No. 11-17483

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BENJAMIN JOFFE, *et al.*,

Plaintiffs-Appellees,

v.

GOOGLE INC.,

Defendant-Appellant

On Appeal from the United States District Court
for the Northern District of California, Case No. 5:10-MD-2184-JW
Hon. James Ware, U.S. District Judge

REPLY BRIEF OF APPELLANT GOOGLE INC.

David H. Kramer
Michael H. Rubin
Brian M. Willen
Caroline E. Wilson
WILSON SONSINI GOODRICH & ROSATI
PROFESSIONAL CORPORATION
650 Page Mill Road
Palo Alto, CA 94304
(650) 493-9300

Counsel for Appellant Google Inc.

April 20, 2012

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTRODUCTION

In their brief, Plaintiffs agree with—or offer no response to—many of the key points made in Google's opening brief:

Google's Statement	Plaintiffs' Response
Wi-Fi transmissions are radio-based. Google Br. 3-4, 21.	Agree. Pl. Br. 15.
The term "radio communication" in the Wiretap Act should be given its ordinary meaning. Google Br. 26-27.	Agree. Pl. Br. 17.
The ordinary meaning of "radio communication" includes all communications made by radio. Google Br. 27-28.	None
Wi-Fi transmissions are "radio communications" under the Communications Act definition. Google Br. 30-31.	None
An "electronic communication" can also be a "radio communication" under the Wiretap Act. Google Br. 24-25.	Agree. Pl. Br. 26.
Plaintiffs' Wi-Fi transmissions were not scrambled or encrypted. Google Br. 22.	None
Both cellular telephone calls and pager transmissions are "radio communications" under the Wiretap Act. Google Br. 37-42.	Agree. Pl. Br. 47-48 & nn.22-23.
The 1994 amendments to the Wiretap Act show that Congress understood transmissions like Wi-Fi to be "radio communications." Google Br. 34-35.	None

Google's interpretation of "radio communication" would not lead to absurd results under Section 2511(2)(g)(ii). Google Br. 54-58.	None

Despite conceding or failing to address most of Google's arguments, Plaintiffs still contend that Google violated the Wiretap Act by allegedly intercepting their unencrypted Wi-Fi transmissions. Plaintiffs make two main arguments; neither has merit.

First, Plaintiffs claim that Section 2510(16)'s definition of "readily accessible to the general public" is categorically inapplicable to Section 2511(2)(g)(1) ("G1"). The district court correctly rejected this argument when Plaintiffs made it below. Plaintiffs' position rests on the premise that an "electronic communication" cannot also be a "radio communication." That premise is wrong. The Wiretap Act makes clear—and Plaintiffs admit—that those terms are not mutually exclusive. And Plaintiffs' assertions about the relationship between 2510(16) and G1 are expressly refuted by the legislative history.

Second, Plaintiffs argue that Wi-Fi transmissions are not "radio communications" under the Wiretap Act. According to Plaintiffs, the term "radio communication" is limited to "traditional radio services" and what they call "public-directed radio broadcast communications" (a term that has no grounding in the statute or its legislative history).

Here too, Plaintiffs depart both from what the district court held and from what they themselves argued below. But their new definition is equally misguided. Nothing about the way "radio communication" is used in the Wiretap Act requires a narrow reading of the term or suggests that it means something different from the syntactically identical phrase "communication by radio." Nor can Plaintiffs evade the 1994 amendment and its repeal, which clearly show that Wi-Fi transmissions are radio communications that, unless encrypted, are not protected by the statute. Finally, Plaintiffs defeat their own argument by now conceding that cellular-telephone calls and paging-system transmissions are both "radio communications." Plaintiffs' suggestion that those radio-based communications technologies can be meaningfully distinguished from Wi-Fi is unconvincing.

In sum, Plaintiffs offer nothing to change the simple facts that decide this case: (1) Wi-Fi transmissions are "radio communications" because they are carried by radio waves; (2) radio communications are "readily accessible to the general public" under G1 unless one of Section 2510(16)'s exceptions applies; and (3) none of those exceptions was pleaded or is applicable here.

ARGUMENT

I. SECTION 2510(16) APPLIES TO ANY "RADIO COMMUNICATION" THAT IS ALSO AN "ELECTRONIC COMMUNICATION"

Google showed in its opening brief (at 23-25) why the district court was correct to hold that "the legislative history and text of the statute demonstrate 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). Without even acknowledging Google's arguments, Plaintiffs recycle their claim that the Wiretap Act's definition of "readily accessible" somehow does not apply to the use of that phrase in G1. Pl. Br. 38-43. Plaintiffs are still wrong.

It is true, of course, that G1 refers to "electronic communications," while Section 2510(16) defines what "readily accessible to the general public" means "with respect to a radio communication." As Plaintiffs acknowledge (Pl. Br. 26), however, the terms "electronic communication" and "radio communication" are not mutually exclusive. Indeed, because "all communications transmitted only by radio are electronic communications" (S. Rep. No. 99-541, at 14 (1986)), many electronic communications are simultaneously radio communications. Congress could hardly have been clearer: "Inclusion of the term 'radio' in the def-

inition of 'electronic communication' in Section 2510(12) reflects the fact that radio communications come within the scope of chapter 119." H.R. Rep. No. 99-647, at 36 (1986).

Once the overlapping relationship between electronic communications and radio communications is understood, Plaintiffs' argument collapses. For any electronic communication that is also a radio communication, Section 2510(16) provides a specialized (and objective) definition for the phrase "readily accessible to the general public" in G1. The legislative history on this point is definitive. In describing G1, both the House and Senate Reports observe that "the term 'readily accessible to the general public' is a defined term with respect to radio communications." H.R. Rep. No. 99-647, at 41; S. Rep. No. 99-541, at 18; *see also* S. Rep. No. 99-541, at 15 (explaining, in discussing G1, that "the radio communications specified in proposed subsection 2510(16) are afforded privacy protections under this legislation unless another exception applies"). Congress unquestionably intended the combination of 2510(16) and G1 to govern the interception of radio communications.

Plaintiffs offer no response to this legislative history. They allude to a passage in the Senate Report that gives some examples of specific radio communications that would be protected by G1. Pl. Br. 40 n.17 (citing S. Rep. No. 99-541, at 17). But that passage only further un-

dermines Plaintiffs' argument. The reason the particular radio communications discussed in the Report (the "stereo subcarrier used in FM broadcasting" and "data carried on the VBI to provide closed-captioning of TV programming") are protected from interception is because they are among those that Section 2510(16) deems not "readily accessible to the general public." S. Rep. No. 99-541, at 15, 18 (Section 2510(16)(C)'s subcarrier exception makes it unlawful to intercept "data carried on the Vertical Blanking Interval (VBI) of a television signal").

Plaintiffs also refer to the interpretive canon that generally discourages courts from attributing different meanings to the same statutory phrase. Pl. Br. 41. But that canon does not apply here because the Wiretap Act specifically dictates a different result. *Cf. Atl. Cleaners & Dyers v. United States*, 286 U.S. 427, 433 (1932). For those "electronic communications" that are also "radio communications," the Act expressly gives the phrase "readily accessible to the general public" a specialized definition, which does not apply to other electronic communications. Defining that phrase differently for different types of communications is not anomalous; it is exactly what Congress intended.[1]

[1] Because "readily accessible to the general public" is a defined term with respect to the Wi-Fi transmissions at issue in this case, it is irrelevant whether, as Plaintiffs argue, those transmissions would be considered "readily accessible" under "the normal meaning of that phrase." Pl. Br. 43. For that same reason, the various policy argu-

II. PLAINTIFFS' INTERPRETATION OF "RADIO COMMUNICATION" IS CONTRARY TO THE WIRETAP ACT'S TEXT AND LEGISLATIVE HISTORY

Plaintiffs ultimately recognize that this appeal turns on a straightforward interpretation of the Wiretap Act: does "radio communication" cover all communications made by radio or should it be limited to some narrow subset of radio-based transmissions? Plaintiffs contend that the term extends only to "traditional radio services" and what they label "public-directed radio broadcast communications." According to Plaintiffs, those are "radio communications" because they "are broadcast great distances and/or their content is readily accessible to the public through unsophisticated equipment[.]" Pl. Br. 16.

Plaintiffs' proposed definition is arbitrary and indeterminate, but those are only some of its flaws. Plaintiffs do not attempt to explain how their interpretation accords with, much less is required by, the ordinary meaning of "radio communication." It is telling in that respect that Plaintiffs' new definition differs from the one they posited below. There, Plaintiffs argued, and the district court agreed (ER 21-23), that Congress intended the term "to refer only to radio broadcasts" and thus to exclude transmissions made by cellular telephones. SER 2-5. Now, however, Plaintiffs say that the term "radio communication" includes

---

ments offered by *amicus curiae* Electronic Privacy Information Center have nothing to do with the legal issues raised by this appeal.

more than ordinary radio broadcasts, and Plaintiffs expressly concede that it covers transmissions made by cellular telephones. Pl. Br. 48. Its novelty aside, the latest version of Plaintiffs' interpretation is equally at odds with the Wiretap Act.

A. The Ordinary Meaning of "Radio Communication" Includes Any Communication Made By Radio

Google's opening brief showed (at 26-28, 30-31 & n.11) that the term "radio communication" is naturally and commonly understood to include to all communications made by radio. Plaintiffs offer no response.[2] Instead, while Plaintiffs agree that "radio communication" should be given its ordinary meaning (Pl. Br. 17), their proposed interpretation does nothing of the sort. Plaintiffs propose a definition that is both narrow and nebulous, under which "radio communication" would be limited to "traditional radio services" and "public-directed radio broadcast communications." Pl. Br. 16, 20-21, 46-48. Plaintiffs cite nothing—no dictionaries, no authorities of any kind—to suggest that their approach is consistent with how the term "radio communication"

[2] Plaintiffs argue that "Google's attempt to escape the Wiretap Act's prohibition on interception by equating Wi-Fi communications with traditional radio broadcasts fails." Pl. Br. 17. But Google never tried to equate the two. To the contrary, Google explained that the term "radio communication" is *not* confined, as the district court had mistakenly held, to traditional radio broadcasts.

is used in common parlance. Plaintiffs' definition bears no relationship to the ordinary meaning of radio communication, and Plaintiffs barely even pretend that it does.

1. The uses of "radio communication" throughout the Wiretap Act do not support Plaintiffs' restrictive definition

Plaintiffs point to the four places where the Wiretap Act uses the term "radio communication." Pl. Br. 18-20. But those usages lend no support to Plaintiffs' argument.

Section 2511(2)(g)(ii) ("G2") describes certain radio communications that are always freely interceptable. It does not define "radio communication" narrowly (or at all), depend on a narrow understanding of the term, or provide an exhaustive list of all radio communications. Neither does G2 purport to make it lawful to intercept "any radio communication." It instead identifies four categories of radio communication that may lawfully be intercepted. One set of radio communications that G2 makes freely available to the general public is traditional AM, FM and television services. 18 U.S.C. § 2511(2)(g)(ii)(I); H.R. Rep. No. 99-647, at 42 n.86; 47 C.F.R. § 73 *et seq.* The services G2 identifies comprise just some of the radio-based transmissions encompassed by the term "radio communication"—not all of them.

The same is true of Section 2511(5)(a)(i)(B), which allows the federal Government to bring a suit based on the interception of unscrambled radio communications "transmitted on frequencies allocated" under subpart D of Part 74 of the FCC rules. Those types of transmissions are just other examples of "radio communications," not the full universe of them. Indeed, this example undermines Plaintiffs' argument that "radio communication" refers to publicly directed radio services: Plaintiffs admit that the transmissions covered by Section 2511(5)(a)(i)(B) are not publicly broadcasted or directed. Pl. Br. 19.[3]

The final use of "radio communication" in the statute similarly contradicts Plaintiffs' approach. As explained in Google's opening brief (at 37-42, 49-52), Section 2510(16) presupposes that "radio communication" covers more than just traditional or publicly directed radio transmissions. Ignoring Google's arguments, Plaintiffs contend that 2510(16) is confined to actions that a radio broadcaster can take to bring a "publicly broadcast radio communication into something protected by statute." Pl. Br. 19-20. That is not so. For example, the radio communications protected by 2510(16)(D)'s Common-Carrier Excep-

[3] Likewise, Section 2511(2)(g)(v), which makes it lawful for users of the same frequency to intercept unscrambled "radio communications" on that frequency, does not suggest that the term is limited to traditional radio services. That provision works just as well if it applies to all radio-based transmissions—and Plaintiffs do not claim otherwise.

tion—including cellular telephone calls and pager transmissions—were never intended to be broadcast publicly, and they were not made private by being transmitted by a common carrier. Instead, they are non-traditional radio services that Congress specifically exempted from the statute's presumption that radio communications are readily accessible to the general public. H.R. Rep. No. 99-647, at 32, 37.

Plaintiffs thus are wrong to assert that "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[.]" Pl. Br. 20. Congress did nothing of the sort, and the way it actually used the term confirms that "radio communication" was intended to bear its ordinary broad meaning, not some artificially narrowed one.

2. "Radio communication" and "communication by radio" mean the same thing

Plaintiffs next argue that Congress made a careful distinction between the terms "radio communication" and "communication by radio," using the latter to refer to "all communications that use radio waves." Pl. Br. 20-21. There is no support for this argument. Because both terms are undefined by the Wiretap Act, both must take their ordinary meaning. And, while one is a compound noun and the other uses a prepositional phrase, the two terms mean exactly the same thing in or-

dinary speech. Just as "train travel" and "travel by train" are synonymous, there is no semantic daylight between "radio communication" and "communication by radio."

Plaintiffs nevertheless insist that the two terms should be given totally different meanings. For that counterintuitive result to even possibly be right, there would have to be compelling evidence that Congress intended it. Plaintiffs offer no evidence whatsoever. By citing the various provisions of the Wiretap Act that include the phrase "communication by radio," Plaintiffs show only that the statute uses both phrases, but they provide no basis for thinking that the two terms were deliberately used to refer to different things. Accepting that "communication by radio" has a broad meaning in the statute in no way suggests that the cognate term "radio communication" was intended to (or should) apply narrowly or differently.

3. The Communications Act confirms the ordinary meaning of "radio communication" and "communication by radio"

That is particularly true against the backdrop of the Communications Act, which expressly defines "radio communication" and "communication by radio" as synonyms—and as referring to all communications transmitted by radio. 47 U.S.C. § 153(40). As Google has explained

(Google Br. 30-32), that definition is totally inconsistent with Plaintiffs' interpretation of "radio communication."

Plaintiffs do not respond to Google's argument that the close relationship between the Communications Act and the Wiretap Act—including their mutually dependant regulation of "radio communications"—provides an especially compelling reason to understand the term the same way in both. Instead, Plaintiffs state the obvious, that Congress did not expressly incorporate the Communications Act definition into the Wiretap Act. That changes nothing. For a term like "communication common carrier" (*see* Pl. Br. 44-45), which has a specialized definition under the Communications Act (47 U.S.C. § 153(11)) that might otherwise have been disregarded, it made sense for Congress to specifically adopt that definition in the Wiretap Act. In contrast, the Communications Act definition of "radio communication" reflects its ordinary meaning, notably including that it means the same thing as "communication by radio." There was no need for Congress to expressly incorporate that definition in the Wiretap Act for those terms to carry that same ordinary meaning there.[4]

[4] Plaintiffs make the odd claim that the Communications Act definition should be ignored because of the amount of time that went by before the Wiretap Act was enacted. But the passage of time is hardly a basis for giving "radio communication" a different definition. *Smith v. City of Jackson*, 544 U.S. 228 (2005), does not support that result.

B. The Wiretap Act's Legislative History Refutes Plaintiffs' Interpretation

1. The 1994 amendment confirms that Wi-Fi transmissions are "radio communications"

Google showed in its opening brief (at 32-37) that the Wiretap Act's 1994 amendment (and its prompt repeal) confirmed two critical facts: (1) that "radio communication" includes wireless computer-to-computer transmissions such as Wi-Fi; and (2) that the current version of the statute does not protect such transmissions from interception, unless they are encrypted or another 2510(16) exception applies. Plaintiffs offer no response to the first point. Their response to the second point misunderstands the purpose of the 1994 amendment and the effect of its repeal.

Plaintiffs argue that the 1994 amendment was merely a "belt-and-suspenders effort" that confirmed that the Wiretap Act (as amended by

---

There, the Supreme Court applied the rule that when two related statutes use the same language, "it is appropriate to presume that Congress intended that text to have the same meaning in both statutes." *Id.* at 233. That is quite right, and the Court did not suggest that the rule's force "greatly diminishes when [the statutes] are enacted many years apart." Pl. Br. 45. Nor is that the law. *Cf. United States v. Anderson*, 989 F.2d 310, 312-13 (9th Cir. 1993). The decades that separate the Communications Act from the Wiretap Act actually underscore how deeply seeded it was by the time "radio communication" was first used in the Wiretap Act that the term includes all radio-based transmissions.

ECPA in 1986) protected all radio-based communications in which users had a reasonable expectation of privacy. Pl. Br. 26-29. Plaintiffs' story ignores a basic rule of statutory interpretation. *Gill v. Villagomez*, 140 F.3d 833, 836 (9th Cir. 1998) ("we assume from statutory amendments a purpose to change existing law."). It is also contradicted by the legislative history. Plaintiffs disregard the explanation provided in Google's brief (at 32-37), which showed that the 1994 amendment expanded the Act's protections for radio-based communications.

In particular, Plaintiffs fail to confront the key finding of the 1991 Task Force, which recognized that, under ECPA, whether radio-based wireless data communications "will be legally protected from unauthorized interception will depend" on whether one of the specific Section 2510(16) exceptions applies. S. Hrg. 103-1022, at 183 (Mar. 18 & Aug. 11, 1994). Accordingly, the Task Force concluded, "there is a likelihood that such communications will not be protected unless the user goes to the expense of full data encryption." *Id.* The Task Force Report thus refutes Plaintiffs' argument.

The 1994 amendment was a direct response to the Task Force's recommendation that "the legal protections of ECPA be *extended* to cover new wireless data communications[.]" H.R. Rep. No. 103-827, pt. 1, at 12 (1994) (emphasis added); *see also* S. Hrg. 103-1022, at 183. Con-

gress made clear that the new legislation went beyond existing law, explaining that the amendment "[*e*]*xtends* privacy protections of the [ECPA] to cordless phones and certain data communications transmitted by radio." H.R. Rep. No. 103-827, pt. 1, at 18 (emphasis added). Plaintiffs say nothing about this definitive evidence that the 1994 amendment changed the status quo, and did not merely clarify it.[5]

Plaintiffs also overlook the significance of how Congress expanded the law. The 1994 amendment enacted a new exception to Section 2510(16), which designated "electronic communications" as an additional category of "radio communications" expressly classified as not "readily accessible to the general public." That confirms that wireless data communications, such as Wi-Fi transmissions, are "radio communications" under the Wiretap Act. Understanding them as such was the entire basis for protecting them under the amendment.

Given all that, Plaintiffs are wrong about the consequences of Congress' decision in 1996 to repeal the 1994 amendment. Plaintiffs

---

[5] The legislative history that Plaintiffs cite does not say otherwise. Nothing in then-Director Freeh's testimony suggests that "that the purpose of the amendment was *not* to protect previously unprotected radio communications" (Pl. Br. 27). Freeh merely observed in general terms that the amendment provides "clarification of privacy protection for electronic communications transmitted by radio" (S. Hrg. 103-1022, at 15). That is true, and the clarity that Congress provided came in the form of an amendment that altered existing law.

suggest that it would be odd for the repeal of an amendment to return the statute to the *status quo ante* (Pl. Br. 29-30), but that is precisely what a repeal does. *See, e.g.*, *Yakima Valley Memorial Hospital v. Wash. State Dept. of Health*, 654 F.3d 919, 934 (9th Cir. 2011). What happened here thus is totally different from *Whitman v. American Trucking Associations, Inc.*, 531 U.S. 457, 468 (2001), which applied the presumption that Congress "does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions[.]" Congress did nothing like that in the Wiretap Act. Instead, it enacted—and then deliberately repealed—a statutory amendment. Congress could hardly have failed to expect that the repeal would have the effect of undoing the legislative work done by the original amendment.

Finally, Plaintiffs rely on the statement accompanying the 1996 repeal that "electronic communications 'are already specifically and separately covered by the wiretap statutes.'" Pl. Br. 29-30 (quoting H.R. Rep. No. 104-518 (1996)). And so they are. 18 U.S.C. § 2511(1). But that protection has always been qualified by the provisions allowing an electronic communication that is also a radio communication to be lawfully intercepted unless it falls within one of the Section 2510(16) exceptions. In striking one of those exceptions, Congress returned the Wiretap Act's treatment of radio communications to what it had been before.

Under that framework, unencrypted Wi-Fi transmissions are a form of radio communication that enjoys no special protection.

2. Congress' treatment of cordless telephones further undermines Plaintiffs' argument

Plaintiffs next argue that Congress' treatment of cordless telephone transmissions—radio-based transmissions between the handset of a cordless telephone and the base unit—shows that the term "radio communication" does not cover all radio-based transmissions. Pl. Br. 31-33. It actually shows the opposite.

Cordless telephone transmissions are short-range radio transmissions that are neither traditional radio broadcasts nor publicly directed. *See* H.R. Rep. No. 99-647, at 21. Under Plaintiffs' interpretation, therefore, such transmissions would not count as "radio communications." But it could not be clearer that Congress intended otherwise. In 1994, when the Wiretap Act for the first time made it unlawful to intercept cordless telephone transmissions, Congress provided a reduced penalty for such interceptions. That penalty provision expressly identified "a cordless telephone communication" as a "radio communication." *See* Pub. L. No. 99-508 § 101(d)(2), 100 Stat. 1848 (1986); Pub. L. No. 103-414 § 202, 108 Stat. 4279, 4290-91 (1994); Google Br. 40 n.13.

Ignoring this provision, Plaintiffs claim that if cordless telephone transmissions were "radio communications," Congress would not have

needed to expressly exclude them from the definition of "electronic communication" when, in 1986, it had decided to leave them free to intercept. Pl. Br. 32-33. Plaintiffs' argument is inscrutable. Had cordless transmissions been classified as "electronic communications," their interception still might have been deemed unlawful if they fell within one of the Section 2510(16) exceptions. Congress wanted to leave no doubt that cordless transmissions were unprotected, and so it took the extra step of carving them out of the definitions of both wire and electronic communications. S. Rep. No. 99-541, at 12, 14.

But even assuming this carve-out was not strictly necessary to achieve Congress' goal, that would not help Plaintiffs. As Plaintiffs themselves observe, it is not uncommon for Congress to draft provisions that appear duplicative "to make assurance double sure." Pl. Br. 28 (citation omitted). Congress' decision to make double sure that cordless transmissions were free to intercept does not affect the meaning of "radio communication." It certainly does not change the fact that cordless transmissions were expressly labeled as "radio communications" by the Wiretap Act.

Congress' approach to cordless telephones confirms Google's argument. It demonstrates that "radio communication" includes all radio transmissions, regardless of whether they are traditional radio services,

and that Congress can take targeted action to protect radio communications when it thinks it appropriate. Congress' failure to do that for Wi-Fi transmissions (with the exception of the short-lived 1994 amendment) is no reason for courts to distort the Wiretap Act.

3. Protecting email does not require or allow altering the meaning of "radio communication"

Plaintiffs make a final argument from the legislative history: they claim that because one purpose of the Wiretap Act was to protect email, the statute must be understood to cover Wi-Fi transmissions, which sometimes include emails. Pl. Br. 24-26. This misunderstands both how the Wiretap Act works and the practical effect of Google's position.

As a rule, the Wiretap Act does not protect particular types of content; it protects particular kinds of *communications*. And "[t]he rules governing interception or disclosure may be different for each type of communication." H.R. Rep. No. 99-647, at 35. The medium by which a piece of content (such as an email) is transmitted determines what protection, if any, the Wiretap Act provides. If several different technologies are used to transmit a document, the protection offered that document may vary throughout its journey. *Id.* at 34 ("different aspects of the same communication might be differently characterized"); *see infra* pp. 28-29 (discussing cordless phones).

That matters because radio technology for transmitting data between computers was unknown to Congress when ECPA was enacted in 1986. Neither the statute nor its legislative history directly addressed whether email would be protected while being transmitted via unencrypted radio signals. That does not mean that the Act lacks rules for determining the permissibility of intercepting such transmissions. As discussed, the statute generally left radio-based communications free to intercept unless they were encrypted (or otherwise singled out for protection). There is no basis for abandoning that framework merely because email may be among the content transmitted by radio, and it does not mean open season on email. Under the correct understanding of the Wiretap Act, emails transmitted via Wi-Fi are fully protected so long as the Wi-Fi network is encrypted, as most are and all can be. If Congress thinks additional protections are appropriate, it can change the law.

C. Plaintiffs' Interpretation of "Radio Communication" Founders on the Common-Carrier Exception

Google's opening brief (at 37-42) explained that the district court's effort to limit radio communications to traditional radio broadcasts is irreconcilable with Section 2510(16)(D)'s Common-Carrier Exception. That exception shows that radio transmissions that are not traditional radio services—including cellular telephone calls and paging-system communications—nevertheless are "radio communications." In re-

sponse, Plaintiffs abandon the district court's approach, but their new interpretation is equally belied by the Common-Carrier Exception.

1. Both cellular and Wi-Fi transmissions are "radio communications"

Plaintiffs begin with a significant admission: they concede that cellular telephone calls are "radio communications" based on the Common-Carrier Exception. Pl. Br. 47-48. With that, Plaintiffs significantly depart from the district court's interpretation of the term, which was premised on *excluding* cellular transmissions. ER 21-23.[6] Plaintiffs nevertheless argue that even though cellular transmissions are "radio communications," Wi-Fi transmissions are not. Plaintiffs cannot walk that tightrope.

Plaintiffs first claim that cellular transmissions, in contrast to Wi-Fi, are "publicly-directed transmissions." Pl. Br. 47. Plaintiffs cite nothing to support that counterintuitive statement. If cellular telephone calls—quintessential one-to-one private transmissions—are "publicly directly transmissions," then that term has no meaning. *Cf.* ER 24 (district court observing that, "as alleged," Wi-Fi technology and cellular

[6] Plaintiffs' concession also departs from their own argument below that cellular telephone calls are "transmitted in part by radio waves, yet the Act is clear that they are wire communications, not radio communications." SER 5.

telephone technology "are both designed to send communications privately, as in solely to select recipients").[7]

Plaintiffs next try to distinguish cellular phone calls from Wi-Fi on the grounds that cellular transmissions (i) can travel for "miles" between a cell tower and a handset, and (ii) could, at least when ECPA was enacted, sometimes be intercepted using "sophisticated scanners designed for that purpose[.]" Pl. Br. 47 (quoting H.R. Rep No. 99-647, at 20). Even if these were plausible factual distinctions (which they are not), they would provide no viable basis for treating cellular calls, but not Wi-Fi transmissions, as radio communications. Nothing in the Wiretap Act or its legislative history indicates that Congress expected the definition of "radio communication" to turn on either the distance that a particular radio transmission travels or the relative sophistication of the equipment needed to acquire it.

Indeed, Plaintiffs' approach undermines the basic purpose of Section 2510(16). That provision is designed to provide clear rules for when a radio communication is "readily accessible to the general public." Rather than leave that question to the vagaries of the "reasonable expectation of privacy" test, Congress provided that a radio communica-

[7] As shown in Google's opening brief (at 5 n.2), moreover, many Wi-Fi communications *are* publicly directed transmissions. Plaintiffs do not even address that, much less rebut it.

tion is "readily accessible" as long as it is not one of the specific kinds of communications described in the 2510(16) exceptions. H.R. Rep. No. 99-647, at 37. Each of those exceptions turns on objective and readily ascertained criteria. Plaintiffs would subvert that structure by importing into the definition of "radio communication" itself the very subjectivity and uncertainty that Congress tried to avoid.[8]

Moreover, Plaintiffs' purported distinctions between cellular communications and Wi-Fi transmissions (Pl. Br. 16-17, 47-48) rest on unsupported, unpleaded, and incorrect factual assumptions. It is not true, for example, that cellular transmissions are necessarily broadcast over "great distances" while Wi-Fi signals travel "very short distances." Pl. Br. 16. The distance that a radio signal travels is not inherent in the mode of transmission, but depends on location-specific factors. *See* Encyclopædia Britannica Online, *Radio-wave propagation*, http://www.britannica.com/EBchecked/topic/585825/telecommunications-media/76247/Radio-wave-propagation (last visited April 20, 2012).

[8] Plaintiffs do not explain how far a transmission must travel before it becomes a radio communication; how readily available the equipment must be that allows members of the public to intercept it; or what happens when technology evolves so that a given radio transmission can travel farther or become easier to intercept. The definition and regulation of "radio communications" was not meant to turn on such indeterminate and variable factors.

Some Wi-Fi signals travel considerable distances and some cellular telephone signals do not. At a given location, the signals used to connect to a Wi-Fi network may travel considerably farther than the signals used to place a cellular telephone call.[9]

Nor is it accurate that unencrypted Wi-Fi transmissions are significantly more difficult to intercept than cellular transmissions were when ECPA was enacted. What is needed to intercept unencrypted Wi-Fi transmissions is widely available off-the-shelf or freely downloadable from the Internet, and is no more advanced than the "sophisticated scanners" designed to intercept cellular transmission that Plaintiffs invoke (Pl. Br. 47) (citation omitted). *See, e.g.*, ER 55; Electronic Frontier Foundation, *Surveillance Self-Defense—Wi-Fi*, https://ssd.eff.org/tech/wifi (last visited April 20, 2012) ("Listening in on unencrypted Wi-Fi communications is *easy*: almost any computer can do it with simple

---

[9] *Compare* Wi-Fi Alliance, *Range*, http://www.wi-fi.org/knowledge-center/glossary/range (last visited April 20, 2012) ("Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to a mile."), *with In re Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006) (in some areas, cell towers may only cover "several hundred feet"). The range of Wi-Fi networks can also be extended using antennas and repeaters. Wi-Fi Alliance, *Wi-Fi Range and Environmental Issues*, http://www.wi-fi.org/files/kc_37_Wi-Fi%20Range%20and%20Environment%20Issues.pdf (last visited April 20, 2012).

packet-sniffing software. Special expertise or equipment isn't necessary.").[10]

In short, neither the distance a transmission travels nor the availability of technology that allows it to be intercepted is a plausible basis, as a matter of law or fact, to treat cellular telephone calls—but not Wi-Fi transmissions—as "radio communications." Plaintiffs' distinction fails, and with it so does their interpretation of the Wiretap Act.

2. Plaintiffs have no answer to the classification of pager transmissions as radio communications

Plaintiffs' arguments are further undone by their footnoted discussion of paging-system communications. Pl. Br. 48 n.23.

It is true, as Plaintiffs observe, that the Common-Carrier Exception designates "tone only paging system communications" as "readily accessible to the general public," while leaving other paging-system communications protected, insofar as they are transmitted by a common carrier. But Plaintiffs ignore the critical point, which is that under Section 2510(16), *all* radio transmissions made to electronic pagers qualify

---

[10] Of course, Wi-Fi users can protect themselves simply by encrypting their Wi-Fi transmissions. *See* FCC, *FCC Consumer Tip Sheet — Wi-Fi Networks and Consumer Privacy*, http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0417/DOC-313634A1.pdf (last visited April 20, 2012) ("encrypting information transmitted on your Wi-Fi network is as easy as activating the encryption feature on your wireless router").

as "radio communications." Google Br. 41. That is critical because paging-system communications clearly are not traditional radio broadcasts. Nor are they publicly directed. H.R. Rep. No. 99-647, at 23 ("Radio paging is essentially a one-way message service."). And Plaintiffs do not suggest that there is (or was) available equipment that allows such transmissions to be easily intercepted by the public. Paging transmissions are radio communications not based on the factors Plaintiffs say are relevant, but because—like cellular telephone calls and Wi-Fi transmissions—they are transmitted using radio waves. Plaintiffs have no answer to that.

III. GIVING "RADIO COMMUNICATION" ITS ORDINARY MEANING LEADS TO NO ABSURD RESULTS AND IS MANDATED BY THE RULE OF LENITY

A. No Absurd Results Flow from The Ordinary Meaning of "Radio Communication"

Google showed in its opening brief (at 54-58) that the "absurd results" that the district court feared would flow from a straightforward understanding of the Wiretap Act were not actual concerns. Plaintiffs offer no response. Instead, they suggest that treating Wi-Fi transmissions as radio communications under Section 2510(16) leads to a different set of supposed absurdities. Pl. Br. 33-36. Plaintiffs' claims are equally misplaced.

First, Plaintiffs say that Google's interpretation would mean that "the protection afforded a communication could change after it is sent, regardless of the protections implemented by the sender." Pl. Br. 33-34. That is not an absurdity; it is reality. The protections that attach to a given message are *always* subject to change based on the actions of the recipient after the message is sent. If Bob sends an email to Mary, and Mary reads it aloud, or forwards it to someone else, or leaves a printout of it in a public place, the protection afforded Bob's message would change—notwithstanding his intent that it be private. This is a fact of life, and not one that the Wiretap Act attempts to solve.

That is illustrated by the treatment of cordless telephones under the original version of ECPA. *See supra* pp. 18-20. In excluding the radio portion of a cordless telephone call from Wiretap Act protection, Congress understood that in some cases the same call would be simultaneously protected from interception and free to intercept, depending on whether the signal was passing through a wire (protected) or being transmitted by radio from the base unit to the handset (unprotected). H.R. Rep. No. 99-647, at 33; S. Rep. No. 99-541, at 8. Congress saw nothing problematic or absurd about that result—even though it meant that the protection available to one party's communication might vary

based on the technology that another party used to receive that communication.

Plaintiffs try to give their argument greater resonance by claiming that, under Google's approach, an email sent by an attorney would forfeit the attorney-client privilege if the client happened to be using an unencrypted Wi-Fi network. Plaintiffs cite nothing to support that bald assertion, and it does not reflect the law. *See, e.g.*, *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 564 (S.D.N.Y. 2008) (lawyers "may communicate confidential information through unencrypted e-mail" without forfeiting the privilege). The Wiretap Act is not the Model Rules of Professional Conduct. It does not follow that merely because a given mode of communication may not be protected from interception by the Wiretap Act, the attorney-client privileged is vitiated for any communication sent in that manner. Those are two separate inquires, and Plaintiffs offer no reason or authority for conflating them. Treating Wi-Fi transmissions as radio communications will not undermine attorney-client relationships.

Nor will doing so "substantially chill the use of Wi-Fi networks." Pl. Br. 34. Like all radio communications, Wi-Fi transmissions are protected from interception if they are encrypted. It is not the case, therefore, that Google's approach would "exclude Wi-Fi communications"

from Wiretap Act protection. *Id.* Only where the owner of a given network chooses to forego encryption do Wi-Fi transmissions become open for interception. If that leads some people to shift from unencrypted Wi-Fi networks to encrypted networks, that's hardly an alarming result or one that justifies distorting the statute to avoid.

Second, Plaintiffs claim that classifying Wi-Fi as a radio communication would mean that whether a given Wi-Fi transmission is "readily accessible" under Section 2510(16) would sometimes turn on arbitrary factors, such as whether the transmission is "carried on a subcarrier" (Section 2510(16)(C)) or transmitted on one of the specific frequencies covered by Section 2510(16)(E). Pl. Br. 35-36. This argument is based on a misunderstanding of Sections 2510(16)(C) and (E).

Section 2510(16)(C) applies to radio communications "carried on a subcarrier or other signal subsidiary to a radio transmission." The provision equates a "subcarrier" to a "signal subsidiary to a radio transmission," in keeping with the standard meaning of that term. *See, e.g.,* FCC, *Broadcast Radio Subcarriers or Subsidiary Communications Authority (SCA),* www.fcc.gov/encyclopedia/broadcast-radio-subcarriers-or-subsidiary-communications-authority-sca (last visited April 20, 2012). This exception, as its text makes clear and its legislative history confirms, applies only to signals (like subcarriers) that are transmitted

subsidiary to some other radio transmission. S. Rep. No. 99-541, at 15 (referring to "data and background music services carried on FM subcarriers"). Wi-Fi is not transmitted subsidiary to other radio transmissions; Wi-Fi is the radio transmission.[11]

Plaintiffs similarly misread Section 2510(16)(E). That exception protects communications "transmitted on frequencies allocated under" certain parts of various FCC Rules. It thus covers the "categories" of communications that were actually allocated under those Rules—not different types of communications that might use the same frequencies. H.R. Rep. No. 99-647, at 38.[12] The FCC has chosen to allocate spectrum for use by Wi-Fi networks under Part 15 of its Rules, not any of the three Parts specified in Section 2510(16)(E). 47 C.F.R. § 15.247; IEEE

---

[11] The lone authority that Plaintiffs cite for their position, *Ex Parte Janevski*, No. 2009-0671, 2009 WL 416502 (B.P.A.I. Feb. 18, 2009), does not address Wi-Fi and does not support Plaintiffs' argument about this exception. Yet, without any evidentiary basis, Plaintiffs characterize certain Wi-Fi protocols as dividing a Wi-Fi transmission into "several parallel data streams or channels and are transmitted by subcarriers." Pl. Br. 35 n.14. Even if that is an accurate description for certain Wi-Fi transmissions, those "parallel data streams" are the *main* Wi-Fi transmission, not subsidiary to some other radio transmission, and thus would not fall within the Section 2510(16)(C) exception.

[12] For example, when the 1991 congressional Task Force inquired whether the Wiretap Act protects "wireless local area networks," it concluded the answer would depend, not on the frequencies used by those networks, but "on where, within its regulatory structure, the FCC decides to allocate spectrum for these uses[.]" S. Hrg. 103-1022, at 183.

Standard 802.11 at 1141 tbl. I.1 (2007); EPIC *Amicus* Br. at 13, 15 (Docket No. 36). This exception is therefore categorically inapplicable to Wi-Fi transmissions, regardless of what frequencies any given Wi-Fi router happens to use.

Plaintiffs' misunderstanding of these exceptions means not only that the "absurd results" they conjure do not exist, but also that Plaintiffs could not plead—even if given the opportunity (*cf.* Pl. Br. 36 n.16)—that their Wi-Fi networks were protected from interception under Section 2510(16)(C) or (E).

B. Plaintiffs Cannot Evade The Rule of Lenity

Google agrees that the rule of lenity is not necessary to decide this appeal because the Wiretap Act is clear that (1) Wi-Fi transmissions are radio communications, and (2) a radio communication can lawfully be intercepted unless it falls within one of the 2510(16) exceptions (none of which applies here). But, as Google has explained, insofar as there is any ambiguity about that result, lenity provides an additional basis for reversing the decision below. Google Br. 42-45.

Plaintiffs' attempt to dismiss the significance of the rule of lenity (Pl. Br. 48-50) is undermined by this Court's en banc decision in *United States v. Nosal*, No. 10-10038, __ F.3d __, 2012 WL 1176119 (9th Cir. April 10, 2012). *Nosal* counsels against a reading of the Wiretap Act

like that proposed by Plaintiffs, under which the public would be left to guess, on pain of prosecution, whether the equipment they were using to receive radio signals was too "sophisticated," whether a transmission had covered a sufficiently long distance, or whether it was meant for a sufficiently large audience. Whereas Congress intended the line between protected and unprotected radio communications to be objective and clear, Plaintiffs' approach invites ambiguity and uncertainty. *See supra* pp. 23-24. As this Court has explained, however, the rule of lenity is meant to prevent criminal liability from turning on such ill-defined and unintended variables. *Nosal,* 2012 WL 1176119, at *7 (lenity ensures both "that citizens will have fair notice of the criminal laws" and that "Congress will have fair notice of what conduct its laws criminalize").

CONCLUSION

The district court's decision misconstrues the Wiretap Act and should be reversed.

Respectfully submitted,

DATED: April 20, 2012

/s/ *Michael H. Rubin*
David H. Kramer
Michael H. Rubin
Brian M. Willen
Caroline E. Wilson
WILSON SONSINI GOODRICH & ROSATI
PROFESSIONAL CORPORATION
650 Page Mill Road
Palo Alto, CA 94304
(650) 493-9300

Counsel for Appellant Google Inc.

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 6,920 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface 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 a proportionally spaced typeface using Microsoft Word in 14-point Century Schoolbook font.

DATED: April 20, 2012

/s/ *Michael H. Rubin*
David H. Kramer
Michael H. Rubin
Brian M. Willen
Caroline E. Wilson
WILSON SONSINI GOODRICH & ROSATI
PROFESSIONAL CORPORATION
650 Page Mill Road
Palo Alto, CA 94304
(650) 493-9300

Counsel for Appellant Google Inc.

TECHNICAL ADDENDUM

ADDENDUM OF TECHNICAL REFERENCES

TABLE OF CONTENTS

Tab

Search

Questions? Feedback? Contact us.

View a print-friendly version of this site.

Wi-Fi

Wireless networking is now a ubiquitous means of connecting computers to each other and to the Internet. The primary privacy concern with Wi-Fi is the interception of the communications you send over the air. In some cases, wireless routers might also store a small amount of information about your computer, such as its name and the unique number assigned to its networking card (MAC address).

Wireless networks are particularly vulnerable to eavesdropping — in the end, "wireless" just means "broadcasting your messages over the radio," and anyone can intercept your wireless signal unless you use encryption. Listening in on unencrypted Wi-Fi communications is *easy*: almost any computer can do it with simple packet-sniffing software. Special expertise or equipment isn't necessary.

Even worse, the legal protections for unencrypted wireless communications are unclear. Law enforcement may be able to argue that it does not need a wiretap order to intercept unencrypted wi-fi communications because there is an exception to the rules requiring such orders when the messages that are being intercepted are "readily accessible to the public." Basically, any communication over the radio spectrum that isn't transmitted by your phone company and isn't scrambled or encrypted poses a privacy risk.

Encrypting a Wireless Network

If you want to protect your wireless communications from the government or anyone else, you must use encryption! Almost all wireless Internet access points come with WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) encryption software installed to encrypt the messages between your computer and the access point, but you have to read the manual and figure out how to use it. WEP is not great encryption (and we recommend strong, end-to-end encryption for sensitive communications regardless of the transmission medium), and practiced hackers can defeat it very quickly, but it's worth the trouble to ensure that your communications will be entitled to the legal protections of the Wiretap Act. WPA is much stronger than WEP, but it still only covers the first step your packets will take across the Internet.

When Using Open Wi-Fi

If you're using someone else's "open" — unencrypted — wireless access point, like the one at the coffee shop, you will have to take care of your own encryption using the tools and methods described in other sections. Tor is especially useful for protecting your wireless transmissions. If you don't use Tor, and even if you do, you should also always use application-level encryption over open wireless, so no one can sniff your passwords.

Because of the threat of password sniffing, it is crucially important that you do not use the same password for all your accounts! For example, http://www.nytimes.com/ requires a username and password to log in, but the site does not use encryption. However, web sites for banks, like https://www.wellsfargo.com/, always use encryption due to the sensitive nature of the transactions people make with banks. If you use the same passwords for the two sites, an eavesdropper could see your unencrypted password traveling to the newspaper site, and guess that you were using the same password for your bank account.

‹ **Previous:** Instant Messaging (IM) **Next:** Tor›

Printer-friendly version Български

9th Circuit Case Number(s): 11-17483

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

****

CERTIFICATE OF SERVICE

I hereby certify that 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 on April 20, 2012.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

s/ Deborah Grubbs
Deborah Grubbs