepted jurisdiction.

STATEMENT OF FACTS

I. Google Intentionally Intercepted Plaintiffs-Appellees' Wi-Fi Data, Which Were Not Readily Accessible to the General Public.

First launched in the United States in 2007, Google Street View is a feature of Google's "Google Maps" and "Google Earth" products that offers panoramic views along many streets around the United States and the world. ER 241 (¶¶ 54-55).[2] Specifically, Google Street View displays images taken by cameras mounted on Google vehicles. ER 241 (¶¶ 55, 58). The vehicles also have Wi-Fi antennae and sophisticated hardware and software that capture and store Wi-Fi signals and data from nearby homes. ER 242 (¶¶ 60-61).

Google intentionally included computer code to sample, collect, decode, and analyze data sent and received over Wi-Fi connections. ER 228-29, 242 (¶¶ 4, 61). As data streams flowed across Wi-Fi connections, Google's "wireless sniffer" captured individual data packets, then decoded/decrypted and analyzed the

[2] References to "ER" are to excerpts from the record Google filed with this Court on February 8, 2012 (Dkt. No. 25). References to "¶ __" are to paragraphs of the Consolidated Class Action Complaint filed by Plaintiffs-Appellees on November 8, 2010.

contents. ER 242 (¶ 62). The data Google collected included, among other things, personal e-mails, passwords, videos, audio, documents, and Voice Over Internet Protocol (VOIP) information (collectively, "payload data") transmitted over Plaintiffs-Appellees' Wi-Fi networks. ER 228-29 (¶ 4).

The Wi-Fi data Google gathered was not readily accessible by members of the general public. ER 229, 243 (¶¶ 5, 64). Sophisticated decoding and processing technology, such as that included in the Google vehicles by its engineers, is required to intercept these data. *Id.*; *see also* ER 228-29, 242 (¶¶ 4, 61).[3]

II. Google Admitted That It Improperly Intercepted These Wi-Fi Communications and Collected Personal Data.

Google initially misled the public regarding its interception of their personal data. Early on, Google stated publicly that it was simply collecting street-level images for its Google Maps and Google Earth products, and Google did not disclose its interception of personal data. ER 243 (¶ 67). But Google's actions contravened these statements and violated its own well-publicized privacy policy, which stated "we will not collect or use sensitive information for purposes other than those described in this Privacy Policy and/or in the supplementary service privacy notices, unless we have obtained your prior consent." ER 243-44 (¶ 68).

[3] By contrast, an individual with a mobile devices such as a laptop or smart phone can easily access the internet through an unprotected Wi-Fi network, by viewing the network on his or her device and clicking on it. Such a connection, in itself, does not allow the individual to intercept data being transmitted by other individuals connected to that Wi-Fi network.

Notably, in October 2010, after these practices had come to light, Google revised its privacy policy, deleting this assurance. *Id.*

In spring 2010, after denying that it had intercepted personal data, Google made a series of partial admissions of its wrongful conduct. ER 229, 244-45 (¶¶ 7, 69-77). On April 27, 2010, for instance, in response to inquiries from the German Data Protection Authority ("DPA"), Google acknowledged that it had collected SSIDs (Wi-Fi network names) and MAC addresses (essentially, ID numbers of Wi-Fi networks' hardware). ER 244 (¶ 69). But Google falsely claimed that it had not collected any data traversing those networks. *Id.* (¶ 70).[4] Then, in May 2010, after the DPA threatened to audit the data Google had collected, Google admitted that its April 27 statement was incorrect and that it had, in fact, been "collecting samples of payload data from open (*i.e.*, non-password-protected) Wi-Fi networks." ER 244 (¶ 71). Google further revealed that one of its engineers had developed "code that sampled all categories of publicly broadcast Wi-Fi data," which Google ultimately used to collect and store payload data. *Id.* (¶ 72). Additionally, Google disclosed that it had "accumulated about 600 gigabytes of data transmitted over public Wi-Fi networks in more than 30 countries." *Id.* (¶ 73). This concession, too, was incomplete. Google did not reveal what it later felt

[4] *See also* http://googlepolicyeurope.blogspot.com/2010/04/data-collected-by-google-cars.html (last visited Mar. 21, 2012) ("Networks also send information to other computers that are using the network, called payload data, but Google does not collect or store payload data.").

compelled to disclose: that it had collected data from private—not just public—Wi-Fi networks. ER 244, 245 (¶¶ 74, 77).

Gradually, Google admitted more. In June 2010, Google CEO Eric Schmidt "admitted that he could not rule out the possibility that personal data such as bank account details were among the data collected." ER 244-45 (¶ 75). Schmidt conceded, "We screwed up. Let's be very clear about that." *Id.* Around the same time, Google co-founder Sergey Brin similarly acknowledged, "[W]e screwed up. I'm not going to make any excuses about it." *Id.*

Finally, in October 2010, amid investigations in the United States and abroad, Google admitted that it had captured individuals' entire emails, usernames, passwords, and other private data. ER 245 (¶ 77). At that time, Google Senior Vice President of Engineering & Research Alan Eustace revealed:

> [A] number of external regulators have inspected data as part of their investigations . . . . It's clear from those inspections that while most of the data is fragmentary, in some instances entire emails and URLs were captured, as well as passwords. We want to delete this data as soon as possible, and I would like to apologize again for the fact that we collected it in the first place.

Id. Google later acknowledged to Congress that it "included code in [its] software that collected samples of 'payload data'" and that "[i]t is possible that the payload data may have included personal data if a user at the moment of collection broadcast such information." ER 246 (¶ 80).

III. Plaintiffs-Appellees Filed Complaints Seeking Redress for Google's Conduct.

Plaintiffs-Appellees, on behalf of themselves and proposed classes of similarly situated persons, asserted claims against Google in several jurisdictions. The United States Judicial Panel on Multidistrict Litigation ultimately transferred the cases to Chief Judge James Ware, in the United States District Court for the District of Northern California. ER 261. On November 8, 2010, Plaintiffs-Appellees filed their consolidated complaint, which asserted claims against Google under the Wiretap Act, 18 U.S.C. § 2510 *et seq*., California's unfair competition law, California Business and Professions Code, § 17200 *et seq*. ("UCL"), and numerous state wiretap statutes. ER 252-57 (¶¶ 119-45).

IV. The District Court Denied Google's Motion to Dismiss, Finding That Communications Sent Over Wi-Fi Networks Are Not Within the Wiretap Act's Exception for Certain "Radio Communications."

On December 17, 2010, Google moved to dismiss Plaintiffs-Appellees' complaint. Google argued that, despite its broad prohibitions on intercepting electronic communications, the Wiretap Act permits anyone to intercept every packet of information traveling over a non-password-protected Wi-Fi network, and that as a result, Plaintiffs-Appellees' federal and state law claims must be dismissed. Following full briefing, the District Court heard oral argument on March 21, 2011. The District Court then requested supplemental briefing on three issues under the Wiretap Act: the meaning of "radio communication," whether

Wi-Fi communications are "radio communications," and whether cellular telephone calls are "radio communications."

On June 29, 2011, the District Court denied Google's request to dismiss Plaintiffs-Appellees' Wiretap Act claim. The court's order was based on an exhaustive analysis of the text, history, and purpose of the Wiretap Act. The court started with the statutory text, noting that the provision on which Google relied, 18 U.S.C. § 2510(16), does not "specifically address wireless internet technologies" but instead "predominantly addresses radio broadcast technologies." ER 14. The court also considered the three other places where the statute uses the term "radio communications," and found the "usage of 'radio communication' throughout the Act does not lend itself to a broad interpretation of the term." ER 15. Instead, the Act uses the term to refer to "radio broadcast technologies" and not to "other communications technologies that transmit using radio waves." *Id.*

The court also noted that "radio communication" is a compound term. The court found that, when Congress used other compound terms that it expressly defined in ECPA, such as "wire communication," it "intended more refined definitions than simply combining the independent meanings of each word." ER 17. Thus, for example, "wire communication" does not mean "any communication transmitted by wire." *See* 18 U.S.C. § 2510(1). The court noted that Congress' decision not to define "radio communication" did not preclude the court from

finding that this compound term, too, has a "compound meaning" narrower than "all communications transmitted by radio." ER 18.

The court next turned to the legislative history for clarification, noting that Congress amended the Wiretap Act in 1986, through ECPA, specifically to "provide statutory privacy protection and a civil right of action for interceptions of electronic communications," such as "computer-to-computer transmissions and electronic mail." ER 19. At the same time, Congress wanted to protect hobbyists and users of radio scanners from liability for inadvertently intercepting communications that ought to be protected but that might easily be picked up while scanning for public broadcasts. Congress, therefore, adopted 18 U.S.C. § 2511(2)(g)(i) and (ii), which exempts interceptions of electronic communications and radio communications from liability under certain circumstances.

The court found it noteworthy that, in doing so, Congress addressed only the interception of "traditional radio broadcast mediums" and did "not address any broader radio-based communications technology." ER 20. Based on this legislative history, the court found that it was "clear" that "Congress intended 'radio communication' to include 'traditional radio services,'" so that "public-directed radio broadcast communication . . . would be clearly excluded from liability under the Act." ER 21. At the same time, "Congress did not intend 'radio communications' to be defined so broadly that it would encompass all

communications transmitted over radio waves." *Id.* This, the court found, reflected a "balance being struck" between certain communications "that were designed to be public, like traditional radio broadcast, and others that were designed to be private." ER 22.

For these reasons, the District Court rejected Google's position that "radio communication" means "all communications transmitted by radio," and therefore rejected Google's argument that the Wiretap Act provides no protection from interception for every communication transmitted by radio that does not meet one of the enumerated exceptions in Section 2510(16). Instead, the court found that Congress did not mean for Section 2510(16) to apply to the interception of "electronic communications," such as Wi-Fi transmissions, "that could not be fairly classified as 'traditional radio services,' or radio broadcast technology." ER 23.

The court then found that the complaint sufficiently alleged a violation of the Wiretap Act—in particular, that Google intentionally intercepted private communications that "were not readable by the general public without the use of sophisticated packet sniffer technology." ER 23. The court recognized that Wi-Fi is "designed to send communications privately, as in solely to select recipients" and is "architected in order to make intentional monitoring by third parties difficult." ER 24. The court found that the facts pled in the complaint, therefore,

were "sufficient to support a claim that the Wi-Fi networks were not 'readily accessible to the general public'" under the ordinary meaning of that term. ER 25.[5]

On Google's motion, the District Court then certified its order for interlocutory review under 28 U.S.C. § 1292(b) and stayed the action pending the appeal. This Court subsequently granted Google's petition for interlocutory appeal. ER 1.

SUMMARY OF ARGUMENT

The Wiretap Act is a fundamental safeguard of individual privacy, ensuring that Americans' private communications are protected from the prying eyes of government, corporations, and other individuals. Wi-Fi networks carry electronic communications, such as e-mails, between a person's home computer and her home Wi-Fi router, that are protected from interception pursuant to the Wiretap Act, 18 U.S.C. § 2511(1)(a). When Google intentionally intercepted Plaintiffs-Appellees' Wi-Fi communications through the sophisticated hardware and software with which it equipped its Google Street View vehicles, Google violated Section 2511(1)(a).

Google argues that Wi-Fi communications fall into Section 2511(2)(g)(i), one of the Act's narrow exceptions, because they allegedly are electronic

[5] The District Court dismissed Plaintiffs-Appellees' state wiretap claims with prejudice on preemption grounds and dismissed, without prejudice, the California UCL claims based on lack of standing. ER 6-31.

communications that are "readily accessible to the general public." This argument is explicitly premised on Google's conclusion that Wi-Fi communications are "radio communications" under Section 2510(16). *See* Google Brief, p. 9-10. Google is incorrect.

As the District Court correctly found, Section 2511(2)(g)(i) does not exempt Google's conduct from the Wiretap Act's broad prohibition on the interception of private communications. First, while the Wiretap Act does not define the term "radio communication," the statutory text and structure demonstrate that "radio communications" means traditional, broadcast radio services, not all communications transmitted by radio waves. In those places where the Wiretap Act uses the term "radio communications," the communications described—*e.g.*, Citizen's Band (CB) radios, amateur radio, and police and fire bands—are broadcast radio services. These communications are broadcast long distances and/or their content is easily accessed using widely-available equipment. They are not privately-directed communications like Wi-Fi communications that travel short distances and whose content can be accessed only with sophisticated hardware and software.

Second, the legislative history and purpose of ECPA confirm that "radio communications" are limited to traditional radio services. The paramount purpose of the Wiretap Act is to effectively protect the privacy of communications. The

statute broadly prohibits the interception of oral, wire, and electronic communications with narrow exceptions. Google interprets the exception on which it relies, Section 2511(2)(g)(i), in an unreasonably expansive manner. The exceptions to liability that Congress carved out for "radio communications" were designed to protect amateur radio hobbyists who can easily access the content of far flung radio broadcasts.

Third, public policy considerations further demonstrate that Congress intended to protect Wi-Fi communications. Finding that Wi-Fi communications are radio communications would produce absurd results that Congress could not have intended. Under Google's interpretation, whether the Wiretap Act protects a confidential e-mail sent by a patient from her personal computer connected to the Internet by cable to her doctor turns on whether or not the doctor's office is connected to the Internet wirelessly without password protection. Congress could not have intended for the Act's protection to be subject to such vagaries.

In any event, Section 2510(16)'s definition of "readily accessible to the general public" does not apply to the use of that phrase in Section 2511(2)(g)(i). Rather, that definition only applies to that phrase as it appears in a different exemption (Section 2511(2)(g)(ii)(II)) on which Google does not and cannot rely. Thus, whether the Wi-Fi transmissions intercepted by Google were "readily accessible to the general public" under Section 2511(2)(g)(i) must be determined

according to the ordinary meaning of that phrase. Wi-Fi communications manifestly are not readily accessible to the general public. They are not designed or intended to be public, they travel only short distances, and their content is accessible only with sophisticated hardware and software—like that used by Google in its Street View cars—that are not widely available to the public. Because Wi-Fi communications are not readily accessible to the general public, Google's interception of those communications violated the Wiretap Act.

ARGUMENT

I. The Wiretap Act Protects Communications Over All Wi-Fi Networks from Interception.

Wi-Fi networks carry electronic communications that are protected from interception by the Wiretap Act. These networks allow computers and other devices (such as smart phones and tablets) to connect to the Internet without wires, and carry wireless packets containing information, such as e-mails, passwords, electronic purchases, and interactions with websites, over short distances within a person's home. Specifically, in a section titled "Interception And Disclosure Of Wire, Oral, Or Electronic Communications Prohibited," the Wiretap Act makes it unlawful to "intentionally intercept[] . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). When Google intentionally intercepted the electronic communications of the putative class members, it violated the Wiretap Act.

The Wiretap Act is a pro-privacy statute. It contains numerous robust restrictions designed to protect individuals' communications. Consistent with that purpose, Congress amended the Wiretap Act in 1986 to keep pace with evolving technology and to ensure that private communications remained protected from prying eyes. Indeed, the "most important" factor underlying ECPA was the changing nature of communications and the concern that, "if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right." H.R. Rep. No. 99-647, at 19 (1986). One such technological change Congress observed in 1986 was the development and increasingly mainstream use of electronic communications. And so, under the Wiretap Act, interception of wire, oral, and electronic communications is prohibited, unless the interception is conducted with consent or falls into one of a few narrow categories of conduct that Congress has determined merits an exception, consistent with individuals' basic privacy rights.

Google, in seeking to expand one of these narrow exceptions into a giant loophole, would turn the Wiretap Act on its head. It relies on the exception for electronic communications "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) ("exemption G1"). Although the Act does not define "readily accessible to the general public" with respect to electronic

communications, it defines that term, "with respect to a radio communication," to mean "that such communication is not . . . scrambled or encrypted" or that has certain other enumerated characteristics. 18 U.S.C. § 2510(16). Google's effort to escape liability under the Wiretap Act rests on two arguments: (1) that the Section 2510(16) definition of "readily accessible to the general public" applies to exemption G1, even though the definition by its terms applies only to radio communications, which are covered in 18 U.S.C. § 2511(2)(g)(ii)(II) ("exemption G2"), and (2) that the Section 2510(16) definition applies to Wi-Fi communications because they constitute "radio communications." In support of this second argument, Google contends that, because Wi-Fi networks use radio signals, they must be "radio communications." For Google's argument to succeed, "radio communications" must be interpreted to include *all* "communications by radio technology"—an interpretation the District Court properly rejected.[6]

Instead, as the District Court found, the term "radio communications," within the Wiretap Act, has a specific meaning limited to radio broadcast

[6] This Court has already rejected Google's mechanistic approach to interpreting a phrase like "radio communication." In *In re Application of the United States, for an Order Authorizing the Roving Interception of Oral Commc'ns*, 349 F.3d 1132 (9th Cir. 2003), this Court held, under the Wiretap Act, that a communication that occurs in part by radio (there, a cell phone call) can be a "wire communication." *Id.* at 1138 n.12 ("Despite the apparent wireless nature of cellular phones, communications using cellular phones are considered wire communications under the statute, because cellular telephones use wire and cable connections when connecting calls.").

communications. In short, not all "communications by radio" are "radio communications" for purposes of the Act. Rather, the text and history of the Wiretap Act shows that the Act used "radio communications" to refer only to "traditional radio services" or "public-directed radio broadcast communications," such as Citizen's Band (CB) radios, amateur radio, and police and fire bands. ER 21.

These traditional types of radio transmission are considered public because they are broadcast great distances and/or their content is readily accessible to the public through unsophisticated equipment, such as the common radio scanner available at Radio Shack. Under these circumstances, the broadcasters can have no reasonable expectation of privacy in those communications. They are, therefore, properly defined as "readily accessible to the general public."

Communications over Wi-Fi networks are quite different. First, they are private. Individuals purchase and set up Wi-Fi routers for convenient, wireless access to the Internet within their homes, not to broadcast their private thoughts and secrets to the world at large. Second, there is no public benefit in allowing outsiders to intercept individuals' private communications sent over Wi-Fi networks. Third, Wi-Fi signals travel very short distances, usually covering parts (but often less than 100%) of a person's house, while also extending a few dozen feet beyond some of the house walls. Fourth, Wi-Fi communications are coded,

and, whether or not encrypted, their content can only be deciphered with sophisticated software. These critical factors distinguish Wi-Fi communications from the traditional, broadcast "radio communications" addressed as such in the Wiretap Act. Accordingly, Google's attempt to escape the Wiretap Act's prohibition on interception by equating Wi-Fi communications with traditional radio broadcasts fails. The District Court's opinion denying Google's motion to dismiss Plaintiffs-Appellees' complaint should be affirmed. *See* ER 23-24.

A. The Wiretap Act's Language and Structure Show that Congress Understood "Radio Communications" Narrowly as "Traditional Radio Broadcast Services."

The first step in ascertaining congressional intent is to "look to the plain language of the statute." *United States v. Daas*, 198 F.3d 1167, 1174 (9th Cir. 1999) (citations omitted). "To determine the plain meaning of a particular statutory provision, and thus congressional intent, the court looks to the entire statutory scheme. If the statute uses a term which it does not define, the court gives that term its ordinary meaning." *Id.*; *see Lamie v. United States Tr.*, 540 U.S. 526, 534 (2004); *see also K Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988) ("In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole.").

Congress uses the term "radio communication" only four times in the Wiretap Act. In all four instances, the term denotes forms of radio broadcasts that are directed to the public and/or whose content is easily accessed.

First, "radio communication" is used in Section 2511(2)(g)(ii), which describes "radio communication[s]" that are "transmitted" by one of four specific types of broadcasters: (i) a "station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;" (ii) a "governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;" (iii) "a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services;" or (iv) a "marine or aeronautical communications system." 18 U.S.C. § 2511(2)(g)(ii). This list of senders of radio communications is highly specific, and their communications are publicly directed in that they travel long distances and/or their content is readily accessible. *See DIRECTV, Inc. v. Barczewski*, 604 F.3d 1004, 1006 (7th Cir. 2010) ("*Section 2511(2)(g) as a whole deals* with unencrypted communications, *broadcast in the clear* to promote public safety or open discourse." (Emphasis added).

Second, Congress allows "other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by

individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted." 18 U.S.C. § 2511(2)(g)(v). Again, Congress' rationale is readily understood—multiple users of the same radio frequency can easily, even inadvertently, receive the content of each other's communications.

Third, 18 U.S.C. § 2511(5)(a)(i)(B) gives the Federal Government a claim for certain unlawful interceptions of an unencrypted "radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission . . . ." Subpart D of part 74 of those rules regulates "Remote Pickup Broadcast Stations." This section of the Wiretap Act addresses the unencrypted transmission of news broadcasts from field reporters back to their radio or television stations, which are then, in turn, broadcast to the public. These radio communications thus are destined for public broadcast, but Congress chose to give them some interim protection en route to being broadcast. 47 C.F.R. § 74. *See also* 18 U.S.C. § 2520(c)(1) (prescribing statutory damages amounts for unlawful interception of these radio communications).

Fourth, § 2510(16) defines what the term "'readily accessible to the general public' means, with respect to a radio communication." This section delineates the actions a broadcaster can take to bring an otherwise public radio communication within the protection of the Act, such as by scrambling or encrypting them,

§ 2510(16)(A), or by using certain modulation techniques, § 2510(16)(B). These actions transform a publicly broadcast radio communication into something protected by statute.

The District Court correctly recognized that each of these four statutory sections addresses traditional radio services, *i.e.*, publicly directed radio broadcasts:

> [T]he usage of "radio communication" throughout the Act [2511(2)(g)(ii); 2511(2)(g)(v); 2511(5)(a)(i)(B); and 2510(16)] does not lend itself to a broad interpretation of that term. In particular, references to "radio communication" throughout the Act predominantly pertain to and are drafted for the particular design of radio broadcast technologies, and do not address other communications technologies that transmit using radio waves.

ER 15. Thus, Congress *consistently* used the term "radio communication" when referring to traditional radio services or broadcast radio, and did not use that term to discuss other means of communicating using radio signals, like Wi-Fi networks.

Furthermore, Congress used a different phrase, "communication by radio"—or variants of that phrase—when it wanted to address *all* communications that use radio waves, including non-broadcast transmissions. For example, Congress defined "electronic communication," which is expressly protected under the Act, to include any communication "transmitted in whole or in part by . . . radio." 18 U.S.C. § 2510(12). In addition, Congress made it unlawful to use a "device to intercept any oral communication," which is also expressly protected under the Act, if the "device transmits communications by radio"—that is, if it relays the

intercepted communication to the eavesdropper using radio waves. 18 U.S.C. § 2511(1)(b)(ii). And Congress authorized employees of the FCC, in carrying out their official duties, "to intercept . . . [an] oral communication transmitted by radio." 18 U.S.C. § 2511(2)(b). Each of these uses of "communication by radio" or the like clearly shows that, when Congress intended to address *all* communications that use radio waves, it used this phrase, rather than the compound term "radio communication."

In sum, Congress' different usages of "radio communication" and "communication by radio" in the Wiretap Act demonstrate that Congress meant to use the former term to refer only to radio *broadcasts*, while the latter term includes *non-broadcasts* using a radio device. Nowhere in the Act did Congress use "radio communication" to mean all communications by radio.

B. The Legislative History and Purpose of the Wiretap Act Confirm That "Radio Communication" Means Traditional Radio Services.

1. The Wiretap Act Was Passed and Has Evolved Under Circumstances That Reflect Congress' Paramount Concern for Individual Privacy.

Importantly, the Wiretap Act's purpose, evidenced by voluminous legislative history,[7] is to protect private communications like those over Wi-Fi networks, using the Fourth Amendment's privacy protections as a touchstone. The

[7] *See SEC v. McCarthy*, 322 F.3d 650, 655 (9th Cir. 2003) ("When the statute is ambiguous or the statutory language does not resolve an interpretive issue, 'our approach to statutory interpretation is to look to legislative history.'") (quoting *Northwest Forest Res. Council v. Glickman*, 82 F.3d 825, 834 (9th Cir. 1996)).

Senate Judiciary Committee explained in its report recommending passage of ECPA that "the law must advance 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, *reprinted in* 1986 U.S.C.C.A.N. 3555, at 3559 (1986); *see also* H.R. Rep. No. 99-647, at 16-19 (1986) (stating that one of Congress' goals in passing ECPA was to keep the privacy protection of electronic communications consistent with expectations arising from the Fourth Amendment).

Throughout U.S. history, protection of individual privacy rights and interests has been a paramount concern of Congress and the courts. Initially, the focus was on limiting inappropriate governmental intrusions. In passing ECPA, the Senate Report invoked a statement by Justice Brandeis:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?

S. Rep. No. 99-541, 1986 U.S.C.C.A.N. 3555, at 3556 (1986) (quoting *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting)).[8] During the

[8] In *United States v. Jones*, 132 S. Ct. 945 (2012), Justice Scalia's majority opinion noted, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* [reasonable expectation of privacy] analysis." *Id.* at 953; *see also id.* at 959 (Alito, J., concurring) & 955 (Sotomayor, J., concurring).

20th century, two important developments gave life to Justice Brandeis' concern. First, the development of increasingly sophisticated technology made invasions of privacy all the more possible. Second, as those new technologies became cheaper and more widely available, the ability to spy on individuals was no longer the purview primarily of the government—individuals, corporations, and other entities gradually gained greater power to violate people's privacy rights and interests. Hence, a need arose to protect individuals from non-governmental prying eyes.

Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 in order to ensure that the privacy of the latest technology of *that* time—voice communications carried by wire (*i.e.*, telephones)—would be protected from governmental and non-governmental interception. *See* S. Rep. No. 99-541, 1986 U.S.C.C.A.N. 3555, at 3556 (1986). For almost twenty years, Title III was "the primary law protecting the security and privacy of business and personal communications in the United States." *Id.*

However, with even more technological advancements during that two-decade period in the telecommunications industry (*e.g.*, cellular telephones) and the booming computer industry (*e.g.*, e-mail), Title III's protection of only "the unauthorized aural interception of wire or oral communications" was no longer sufficient. *Id.* Consequently, in 1986, Congress amended the Wiretap Act by enacting ECPA in order to "protect against the unauthorized interception of

electronic communications" and to "update and clarify Federal privacy protections and standards in light of dramatic changes in *new computer* and telecommunications technologies." *Id.* at 3555 (emphasis added). Congress thus drafted ECPA so that "the law would advance with the technology to ensure the continued vitality of the Fourth Amendment." *Id.* at 3559.

In drafting ECPA, Congress demonstrated its intent to extend privacy protections to the analogues of first-class mail that developed thanks to technological innovations. According to Senator Leahy:

> From the beginning of our history, first-class mail has had the reputation of preserving privacy while promoting commerce. It is high time we updated our laws so that we can say the same about new forms of technology which are being used side by side with first-class mail.

132 Cong. Rec. S7978-04, 1986 WL 776264, at *12 (1986). The Senate Report reiterates the idea that email should enjoy the same strong protections as first class mail:

> A letter sent by first class mail is afforded a high level of protection against the unauthorized opening by a combination of constitutional provisions, case law, and U.S. Postal Service statutes and regulations. . . .
>
> But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or *new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services*. . . .

> This gap results in legal uncertainty. It may unnecessarily discourage potential customers from using innovative communications systems. It probably encourages unauthorized users to obtain access to communications to which they are not a party. It may discourage American businesses from developing new innovative forms of telecommunications and computer technology.

S. Rep. No. 99-541, 1986 U.S.C.C.A.N. 3555, at 3559 (1986) (emphasis added).

E-mails sent wirelessly from a laptop, smartphone, or tablet to a Wi-Fi router within one's home—and, from there, through the Internet to its final destination—are the equivalent of first-class mail today. Both carry the same reasonable expectation of privacy. Put another way, without protection, "unauthorized users," such as Google, could "obtain access to [electronic] communications to which they are not a party." *Id.*

Therefore, one of Congress' goals in passing ECPA was to protect e-mail communications, in which it found individuals "likely . . . have a 'reasonable expectation of privacy.'" H.R. Rep. No. 99-647, at 22 (1986); 132 Cong. Rec. 039-01, 1986 WL 776505 (1986) (statement of Congressman Kastenmeier) (right to privacy "will evaporate" if fourth amendment protection is not extended to computer services, "which store [citizens'] bank records, credit card data, electronic mail and other personal data"); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (finding a reasonable expectation of privacy in e-mails); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 974-75 (C.D. Cal. 2010) (equating a

person's privacy rights regarding a profile or inbox on a social networking site to privacy rights regarding employment or bank records).

Congress' goal of protecting e-mails can be realized under the District Court's interpretation of the Wiretap Act; it cannot under Google's construction.

2. Amendments Since ECPA Further Support the District Court's Conclusion That Wi-Fi Communications Are Not "Radio Communications."

In 1994, in response to evolving technology, Congress amended the Wiretap Act again, passing the Communications Assistance For Law Enforcement Act ("CALEA"). *See* CALEA, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 18 U.S.C. § 2510 *et seq.*) (1994). CALEA was designed to ensure that, as telephone transmission technology and features advanced, law enforcement personnel would not lose the technical ability lawfully to intercept communications. *See, e.g.*, S. Rep. No. 103-402, 1994 WL 562252, at *9. But

CALEA also amended Section 2510(16) to make it clearer that the Act protected all forms of electronic communications that were also radio communications. *See id.* § 203, 108 Stat. 4279, 4291. Specifically, CALEA added "electronic communications" to the list of "radio communications" that are not "readily accessible to the general public" under Section 2510(16) and that are,

therefore, protected from unauthorized interception.[9] This addition clarified what Congress already believed to be the case—that the Wiretap Act protected electronic communications from eavesdropping. S. Hr'g 103-1022, at 278 (1994) (summary of bill stating that Congress' "intention is to provide clarification that there is protection for all forms of electronic communication, including data, even when they may be transmitted by radio"); *id.* at 15 (testimony of FBI Director Louis Freeh before the Senate Judiciary Committee that the purpose of the amendment was *not* to protect previously unprotected radio communications from interception, but rather to provide "clarification of privacy protection for electronic communications transmitted by radio").[10]

The legislative record of the 1994 amendment further confirms that the touchstone of the Wiretap Act has been individuals' reasonable expectations of privacy, consistent with Fourth Amendment norms. The Final Report of the Privacy and Technology Task Force, created by Congress to examine ECPA's application to developing communications technology, evidences this approach:

> The drafters of ECPA relied on distinctions between communications technologies which, in 1986, made it difficult to intentionally target

[9] "'Readily accessible to the general public' means, with respect to a radio communication, that such communication is not . . . (F) an electronic communication." 18 U.S.C. § 2510(16) (1994).

[10] Similarly, the summary of the bill included in the Senate Hearing states that Congress's "intention is to provide clarification that there is protection for all forms of electronic communication, including data, even when they may be transmitted by radio." S. Hr'g 103-1022, at 278 (1994).

> and monitor specific communications (where a reasonable expectation of privacy could be said to exist) and those in which the communication was "out in the clear", where specific monitoring was easily achieved and where no reasonable expectation could be found.

Final Report of the Privacy and Technology Task Force Submitted to Senator Patrick Leahy (May 29, 1991), reprinted in S. Hr'g. 103-1022, at 179 (March 18 & Aug. 11, 1994).[11] Wi-Fi communications fall into the first category, and so have been protected from interception since the passage of ECPA in 1986. The Task Force recommended that Congress reinforce this by amending Section 2510(16), because it was concerned that developing radio-based communications "will not fall neatly into the distinctions drawn by ECPA." *Id*. at 181.

Thus, Congress understood in 1994, when it passed the CALEA, that the Wiretap Act already barred interception of electronic communications carried by radio waves—like the Wi-Fi communications at issue in this case—and added this additional provision as a belt-and-suspenders effort to make that protection clearer. *See, e.g.*, *Shook v. D.C. Fin. Responsibility & Mgmt. Assistance Auth.*, 132 F.3d 775, 782 (D.C. Cir. 1998) (explaining that Congress "sometimes drafts provisions that appear duplicative of others simply, in Macbeth's words, 'to make assurance

[11] Similarly, both the House and Senate reports regarding CALEA indicate that the categories of Section 2510(16) "enjoy protection because they usually are not susceptible to interception by the general public." H.R. Rep. No. 103-827, 1994 U.S.C.C.A.N. 3489, at 3511; S. Rep. No. 103-402, 1994 WL 562252, at *30.

double sure.' That is, Congress means to clarify what might be doubtful that the mentioned item is covered without meaning to exclude the unmentioned ones.").

Two years later, Congress passed the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA"). AEDPA was almost exclusively concerned with habeas corpus reform and antiterrorism measures. But Congress also amended Section 2510(16) to remove the explicit reference to "electronic communications" that it had added in 1994.

Google mistakenly argues that the 1994 and 1996 amendments to the Wiretap Act—adding and removing "electronic communications" to and from Section 2510(16)'s list shows that communications over Wi-Fi networks qualify as "radio communications" under the Wiretap Act. *See* Google Br. at 32-37. In essence, Google argues that, in 1994, Congress made individuals liable for intercepting data traveling over home Wi-Fi networks lacking password protections, but gave the green light to such interceptions in 1996.

Instead, as shown above, Congress in 1994 clarified, and did not expand, the scope of the Wiretap Act's protection for electronic communications transmitted by radio. Therefore, the 1996 amendment did not eliminate that pre-1994 protection. The Wiretap Act simply reverted back to its pre-1994 meaning, which already protected electronic communications, including Wi-Fi communications. Congress explicitly stated as much, noting that electronic communications "are

already specifically and separately covered by the wiretap statutes." H.R. Conf. Rep. No. 104-518, 1996 U.S.C.C.A.N. 944, at 957 (1996) (emphasis added).

The legislative history further confirms that the 1996 amendment was merely a "technical" one.[12] This amendment was far from the monumental reversal of course that Google claims it was. *See Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468 (2001) (noting that Congress does not "hide elephants in mouseholes"). Indeed, had Congress really intended to reverse course just two years later—from protecting non-password-protected electronic communications sent by radio to allowing their interception with impunity—surely those who just two years earlier had added language to clarify their protected status would not have stood by in silence.

The legislative history also reveals that Congress believed the 1994 amendment had yielded unintended consequences, by creating the potential for liability when hobbyists using scanners, CBs, and Ham radios intercepted traditional, broadcast radio transmissions. *See* H.R. Conf. Rep. No. 104-518, 1996 U.S.C.C.A.N. 944, 957. Indeed, Senator Leahy, a key sponsor of this amendment to the Wiretap Act, explained that, "[i]n order to address radio hobbyists' concerns, we modified the original language of [the Wiretap Act] to clarify that intercepting

[12] Hearings before the Committee on the Judiciary, House of Representatives, on H.R. 1710, Testimony of law school professor and former Assistant U.S. Attorney James P. Fleissner, June 12, 1995, at 315 (describing the removal of "electronic communications" from Section 2510(16) as a "technical amendment[]").

traditional radio services is not unlawful." 132 Cong. Rec. S7987-04, 1986 WL 776264, at 18 (1986).

Congress' treatment of cordless telephone communications in 1986 and 1994 provides further confirmation that Wi-Fi communications are protected under the Wiretap Act. When Congress enacted ECPA, it "explicitly excepted protection for the radio portion of a cordless telephone" because "cordless phones acted essentially as a radio transmitter and could be intercepted easily with readily available technology, such as an AM radio. Congress therefore concluded that it would be inappropriate to criminalize the interception of such communications." *Price v. Turner*, 260 F.3d 1144, 1147-48 (9th Cir. 2001). Thus, the definitions of "wire communication and electronic communication expressly provided that such terms did not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit." *Id.* at 1147. By 1994, however, "when technological advances [had] made it more difficult to intercept cordless radio transmissions, Congress amended the Wiretap Act to include protection for cordless phone transmissions that could no longer be analogized to AM/FM radio transmissions." *Id.* at 1148. It did so by "simply omit[ing] the . . . language excepting the radio portion of cordless phone

communications" in the definitions of electronic communication and wire communication. *Id.* at 1147 n.1.[13]

Congress' treatment of cordless telephones—which communicate by radio between the handset and the base station within a person's home—confirms that Congress did not intend "radio communication," as used in the Wiretap Act, to encompass all communications by radio. That is because, if Google's interpretation of "radio communication" were correct, Congress only would have needed to amend the definition of wire communication, and would not have needed also to exclude cordless phone calls from the definition of electronic communication, to avoid criminalizing the interception of the radio portion of cordless calls in 1986. Such "radio communications" would have been "readily accessible to the general public" under § 2510(16) and "readily accessible" "electronic communications" under exemption G1 because they were not scrambled or encrypted—just as Google claims is true of communications over non-password-protected Wi-Fi networks. The fact that Congress found it necessary to draft the statutory definition of electronic communication to address

[13] Although Wi-Fi communications contain a radio portion, it is not the type that can be easily intercepted without sophisticated equipment, such as that used by Google. *See* Daniel Kamitaki, Comment, *Beyond E-Mail: Threats to Network Security and Privileged Information for the modern Law Firm*, 15 S. Cal. Interdisc. L.J. 307, 340 (2006) ("An attorney would probably not breach her ethical duty of confidentiality by using a WLAN *because the wireless signal offers comparable or greater security than most cordless or cellular phones*") (emphasis added).

specifically these private communications by radio is therefore further evidence that the district court correctly rejected Google's claim that "radio communication" includes *all* communications by radio.

Accordingly, as the District Court found, the legislative history of the Wiretap Act confirms that Congress used the term "radio communications" to exempt from liability the interception of public-directed, traditional radio services. Communications over Wi-Fi networks, whether password-protected or not, have been and remain private transmissions by radio that the Wiretap Act protects from unauthorized interception.

C. The District Court's Interpretation Is Consistent with the Wiretap Act's Purpose.

The Court should affirm the District Court's statutory interpretation for the additional reason that it comports with the purpose of the Wiretap Act by protecting private communications within the home from unauthorized interception. In contrast, Google's interpretation would lead to absurd and arbitrary results at odds with the "paramount objective" of the Wiretap Act: to "protect effectively the privacy of communications." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003).

First, Google's view that all data transmitted over a non-password-protected Wi-Fi network can be intercepted without statutory liability leads to the absurd result that the protection afforded to a communication could change after it is sent,

regardless of the protections implemented by the sender. For example, Google concedes that it cannot intercept an e-mail that Bob sends to Mary by tapping into Bob's wired connection to the Internet or his password-protected home Wi-Fi network. But, when Mary receives that same e-mail on her iPad, which is connected to her home Wi-Fi network (which, like many, is not password protected), Google could intercept that e-mail without liability. Bob, therefore, would be powerless to ensure that the privacy of his communication was protected. That is bad enough for personal e-mail, but if Bob is an attorney and Mary is his client, the undermining of the attorney-client communication is readily apparent.

Thus, under Google's incorrect reading of the Wiretap Act, the government and any business or individual would be free to employ sophisticated technology to intercept these confidential communications. In effect, such a circumstance would thwart individuals who reasonably rely on the privacy of Wi-Fi transmissions, and ultimately substantially chill the use of Wi-Fi networks. Considering that the original Wiretap Act, ECPA, the CALEA were all passed by Congress in order to keep pace with advancing technology, preserve confidential communications among individuals, and promote commerce, *see* 132 Cong. Rec. S7978-04, 1986 WL 176264, at *12, the Wiretap Act should not, unless its language demands otherwise, be interpreted to exclude Wi-Fi communications from its protection. Nothing in the Act's language requires that exclusion.

Second, Google's position creates a patchwork, crazy-quilt of protections for Wi-Fi networks, which Congress could not have intended. As Google concedes, if its interpretation of the statute were correct, it still could not intercept data carried over password-protected Wi-Fi networks, because such communications are "scrambled or encrypted." 18 U.S.C. § 2510(16)(A).

But even non-password-protected Wi-Fi networks could still fall within the protection of § 2510(16), under Google's expansive (and incorrect) interpretation of the statutory term "radio communication." For example, § 2510(16)(C) protects "radio communications" that are "carried on a subcarrier." Many common Wi-Fi protocols—though not all of them—are carried on a subcarrier.[14] Similarly, § 2510(16)(E) protects "radio communications" that are "transmitted on frequencies allocated under" certain FCC rules. Again, many of the channels that common Wi-Fi protocols use—though not all of them—use frequencies allocated under those rules.[15]

---

[14] In particular, transmissions using Wi-Fi protocols 802.11a, 802.11g, and 802.11n are divided into several parallel data streams or channels and are transmitted by subcarriers. *Ex Parte Janevski*, No. 2009-0671, 2009 WL 416502 (B.P.A.I. Feb. 18, 2009).

[15] For example, three of the channels that Wi-Fi protocol 802.11b uses (9, 10, and 11) transmit on frequencies between 2452 MHz and 2462 MHz, which have been allocated under FCC rules listed in § 2510(16)(E). *See* IEEE Standard 802.11 at 566 tbl. 15-7 (2007) (indicating the frequencies of the channels for the 802.11b protocol), http://standards.ieee.org/about/get/802/802.11.html (last visited Mar. 22, 2012); 47 C.F.R. § 74.602 (indicating that the frequencies allocated under FCC Rules Part 74(F) include 1990-2483 MHz); 47 C.F.R. § 101.147(a)(12) (indicating

Footnote continued on next page

Therefore, on Google's interpretation of the term "radio communication," whether particular Wi-Fi data packets are protected from interception would not turn merely on whether the network owner enabled password protection. It would also turn on the happenstance of the particular protocol a wireless device used to connect to a Wi-Fi router, or the particular channel the Wi-Fi router was using at the time. Yet Congress sought to avoid a situation where the Wiretap Act's protections are:

> the unanticipated byproduct of technology changes, and not a careful balancing of the needs of law enforcement and the privacy rights of individuals. Nor [would] they reflect a substantive difference in the nature of the information; rather they reflect the fact that the ECPA was enacted in 1986—six years before Congress authorized commercial activity on the Internet . . . .

Burr, J. Beckwith, *The Electronic Communications Privacy Act of 1986: Principles for Reform*, at 8, http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf (last visited March 22, 2012). As this Court noted in *Konop v. Hawaiian Airlines, Inc.*, "until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of the law." 302 F.3d 868, 874 (9th Cir. 2002). Google's interpretation aggravates, rather than relieves, such confusion and uncertainty.[16]

Footnote continued from previous page
that the frequencies allocated under FCC Rules Part 101, formerly Part 94, include 2450-2500 MHz).

[16] Although Plaintiffs-Appellees did not plead that certain of the class members' communications over their Wi-Fi networks are protected because they were

Footnote continued on next page

D. As the District Court Correctly Held, Plaintiffs-Appellees Properly Pled that Wi-Fi Communications Are Not "Readily Accessible to the General Public."

Wi-Fi communications are private, local transmissions, the contents of which can only be obtained and deciphered with sophisticated equipment. They are decidedly unlike traditional radio services such as CBs, Ham radios, television transmissions, and AM/FM radio broadcasts, which are intended to be received and decipherable by a broad audience over a large area. These "radio communications" are broadcast on systems designed and configured to broadcast messages to multiple and unidentified recipients—*i.e.*, anyone who can pick up the signal by dialing into the frequency. In sharp contrast, Wi-Fi communications are sent on systems designed to communicate privately and only with specific, identified recipients through technology such that the general public could not intercept and understand their communications.

The District Court aptly observed this distinction between traditional radio services and Wi-Fi communications. "Unlike in the traditional radio services context, communications sent via Wi-Fi technology, as pleaded by Plaintiffs-Appellees, are not designed or intended to be public." ER 24. Interception of

---

Footnote continued from previous page
transmitted by subcarrier or over frequencies allocated under the FCC rules listed in § 2510(16)(E)—because, properly interpreted, the Wiretap Act protects data transmitted over non-password-protected Wi-Fi networks—Plaintiffs-Appellees could readily plead such facts were the Court to accept Google's interpretation of the statute, and should be given the opportunity to do so.

Plaintiffs-Appellees' communications requires sophisticated, specially-designed software and hardware. As plead in Plaintiffs-Appellees' complaint, "the networks were themselves configured to render the data packets, or electronic communications, unreadable and inaccessible without the use of rare packet sniffing software; technology allegedly outside the purview of the general public." ER 25.

The District Court, therefore, correctly found that the complaint stated a claim under the Wiretap Act.

II. Congress Did Not Intend for § 2510(16) To Apply to Electronic Communications.

The Court may also affirm the District Court on an alternative ground: the definition of "readily accessible to the general public" in § 2510(16) on which Google relies does not apply to the statutory exemption (G1).

A. Because Congress Did Not Define "Readily Accessible To The General Public" With Respect to Electronic Communications, Its Ordinary Meaning Should Be Used.

Exemption G1 permits a 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." 18 U.S.C. § 2511(2)(g)(i). But Congress did not define the term "readily accessible to the general public" in the context of "electronic communications." It only defined that term "with respect to a radio

communication," *id.* § 2510(16), which thus limits the applicability of the term's definition to a separate exemption (G2) for certain "radio communication[s]" that are "readily accessible to the general public," *id.* § 2511(2)(g)(ii)(II).

Therefore, the phrase "readily accessible to the general public," which is undefined in the context of *electronic communications*, must be understood in light of the normal meaning of the words used in that phrase. *See S.D. Warren Co. v. Me. Bd. of Envtl. Prot.*, 547 U.S. 370, 370 (2006) ("[S]ince [the term] is neither defined nor a term of art, it should be construed in accordance with its ordinary or natural meaning.") (quotation omitted); *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."). Since Wi-Fi communications are not "readily accessible to the general public" within the ordinary meaning of that phrase—due to the sophisticated equipment needed to intercept these communications—Wi-Fi communications are not excluded from the protection of the Wiretap Act by Section 2511(2)(g)(i).

When Congress enacted ECPA, it added to the Wiretap Act two provisions that use the phrase "readily accessible to the general public." The first is Section 2511(2)(g)(i)—exemption G1—which permits the interception of "electronic communications" from an "electronic communication system that is configured so

that such electronic communication is readily accessible to the general public."[17] The second is Section 2511(2)(g)(ii)(II)—exemption G2—which permits the interception of "radio communications" from certain types of communications systems that are "readily accessible to the general public."

At the same time Congress enacted those provisions, it also enacted Section 2510(16), which defines the phrase "readily accessible to the general public," but only "with respect to a radio communication." *See* Pub. L. No. 99-508, §§ 101(a)(6), (b)(4) (1986). That is, in ECPA, Congress used the phrase "readily accessible to the general public" *twice*—once with respect to "electronic communications" (G1) and once with respect to "radio communications" (G2)—yet chose to define the phrase *only* "with respect to a *radio communication*." 18 U.S.C. § 2510(16) (emphasis added).

Congress' decision not to define the phrase with respect to electronic communications (or even the subset of electronic communications that are transmitted by radio) must be given meaning. The natural conclusion is that

---

[17] In debating the meaning of "readily accessible to the general public" in exemption G1 as applied to electronic communications, Congress listed some examples, and each example is a form of traditional public broadcast radio, *i.e.*, "radio communication": "subcarrier and UBI communications that are transmitted for the use of the general public . . .[,] includ[ing] the stereo subcarrier used in FM broadcasting or data carried on the VBI to provide closed-captioning of TV programming for hearing-impaired." S. Rep. No. 99-541, p. 17 (1986), 1986 U.S.C.C.A.N. 3555, 3572. These subcarriers are broadcast signals with information used in stereo sound generation and closed-captioning, for example.

Congress intended for the definition in Section 2510(16) to apply *only* to exemption G2 and not also to exemption G1. *See, e.g.*, *Lindh v. Murphy*, 521 U.S. 320, 330 (1997) (noting "the familiar rule that negative implications raised by disparate provisions are strongest when the portions of a statute treated differently had already been joined together and were being considered simultaneously when the language raising the implication was inserted").

Google's reading—that Congress intended the definition in § 2510(16) to apply to *some* electronic communications (those transmitted by radio)—also violates the rule that courts "refuse 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); *accord Harper v. U.S. Seafoods LP*, 278 F.3d 971, 975-76 (9th Cir. 2002). Under Google's interpretation, Section 2510(16) would define when an electronic communication transmitted by radio is "readily accessible to the general public," but would *not* define that phrase in the context of electronic communications transmitted by any other means recognized in the statute—whether "by a wire . . . electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12). Instead, the ordinary meaning of the words in the phrase "readily accessible to the general public," rather than the special definition in Section 2510(16), would apply to electronic communications

transmitted by a means other than radio. That is not consistent with the way courts construe statutes.[18]

Although the District Court found "congressional intent to apply Section 2510(16)'s definition of 'readily accessible to the general public' to exemption G1, and not merely to limit the application of Section 2510(16) to radio communications in exemption G2," ER 22, the court did not explain how that conclusion could be squared with the plain language of § 2510(16), or the canons of construction set forth above. Because Google relied exclusively on exemption G1 in its motion to dismiss—and cannot claim that exemption G2 applies here—this Court can uphold the District Court's judgment on the alternative ground that § 2510(16) should be interpreted according to its terms.

Furthermore, for the same reasons discussed above, Google's view that the Act provides a very substantial exemption to anyone who seeks to intercept any electronic communication sent over a radio network is flatly inconsistent with the purposes and objectives of ECPA. The Department of Justice agrees, noting that

[18] Although there is also a "natural presumption that identical words used in different parts of the same act are intended to have the same meaning," that presumption "is not rigid and readily yields" where, as here, there is reason to "conclud[e] that they were employed in different parts of the act with different intent." *Env. Def. v. Duke Energy Corp.*, 549 U.S. 561, 574 (2007) (internal quotation marks omitted). Congress' express statement that its definition in Section 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.

the Wiretap Act generally "bars third parties (including the government) from . . . installing electronic 'sniffers' that read Internet traffic."[19] Google's position would turn ECPA upside down, transforming it from a statute that broadly protects electronic communications from interception into one that broadly authorizes the interception of wireless electronic communications, unless the communicator takes affirmative steps to encrypt those communications.[20]

For these reasons, "readily accessible to the general public" in exemption G1 should be read according to its ordinary meaning.

B. Wi-Fi Communications Are Not "Readily Accessible to the General Public" Within the Normal Meaning of That Phrase.

As Plaintiffs-Appellees explain more fully above, Wi-Fi communications are not "readily accessible to the general public" within the normal meaning of that phrase. First, they are sent over very short distances, such that interception requires the listener to be in very close proximity (such as on the street in front of the individual's house). Second, the content of Wi-Fi communications cannot be accessed easily. Reading a Wi-Fi communication requires sophisticated

---

[19] COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, DEPT. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, at 167 (2009).

[20] If using thermal imaging to detect heat sources emanating from a home constitutes a Fourth Amendment search that requires a warrant, *see Kyllo v. United States*, 533 U.S. 27 (2001), a pro-privacy statute like the Wiretap Act should be interpreted to prohibit using packet sniffers to intercept Wi-Fi communications emanating a short distance from a house.

technology that is not readily available. Third, the general public is not even aware that Wi-Fi communications can be intercepted. While most people know that an unencrypted Wi-Fi network can be used by nearby individuals to access the Internet, few are aware that nearby individuals can, with the proper equipment, download all data passing through that network. ER 251 (¶¶ 110-16).

For these reasons, Wi-Fi communications are not "readily accessible to the general public," and regardless of whether they are radio communications, they do not fall within exemption G1 on which Google relies.

III. Google's Other Arguments Lack Merit.

A. The Communications Act Does Not Control the Meaning of "Radio Communications" in the Wiretap Act.

Google suggests that, because Congress in the Communications Act equated the terms "radio communications" and "communications by radio" in a definition provision, it must have also meant for the two terms to mean the same thing in the Wiretap Act, which contains many definition provisions, but not one that defines "radio communication" or "communication by radio." To the contrary, the Communications Act, and its relationship to the Wiretap Act, support the conclusion that plain meaning of "radio communication" is not, as Google argues, "communication by radio."

First, when Congress has intended for a definition from the Communications Act to apply to the Wiretap Act, it has explicitly said so. For example, the Wiretap

Act specifies that "'communication common carrier' has the meaning given that term in section 3 of the Communications Act of 1934." 18 U.S.C. § 2510(10). The fact that Congress explicitly chose to adopt the Communications Act definition for "communication common carrier" in the Wiretap Act indicates that Communications Act definitions should not apply where, as with radio communications, Congress chose not to incorporate them.

Second, Google relies on a canon of statutory construction that is simply inapplicable here. Congress defined "radio communication" in the Communications Act in 1934, three decades before the Wiretap Act was passed and half a century before that act was amended to include the term "radio communication." While, as a general rule, similar language in different statutes may inform how both statutes are to be construed, the interpretational aid one statute provides to another greatly diminishes when they are enacted many years apart. *See Smith v. City of Jackson*, 544 U.S. 228, 233 (2005) (presumption that Congress intended that the same language in two statutes having similar purposes to mean the same thing is most appropriate "when one is enacted shortly after the other"). Given the substantial amount of time between enactment of the Communications Act of 1934 and enactment of both the Wiretap Act and ECPA, the Communications Act offers little aid for interpreting the meaning of "radio communication" in the Wiretap Act.

Finally, as demonstrated above, Congress used the term "radio communication" and the phrase "communication by radio," or its cognates, differently in the Wiretap Act, with the natural reading that the term "radio communication" is not synonymous with the phrase "communication by radio." *See* Section I.A. at p. 20. In contrast, Congress has always treated the two terms as synonyms in the Communications Act. *See* Communications Act of 1934, § 3(b) (defining "'Radio communication' or 'communication by radio'" to "mean[] the transmission of by radio" of information); 47 U.S.C. § 153(40) (retaining the same definition, but now as a definition of the term "Radio communication").

B. Section 2510(16)'s Common Carrier Provision Reinforces the Wiretap Act's Protection of Private Radio Transmissions.

Google relies on Section 2510(16)(D), which defines radio communications that are "transmitted over a communications system provided by a common carrier" as not "readily accessible to the general public," to claim that "radio communications" in § 2510(16) encompasses more than traditional radio broadcasts. *See* Google Br. at 37-42. Google's reliance is misplaced. On the contrary, that provision—like the others in 2510(16)—confirms that Congress intended to distinguish publicly-directed radio broadcasts, for which the broadcaster has no reasonable expectation of privacy, from private radio transmissions, for which the transmitter has such an expectation and which Congress therefore has decided to protect from interception.

While cellular calls are essentially private, two-way communications, those communications are accomplished by broadcasting radio transmissions between cellular towers and handheld phones, which typically are located miles apart. These publicly-directed transmissions are radio communications that could, when ECPA was passed, be intercepted by anyone in a "large service area[] . . . either by sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls." H.R. Rep. No. 99-647, at 20 (1986); S. Rep. No. 99-541, 1986 U.S.C.C.A.N. 3555, at 3563 (1986). Cellular calls could even be inadvertently picked up by radio hobbyists "scanning radio frequencies in order to receive public communications," S. Rep. No. 99-541, 1986 U.S.C.C.A.N. 3555, at 3560 (1986), and even as late as 2001 it was "estimated that over 20 million scanners capable of intercepting cellular transmissions currently are in operation," *Bartnicki v. Vopper*, 532 U.S. 514, 549 (2001).[21]

At the time, all cellular voice communications were transmitted, in part, over a wire or cable, and thus were protected as "wire communications" under the Wiretap Act. *See* 18 U.S.C. § 2510(1), (18). However, in the face of "a real-life conflict as interception technology catches up with communication development," H.R. Rep. No. 99-647, at 21 (1986), Congress wanted to make clear that cellular calls could not be intercepted without penalty, and so also protected them through

[21] Congress did not even prohibit the marketing of such devices until 1993, well after it enacted ECPA. *See Bartnicki*, 532 U.S. at 549.

the common carrier exception in Section 2510(16)(D).[22] The fact that technology has changed—and such communications are no longer so easily intercepted—does not support Google's view that this provision evidences a congressional intent that "radio communications" means all communications transmitted by radio.[23] Rather, Congress' classification of cell phone calls as radio communications—given the distance they travel and the ease with which, for years, their content could be intercepted—is perfectly consistent with radio communications being publicly-directed broadcasts.

C. The Rule of Lenity Is Inapplicable Here.

Google claims that, if there is "*any* ambiguity in the Wiretap Act," the rule of lenity requires the Court to resolve that ambiguity in Google's favor and against

---

[22] The inclusion of cellular communications in Section 2510(16) was also intended to ensure such communications remained protected from interception if future cellular technology allowed for end-to-end transmissions without ever using a wire, at which point those communications would no longer be protected as wire communications. *See* H.R. Rep. No. 99-647, at 32 (1986).

[23] Congress treated tone-only paging systems differently from other common carrier communication systems, but this distinction does not support Google's position here. In 1986 there were three types of paging devices: tone-only, digital, and voice. *See* H.R. Rep. No. 99-647, at 23 (1986). Digital and voice pagers could receive actual messages (alphanumeric or audio). Users had a reasonable expectation of privacy in such communications, and they were, appropriately, protected under section 2510(16)(D). By contrast, tone-only pagers could not receive messages; they simply notified the user that a message was waiting elsewhere. To get the message, the user had to call an answering service. *See id.*, at 23-24. On the recommendation of the Department of Justice, Congress concluded that users of tone-only pagers had no reasonable expectation of privacy in that fact. *See Id.* at 24.

the protection of Wi-Fi users in their homes. *See* Google Br. at 42 (emphasis added). Google misstates when the rule of lenity may be applied. Rather, the rule of lenity "only applies if, after considering text, structure, history, and purpose, there remains a *grievous* ambiguity or uncertainty in the statute, such that the Court must simply *guess* as to what Congress intended." *Barber v. Thomas*, 130 S. Ct. 2499, 2508-09 (2010) (emphasis added, citation omitted) (quoting *Muscarello v. United States*, 524 U.S. 125, 139 (1998), and *Bifulco v. United States*, 447 U.S. 381, 387 (1980)); *see also Smith v. United States*, 508 U.S. 223, 239 (1993) (rule of lenity is not triggered unless grievous ambiguity persists after "seizing every thing from which aid can be derived") (quotation marks and alterations omitted). "The simple existence of some statutory ambiguity . . . is not sufficient to warrant application of that rule, for most statutes are ambiguous to some degree." *Dean v. United States*, 129 S. Ct. 1849, 1856 (2009) (quoting *Muscarello*, 524 U.S. at 138).

Here, the text, structure, history, and purpose of the Wiretap Act, as discussed above, supports the District Court's reading, which harmonizes the Act with Fourth Amendment protections and individuals' realistic and reasonable expectations of privacy in their homes and private communications. Furthermore, Google cannot demonstrate a "grievous ambiguity" in the term "radio communication" as used in the Wiretap Act. In fact, as shown above, the District Court properly concluded—after using the normal tools of statutory construction—

that "radio communication" excludes the Wi-Fi communications at issue here. In short, the rule of lenity has no application here.

CONCLUSION

For the foregoing reasons, the District Court's Opinion denying Google's motion to dismiss should be affirmed.

Dated: March 23, 2012

Respectfully submitted,

By: */s/ Jeffrey L. Kodroff*

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

By: */s/ Daniel A. Small*

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

Interim Co-Lead Counsel

Dated: March 23, 2012

By: */s/ Elizabeth J. Cabraser*

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

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

Interim Liaison Counsel

STATEMENT OF RELATED CASES

Appellee is not aware of any related case pending before this Court.

Dated: March 23, 2012

/s/ Jeffrey L. Kodroff

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

CERTIFICATE OF SERVICE

I hereby certify that on March 23, 2012, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: March 23, 2012

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

By: */s/ Jahan C. Sagafi*
Jahan C. Sagafi

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

CERTIFICATE OF COMPLIANCE

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

This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 11,491 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

Dated: March 23, 2012

/s/ Jeffrey L. Kodroff

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