FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BENJAMIN JOFFE; LILLA MARIGZA; RICK BENITTI; BERTHA DAVIS; JASON TAYLOR; ERIC MYHRE; JOHN E. REDSTONE; MATTHEW BERLAGE; PATRICK KEYES; KARL H. SCHULZ; JAMES FAIRBANKS; AARON LINSKY; DEAN M. BASTILLA; VICKI VAN VALIN; JEFFREY COLMAN; RUSSELL CARTER; STEPHANIE CARTER; JENNIFER LOCSIN, *Plaintiffs-Appellees*, v. GOOGLE, INC., *Defendant-Appellant*.	No. 11-17483 D.C. No. 5:10-md-02184-JW OPINION

Appeal from the United States District Court
for the Northern District of California
James Ware, District Judge, Presiding

Argued and Submitted
June 10, 2013—San Francisco, California

Filed September 10, 2013

Before: A. Wallace Tashima and Jay S. Bybee, Circuit Judges, and William H. Stafford, Senior District Judge.[*]

Opinion by Judge Bybee

SUMMARY[**]

Wiretap Act

The panel affirmed the district court's order denying a motion to dismiss claims that Google, Inc., violated the Wiretap Act when, in the course of capturing its Street View photographs, it collected data from unencrypted Wi-Fi networks.

The panel held that Google's data collection did not fall within a Wiretap exemption set forth in 18 U.S.C. § 2511(2)(g)(i) because data transmitted over a Wi-Fi network is not an "electronic communication" that is "readily accessible to the general public." Under 18 U.S.C. § 2510(16)(A), a "radio communication" is by definition "readily accessible to the general public" so long as it is not scrambled or encrypted. The panel held that the Wi-Fi network data collected by Google was not a radio communication, and thus was not by definition readily

[*] The Honorable William H. Stafford, Jr., Senior District Judge for the U.S. District Court for the Northern District of Florida, sitting by designation.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

accessible to the general public. The panel also held that data transmitted over a Wi-Fi network is not readily accessible to the general public under the ordinary meaning of the phrase as it is used in § 2511(2)(g)(i). Accordingly, the district court did not err in denying the motion to dismiss on the basis of the Wiretap Act exemption for electronic communication that is readily accessible to the general public.

COUNSEL

Michael H. Rubin (argued), David H. Kramer, Brian M. Willen, and Caroline E. Wilson, Wilson Sonsini Goodrich & Rosati Professional Corporation, Palo Alto, California, for Defendant-Appellant.

Elizabeth J. Cabraser (argued) and Jahan C. Sagafi, Lieff, Cabraser, Heimann & Bernstein, LLP, San Francisco, California; Kathryn E. Barnett, Lieff, Cabraser, Heimann & Bernstein, LLP, Nashville, Tennessee; Jeffrey L. Kodroff, John A. Macoretta, and Mary Ann Giorno, Spector Roseman Kodroff & Willis, P.C., Philadelphia, Pennsylvania; Daniel A. Small and David A. Young, Cohen Milstein Sellers & Toll, PLLC, Washington, D.C., for Plaintiffs-Appellees.

Marc Rotenberg, Alan Butler, and David Jacobs, Electronic Privacy Information Center, Washington, D.C., for Amicus Curiae Electronic Privacy Information Center.

OPINION

BYBEE, Circuit Judge:

In the course of capturing its Street View photographs, Google collected data from unencrypted Wi-Fi networks. Google publicly apologized, but plaintiffs brought suit under federal and state law, including the Wiretap Act, 18 U.S.C. § 2511. Google argues that its data collection did not violate the Act because data transmitted over a Wi-Fi network is an "electronic communication" that is "readily accessible to the general public" and exempt under the Act. 18 U.S.C. § 2511(2)(g)(i). The district court rejected Google's argument. *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d 1067, 1073–84 (N.D. Cal. 2011). We affirm.

I. BACKGROUND

A. *Facts and History*

Google launched its Street View feature in the United States in 2007 to complement its Google Maps service by providing users with panoramic, street-level photographs. Street View photographs are captured by cameras mounted on vehicles owned by Google that drive on public roads and photograph their surroundings. Between 2007 and 2010, Google also equipped its Street View cars with Wi-Fi antennas and software that collected data transmitted by Wi-Fi networks in nearby homes and businesses. The equipment attached to Google's Street View cars recorded basic information about these Wi-Fi networks, including the network's name (SSID), the unique number assigned to the router transmitting the wireless signal (MAC address), the signal strength, and whether the network was encrypted.

Gathering this basic data about the Wi-Fi networks used in homes and businesses enables companies such as Google to provide enhanced "location-based" services, such as those that allow mobile phone users to find nearby restaurants and attractions or receive driving directions.

But the antennas and software installed in Google's Street View cars collected more than just the basic identifying information transmitted by Wi-Fi networks. They also gathered and stored "payload data" that was sent and received over unencrypted Wi-Fi connections at the moment that a Street View car was driving by.[1] Payload data includes everything transmitted by a device connected to a Wi-Fi network, such as personal emails, usernames, passwords, videos, and documents.

Google acknowledged in May 2010 that its Street View vehicles had been collecting fragments of payload data from unencrypted Wi-Fi networks. The company publicly apologized, grounded its vehicles, and rendered inaccessible the personal data that had been acquired. In total, Google's Street View cars collected about 600 gigabytes of data transmitted over Wi-Fi networks in more than 30 countries.

Several putative class-action lawsuits were filed shortly after Google's announcement, and, in August 2010, the cases were transferred by the Judicial Panel on Multidistrict Litigation to the Northern District of California. In November, 2010, Plaintiffs-Appellees (collectively "Joffe") filed a consolidated complaint, asserting claims against

[1] Google may have also used its software to capture encrypted data, but the plaintiffs have conceded that their wireless networks were unencrypted.

Google under the federal Wiretap Act, 18 U.S.C. § 2511; California Business and Professional Code § 17200; and various state wiretap statutes. Joffe seeks to represent a class comprised of all persons whose electronic communications were intercepted by Google Street View vehicles since May 25, 2007.

Google moved to dismiss Joffe's consolidated complaint. The district court declined to grant Google's motion to dismiss Joffe's federal Wiretap Act claims.[2] *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d at 1084. On Google's request, the court certified its ruling for interlocutory appeal under 28 U.S.C. § 1292(b) because the district court resolved a novel question of statutory interpretation. We granted Google's petition, and we have jurisdiction under 28 U.S.C. § 1292(b).

B. *District Court's Decision*

Google maintained before the district court that it should have dismissed Joffe's Wiretap Act claims because data transmitted over unencrypted Wi-Fi networks falls under the statutory exemption that makes it lawful to intercept "electronic communications" that are "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). The question was whether payload data transmitted on an unencrypted Wi-Fi network is "readily accessible to the general public," such that the § 2511(2)(g)(i) exemption applies to Google's conduct.

[2] The district court granted Google's motion to dismiss Joffe's claims under California law and other state wiretap statutes. *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d at 1085–86. These claims are not at issue here.

To answer this question, the district court first looked to the definitions supplied by the Act. *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d at 1075–76. The statute provides in relevant part that "'readily accessible to the general public' means, with respect to a radio communication, that such communication is not . . . (A) scrambled or encrypted." 18 U.S.C. § 2510(16). An unencrypted *radio communication* is, therefore, "readily accessible to the general public." In short, intercepting an unencrypted *radio communication* does not give rise to liability under the Wiretap Act because of the combination of the § 2511(2)(g)(i) exemption and the § 2510(16) definition.

The district court then considered whether data transmitted over a Wi-Fi network is a "radio communication" because the phrase is not defined by the Act. *In re Google Inc. St. View Elec. Commc'n Litig.*, 794 F. Supp. 2d at 1076–81. The court reasoned that "radio communication" encompasses only "traditional radio services," and not other technologies that also transmit data using radio waves, such as cellular phones and Wi-Fi networks.[3] *Id.* at 1079–83. Since Wi-Fi networks are not a "radio communication," the definition of "readily accessible to the general public" provided by § 2510(16) does not apply because the definition is expressly limited to electronic communications that are radio communications.

Finally, the court addressed whether data transmitted over unencrypted Wi-Fi networks is nevertheless an "electronic communication" that is "readily accessible to the general

[3] It is less clear whether the district court's definition also excludes television broadcasts. Joffe argued at oral argument that television broadcasts are "traditional radio services."

public" under § 2511(2)(g)(i). *Id.* at 1082–84. Although the court determined that Wi-Fi networks do not involve a "radio communication" under § 2510(16) and are therefore not "readily accessible to the general public" by virtue of the definition of the phrase, it still had to resolve whether they are "readily accessible to the general public" as the phrase is ordinarily understood because the statute does not define the phrase as it applies to an "electronic communication" that is not a "radio communication." The court determined that data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public." *Id.* at 1082–83. As a result, the § 2511(2)(g)(i) exemption does not apply to Google's conduct. The court accordingly declined to grant Google's motion to dismiss Joffe's Wiretap Act claims. *Id.* at 1084.

II. OVERVIEW OF THE WIRETAP ACT

The Wiretap Act imposes liability on a person who "intentionally intercepts . . . any wire, oral, or electronic communication," 18 U.S.C. § 2511(1)(a), subject to a number of exemptions. *See* 18 U.S.C. § 2511(2)(a)–(h). There are two exemptions that are relevant to our purposes. First, the Wiretap Act exempts intercepting "an electronic communication made through an electronic communication system" if the system is configured so that it is "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). "Electronic communication" includes communication by radio, 18 U.S.C. § 2510(12), and "'readily accessible to the general public' means, with respect to a radio communication" that the communication is "not . . . scrambled or encrypted," 18 U.S.C. § 2510(16)(A). Second, the Act exempts intercepting "radio communication" by "any station for the use of the general public;" by certain

governmental communication systems "readily accessible to the general public," including police, fire, and civil defense agencies; by a station operating on an authorized frequency for "amateur, citizens band, or general mobile radio services;" or by a marine or aeronautical communications system. 18 U.S.C. § 2511(2)(g)(ii)(I)–(IV).

Google only argues, as it did before the district court, that it is exempt from liability under the Act because data transmitted over a Wi-Fi network is an "electronic communication . . . readily accessible to the general public" under § 2511(2)(g)(i). It concedes that it does not qualify for any of the exemptions for specific types of "radio communication" under § 2511(2)(g)(ii). Joffe, however, argues that if data transmitted over a Wi-Fi network is not exempt as a "radio communication" under § 2511(2)(g)(ii), it cannot be exempt as a radio communication under the broader exemption for "electronic communication" in § 2511(2)(g)(i). This argument has some force, and we wish to address it before we consider Google's claims.

Joffe contends that the definition of "readily accessible to the general public" in § 2510(16) does not apply to the § 2511(2)(g)(i) exemption. Instead, Joffe argues, the § 2510(16) definition applies exclusively to § 2511(2)(g)(ii)(II), which exempts specifically enumerated types of "radio communication" when they are "readily accessible to the general public." We ultimately reject Joffe's alternative reading of the statute, although—as we will explain—we find § 2511(2)(g)(ii) useful as a lexigraphical aid to understanding the phrase "radio communication."

As noted, § 2510(16) defines "readily accessible to the general public" solely with respect to a "radio

communication," and not with respect to other types of "electronic communication." Although § 2511(2)(g)(i) does not use the words "radio communication," the statute nevertheless directs us to apply the § 2510(16) definition to the § 2511(2)(g)(i) exemption. First, "radio communication" is a subset of "electronic communication." *See* 18 U.S.C. § 2510(12) (providing that, subject to certain exceptions, "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, *radio*, electromagnetic, photoelectronic or photooptical system") (emphasis added). Second, the statute directs us to apply § 2510(16) to the entire chapter. The definitions in 18 U.S.C. § 2510 are prefaced with the phrase, "As used in this chapter." We cannot disregard this command by holding that the definition of "'readily accessible to the general public' [ ] with respect to a radio communication" applies to § 2511(2)(g)(ii), but not § 2511(2)(g)(i).

Admittedly, following the plain language of the statute creates some tension with § 2511(2)(g)(ii)(II), which provides an exemption for intercepting "any radio communication which is transmitted . . . by any governmental, law enforcement, civil defense, private land mobile, or public communications system, including police and fire, readily accessible to the general public." Under our reading of the statute—which is the same reading adopted by the district court, Google, and Joffe in his lead argument—§ 2511(2)(g)(i) exempts all electronic communications (including radio communications) that are "readily accessible to the general public" as the phrase is defined in § 2510(16). This reading likely renders § 2511(2)(g)(ii)(II) superfluous. As discussed, that section exempts specific kinds of radio communications that are "readily accessible to the general

public," such as those transmitted by a law enforcement communications system. But this exemption is unnecessary when § 2511(2)(g)(i) already exempts all radio communications that are "readily accessible to the general public."

Although our reading may render § 2511(2)(g)(ii)(II) superfluous or at least redundant, we understand that Congress "sometimes drafts provisions that appear duplicative of others—simply in Macbeth's words, 'to make assurance double sure.' That is, Congress means to clarify what might be doubtful—that the mentioned item is covered." *Shook v. D.C. Fin. Responsibility & Mgmt. Assistance Auth.*, 132 F.3d 775, 782 (D.C. Cir. 1998). This interpretation is especially plausible given that Congress was concerned that radio hobbyists not face liability for intercepting readily accessible broadcasts, such as those covered by § 2511(2)(g)(ii)(II), which can be picked up by a police scanner. *See* 132 Cong. Rec. S7987-04 (1986) ("In order to address radio hobbyists' concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful.").

In short, we agree with Google that the definition of "readily accessible to the general public" in § 2510(16) applies to the § 2511(2)(g)(i) exemption when the communication in question is a "radio communication." With that understanding, we now turn to whether data transmitted over a Wi-Fi network is a "radio communication" exempt from the Wiretap Act as an "electronic communication" under § 2511(2)(g)(i).

III. ANALYSIS

In support of its position that it is exempt under § 2511(2)(g)(i), Google offers two arguments. First, it contends that data transmitted over a Wi-Fi network is an electronic "radio communication" and that the Act exempts such communications by defining them as "readily accessible to the general public," 18 U.S.C. § 2511(2)(g)(i), so long as "such communication is not . . . scrambled or encrypted," 18 U.S.C. § 2510(16)(A). Second, Google contends that even if data transmitted over an unencrypted Wi-Fi network is not a "radio communication," it is still an "electronic communication . . . readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i).

We reject both claims.[4] We hold that the phrase "radio communication" in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi-Fi network. As a consequence, the definition of "readily accessible to the general public [ ] with respect to a radio communication" set forth in § 2510(16) does not apply to the exemption for an "electronic communication" that is "readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i). We further hold that

[4] This case raises a question of statutory interpretation, which we review de novo. *Phoenix Mem'l Hosp. v. Sebelius*, 622 F.3d 1219, 1224 (9th Cir. 2010). We begin by "determin[ing] whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case." *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 450 (2002). We must assume that "the ordinary meaning of that language accurately expresses the legislative purpose [of Congress]." *Park 'N Fly, Inc. v. Dollar Park & Fly, Inc.*, 469 U.S. 189, 194 (1985).

payload data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public" under the ordinary meaning of the phrase as it is used in § 2511(2)(g)(i).

A. *Data Transmitted over a Wi-Fi Network Is Not a "Radio Communication" under the Wiretap Act.*

We turn first to the question of whether data transmitted over a Wi-Fi network is a "radio communication" as that term is used in 18 U.S.C. § 2510(16). If data transmitted over a Wi-Fi network is a radio communication, then any radio communication that is not scrambled or encrypted is considered "readily accessible to the general public," and is exempt from liability under the Wiretap Act. 18 U.S.C. § 2511(2)(g)(i).

1. The ordinary meaning of "radio communication" does not include data transmitted over a Wi-Fi network

The Wiretap Act does not define the phrase "radio communication" so we must give the term its ordinary meaning. *See Hamilton v. Lanning*, 130 S. Ct. 2464, 2471 (2010) ("When terms used in a statute are undefined, we give them their ordinary meaning."); *United States v. Daas*, 198 F.3d 1167, 1174 (9th Cir. 1999) ("If the statute uses a term which it does not define, the court gives that term its ordinary meaning.").

According to Google, radio communication "refers to any information transmitted using radio waves, *i.e.*, the radio frequency portion of the electromagnetic spectrum." Appellant's Br. at 28. The radio frequency portion of the spectrum is "the part of the spectrum where electromagnetic

waves have frequencies in the range of about 3 kilohertz to 300 gigahertz." *Id.* at 27.

Google's technical definition does not conform with the common understanding held contemporaneous with the enacting Congress. *See United States v. Iverson*, 162 F.3d 1015, 1022 (9th Cir. 1998) ("When a statute does not define a term, we generally interpret that term by employing the *ordinary*, *contemporary*, and *common* meaning of the words that Congress used") (emphasis added). The radio frequency portion of the electromagnetic spectrum covers not only Wi-Fi transmissions, but also television broadcasts, Bluetooth devices, cordless and cellular phones, garage door openers, avalanche beacons, and wildlife tracking collars. *See* Fed. Commc'n Comm'n, *Encyclopedia – FM Broadcast Station Classes and Service Countours*, *available at* http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf (last visited Aug. 13, 2013). One would not ordinarily consider, say, television a form of "radio communication." Not surprisingly, Congress has not typically assumed that the term "radio" encompasses the term "television." *See, e.g.*, 18 U.S.C. § 1343 (imposing liability for "[f]raud by wire, radio, *or* television") (emphasis added); 18 U.S.C. § 2101 (imposing liability for inciting a riot by means of "mail, telegraph, radio, *or* television") (emphasis added); 7 U.S.C. § 2156 (defining an "instrumentality of interstate commerce" as "any written, wire, radio, television or other form of communication); *see also FCC v. Nat'l Citizens Comm. for Broad.*, 436 U.S. 775, 815 (1978) (noting that "radio and television stations are given different weight," under the regulations at issue, and describing regulations governing "a radio *or* television broadcast station") (emphasis added).

The Wiretap Act itself does not assume that the phrase "radio communication" encompasses technologies like satellite television that are outside the scope of the phrase as it is ordinarily defined. For example, the statute's damages provision sets out specified penalties when the "violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted *or* if the communication is a radio communication that is transmitted on [frequencies specified by regulation]." 18 U.S.C. § 2520(c)(1) (emphasis added). Congress described separately the act of "viewing [ ] a private satellite video communication" even though such communication is transmitted on a radio frequency and would fall within Google's proposed definition of "radio communication." Taken together, these disparate provisions offer evidence that Congress does not use "radio" or "radio communication" to reference all of the myriad forms of communication that use the radio spectrum. Rather, it uses "radio" to refer to traditional radio technologies, and then separately describes other modes of communication that are not ordinarily thought of as radio, but that nevertheless use the radio spectrum.

Google's proposed definition is in tension with how Congress—and virtually everyone else—uses the phrase. In common parlance, watching a television show does not entail "radio communication." Nor does sending an email or viewing a bank statement while connected to a Wi-Fi network. There is no indication that the Wiretap Act carries a buried implication that the phrase ought to be given a broader definition than the one that is commonly understood. *See Mohamad v. Palestinian Auth.*, 132 S. Ct. 1702, 1707 (2012) (favoring a definition that matches "how we use the word in everyday parlance" and observing that "Congress remains free, as always, to give the word a broader or

different meaning. But before we will assume it has done so, there must be *some* indication Congress intended such a result").

Importantly, Congress provided definitions for many other similar terms in the Wiretap Act, but refrained from providing a technical definition of "radio communication" that would have altered the notion that it should carry its common, ordinary meaning. *See, e.g.*, 18 U.S.C. § 2510(1) (defining "wire communication"); 18 U.S.C. § 2510(12) (defining "electronic communication"); 18 U.S.C. § 2510(15) (defining "electronic communication service"); 18 U.S.C. § 2510(17) (defining "electronic storage"). As Google writes in its brief, "[t]he fact that the Wiretap Act provides specialized definitions for certain compound terms—but not for 'radio communication'—is powerful evidence that the undefined term was not similarly intended [to] be defined in a specialized or narrow way" but rather "according to its ordinary meaning." Appellant's Br. at 29. We agree and, accordingly, we reject Google's proposed definition of "radio communication" in favor of one that better reflects the phrase's ordinary meaning.

2. A "radio communication" is a predominantly auditory broadcast, which excludes payload data transmitted over Wi-Fi networks

There are two telltale indicia of a "radio communication." A radio communication is commonly understood to be (1) predominantly auditory, and (2) broadcast. Therefore, television—whether connected via an indoor antenna or a satellite dish—is not radio, by virtue of its visual component. A land line phone does not broadcast, and, for that reason, is not radio. On the other hand, AM/FM, Citizens Band (CB),

'walkie-talkie,' and shortwave transmissions are predominantly auditory, are broadcast, and are, not coincidentally, typically referred to as "radio" in everyday parlance. Thus, we conclude that "radio communication" should carry its ordinary meaning: a predominantly auditory broadcast.[5]

The payload data transmitted over unencrypted Wi-Fi networks that was captured by Google included emails, usernames, passwords, images, and documents that cannot be classified as predominantly auditory. They therefore fall outside of the definition of a "radio communication" as the phrase is used in 18 U.S.C. § 2510(16).

---

[5] We need not reach the question of what exactly constitutes a "broadcast" because the Wi-Fi transmissions in question were not predominantly auditory. Whether cell phone calls—which are projected wirelessly over great distances—are broadcast would similarly be a close question.

We also need not fully consider the extent to which non-auditory transmissions may be included in a broadcast before that broadcast is no longer a radio broadcast. Modern FM radio stations, for example, commonly transmit small amounts of data denoting the artist and title of the song. But because such data is ancillary to the audio transmission, they likely do not remove the transmissions from the domain of a "radio communication" under the Act.

And, finally, we do not address how to classify a traditional radio broadcast delivered to a web-enabled device connected to a Wi-Fi network, such as a radio station streamed over the internet. Here, Google's collection efforts were not limited to auditory transmissions.

3. Defining "radio communication" to include only predominantly auditory broadcasts is consistent with the rest of the Wiretap Act

Crucially, defining "radio communication" as a predominantly auditory broadcast yields a coherent and consistent Wiretap Act. Google's overly broad definition does not. *See 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.")

Throughout the Wiretap Act, Congress used the phrase "radio communication"—which is at issue here—and the similar phrase "communication by radio." Even within the very provision that we are construing—18 U.S.C. § 2510(16)—Congress used both phrases. We must ascribe to each phrase its own meaning. *See SEC v. McCarthy*, 322 F.3d 650, 656 (9th Cir. 2003) ("It is a well-established canon of statutory interpretation that the use of different words or terms within a statute demonstrates that Congress intended to convey a different meaning for those words."). The phrase "communication by radio" is used more expansively: it conjures an image of all communications using radio *waves* or a radio *device*. *See, e.g.*, 18 U.S.C. § 2510(16)(E) (describing radio communication that "is a two-way voice communication by radio transmitted on a frequency "not exclusively allocated to broadcast auxiliary services.").

When read in context, the phrase "radio communication" tends to refer more narrowly to broadcast radio technologies rather than to the radio waves by which the communication

is made. "Radio communication" is typically surrounded by words that evoke traditional radio technologies whenever it is used in the Act. *See Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995) (""[A] word is known by the company it keeps (the doctrine of *noscitur a sociis*). This rule we rely upon to avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving 'unintended breadth to the Acts of Congress.'"). For example, 18 U.S.C. § 2511(2)(g)(ii), *inter alia*, exempts from liability the interception of "any radio communication which is transmitted . . . by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services." These are traditional audio broadcasts that fit squarely within the ordinary meaning of "radio communication." The phrase "radio communication" is used five times in the Wiretap Act. *See* 18 U.S.C. § 2510(16), 18 U.S.C. § 2511(2)(g)(ii), 18 U.S.C. § 2511(2)(g)(v), 18 U.S.C. § 2511(5)(a)(i)(B), 18 U.S.C § 2520(c)(1). Defining the term as a predominantly auditory broadcast would not distort the meaning of any of these provisions or otherwise lead to incoherence or inconsistency.

On the other hand, the Wiretap Act uses "communication by radio" to refer more broadly to any communication transmitted by radio wave. *See* 18 U.S.C. § 2510(12) (defining "electronic communication" to include any communication "transmitted in whole or in part by . . . radio"); 18 U.S.C. § 2511(1)(b)(ii) (prohibiting the use of a "device to intercept any oral communication" if the "device transmits communications by radio"); 18 U.S.C. § 2511(2)(b) (authorizing FCC employees, in carrying out their official duties, "to intercept . . . [an] oral communication transmitted by radio"). Congress's decision to use both of these phrases implies that it intended to distinguish "radio communication"

from "communications by radio." *See McCarthy*, 322 F.3d at 656. Ideally, Congress would have supplied definitions to make the distinction between these terms more apparent. Nevertheless, by relying on their ordinary meaning and evaluating how they are used in context, we conclude that the former refers more narrowly to a predominantly auditory broadcast while only the latter encompasses other communications made using radio waves.

The way the phrase "radio communication" is used in 18 U.S.C. § 2511(2)(g)(ii) is particularly relevant in defining the term because that provision specifically exempts from liability the interception of certain kinds of radio communication. The provision is not directly at issue here because—as Google acknowledges—Google's conduct is not encompassed by any of the § 2511(2)(g)(ii) exemptions, hence its reliance on § 2511(2)(g)(i). But it is instructive to understand the types of communication exempted by § 2511(2)(g)(ii) since the phrase "radio communication" is "known by the company it keeps," *Gustafson*, 513 U.S. at 575. The exemptions include, *inter alia*, radio communications transmitted "by any station for the use of the general public," 18 U.S.C. § 2511(2)(g)(ii)(I), "by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services," 18 U.S.C. § 2511(2)(g)(ii)(III), and "by any marine or aeronautical communications system," 18 U.S.C. § 2511(2)(g)(ii)(IV). Other than the fact that they all use the radio spectrum, these radio communications have little in common with a home Wi-Fi network. Of course § 2511(2)(g)(i) exempts radio communications that are "readily accessible to the general public" even if they are not specifically set out in § 2511(2)(g)(ii). But it would be odd for Congress to take pains to identify particular kinds of radio

communications that should be exempt in § 2511(2)(g)(ii) only to exempt broad swaths of dissimilar communications, such as data transmitted over a Wi-Fi network, under the auspices of § 2511(2)(g)(i). It is more sensible to read the general exemption in § 2511(2)(g)(i)—insofar as it applies to "radio communication" rather than other kinds of "electronic communication"—in light of the specific exemptions in § 2511(2)(g)(ii).

Relatedly, giving "radio communication" its ordinary meaning as a predominantly auditory broadcast also avoids producing absurd results that are inconsistent with the statutory scheme. *See Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982) ("[I]nterpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available."); *Ariz. State Bd. for Charter Schools v. U.S. Dep't of Educ.*, 464 F.3d 1003, 1008 (9th Cir. 2006) ("[W]ell-accepted rules of statutory construction caution us that 'statutory interpretations which would produce absurd results are to be avoided.' When a natural reading of the statutes leads to a rational, common-sense result, an alteration of meaning is not only unnecessary, but also extrajudicial."). Under the expansive definition of "radio communication" proposed by Google, the protections afforded by the Wiretap Act to many online communications would turn on whether the *recipient* of those communications decided to secure her wireless network. A "radio communication" is "readily accessible to the general public" and, therefore, exempt from Wiretap Act liability if it is not scrambled or encrypted. 18 U.S.C. § 2510(16). Consider an email attachment containing sensitive personal information sent from a secure Wi-Fi network to a doctor, lawyer, accountant, priest, or spouse. A company like Google that intercepts the contents

of that email from the encrypted home network has, quite understandably, violated the Wiretap Act. But the sender of the email is in no position to ensure that the recipient—be it a doctor, lawyer, accountant, priest, or spouse—has taken care to encrypt her own Wi-Fi network. Google, or anyone else, could park outside of the recipient's home or office with a packet sniffer while she downloaded the attachment and intercept its contents because the sender's "radio communication" is "readily accessible to the general public" solely by virtue of the fact that the *recipient's* Wi-Fi network is not encrypted. Surely Congress did not intend to condone such an intrusive and unwarranted invasion of privacy when it enacted the Wiretap Act "to protect against the unauthorized interception of electronic communications." S. Rep. No. 99-541 (1986), at 1; *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) ("The legislative history of the [Wiretap Act] suggests that Congress wanted to protect electronic communications that are configured to be private, such as email."); *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.").

The definition of "readily accessible to the general public" in § 2510(16) is limited to "radio communication," and does not encompass all "electronic communication." Congress's decision to carve out "radio communication" for less protection than some other types of "electronic communication" makes sense if "radio communication" is given its ordinary meaning. Traditional radio services can be easily and mistakenly intercepted by hobbyists. *See* 132 Cong. Rec. S7987-04 (1986) ("In order to address radio hobbyists' concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services

is not unlawful."). But "radio hobbyists" do not mistakenly use packet sniffers to intercept payload data transmitted on Wi-Fi networks. Lending "radio communication" a broad definition that encompasses data transmitted on Wi-Fi networks would obliterate Congress's compromise and create absurd applications of the exemption for intercepting unencrypted radio communications. For example, § 2511(2)(g)(ii)(II) exempts from liability, *inter alia*, the act of intercepting "any radio communication which is transmitted . . . by any governmental, law enforcement . . . or public safety communications system, including police and fire, readily accessible to the general public." This provision reinforces the work performed by § 2511(2)(g)(i), which already exempts a "radio communication" that is "readily accessible to the general public." Congress's decision to ensure that these communications were exempt makes sense if "radio communication" encompasses only predominantly auditory broadcasts since these transmissions can be picked up by widely available police scanners. But if "radio communication" includes data transmitted over Wi-Fi networks, then § 2511(2)(g)(ii)(II) also underscores that liability should not attach to intercepting data from an unencrypted Wi-Fi network operated by, say, a police department or government agency. It seems doubtful that Congress wanted to emphasize that Google or anyone else could park outside of a police station that carelessly failed to secure its Wi-Fi network and intercept confidential data with impunity.

Next, Google strenuously argues that the rest of the Wiretap Act supports its position that "radio communication" in 18 U.S.C. § 2510(16) means "any information transmitted using radio waves." Google leans heavily on § 2510(16)(D) and the accompanying legislative history, which together

suggest that cellular telephone and paging systems are a form of "radio communication." If cell phone and paging systems are a type of "radio communication," Google argues, it must be the case that Congress intended that the phrase include Wi-Fi networks and the rest of the radio spectrum because these technologies differ from paradigmatic radio communications like AM/FM, CB, and shortwave transmissions. But cell phone communications were not dissimilar from CB, shortwave, or other two-way forms of traditional radio broadcasts when § 2510(16)(D) was added to the Wiretap Act in 1986 as part of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848. When Congress enacted § 2510(16)(D), cell phones were still called "cellular radiotelephones." *See* H.R. Rep. No. 99-647, at 20 (1986). As with other audio broadcasts, cellular conversations were often inadvertently picked up by radio hobbyists "scanning radio frequencies in order to receive public communications." S. Rep. No. 99-541, at 3560 (1986); *see also* H.R. Rep. No. 99-647, at 20 ("Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls"). The fact that technology has evolved and cellular communications are no longer as similar to CB broadcasts as they once were does not require us to read "radio communication" to include all communications made using radio waves. Rather, the historical context surrounding Congress's protection of cellular conversations as a form of a "radio communication" is consistent with the commonsense definition of the term because, at the time of the enactment of the definition in 1986, cellular conversations could have reasonably been construed as analogous to a form of two-way

radio.[6] Assuming, *arguendo*, that the phrase "radio communication" covers cell phone transmissions as they existed in 1986 does not inevitably lead to the conclusion that it also encompasses transmissions that are plainly not predominantly auditory broadcasts, such as payload data transmitted over a Wi-Fi network.

Google also looks beyond the Wiretap Act in an effort to fit its expansive definition of "radio communication" into the statutory scheme. It points out that the Communications Act expressly defines the phrases "radio communication" and "communication by radio" broadly to include "the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds." 47 U.S.C. § 153(40). But when Congress wanted to borrow a definition from the Communications Act to apply to the Wiretap Act, it expressly said so. *See* 18 U.S.C. § 2510(1) (giving the phrase "communication common carrier" the meaning that it has "in section 3 of the Communications Act"). Here, Congress refrained from incorporating the definition of "radio

[6] With modern advances in cellular technology, it is less clear how cell phones would fit within the statutory scheme today. We need not resolve this question here. Whether cell phone transmissions are an example of a "radio communication" is relevant to defining the phrase, but it is not a precursor to observing that a "radio communication" is ordinarily a predominantly auditory broadcast or to holding that payload data transmitted over a Wi-Fi network is not a "radio communication." We previously held that cell phone communications are "wire communications" for purposes of the Wiretap Act, but we did not address whether they are an example of a "radio communication." *See In re U.S. for an Order Authorizing Roving Interception of Oral Commc'ns*, 349 F.3d 1132, 1138 n.12 (9th Cir. 2003) ("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.").

communication" used in the Communications Act. And, as previously discussed, the Wiretap Act uses the phrases "radio communication" and "communication by radio" differently, indicating that Congress did not intend to import the Communications Act's definition, which treats them as synonyms. *See* 47 U.S.C. § 153(40). Furthermore, the Communication Act's definition of "radio communication" encompasses technologies like television by including "the transmission by radio of . . . pictures . . . of all kinds," 47 U.S.C. § 153(40), while the Wiretap Act sometimes distinguishes them. *See, e.g.*, 18 U.S.C. § 2520(c)(1) (providing specified penalties when the "violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on [frequencies specified by regulation]"). Separate references to television-related communications would be redundant when paired with the phrase "radio communication" if we were to assume that the Communication Act's definition applied to the Wiretap Act. Importantly, the presumption that a definition set out in one part of the code is intended to govern another is hardly unyielding in the face of such contradictory evidence. *See, e.g.*, *General Dynamics Land Sys., Inc. v. Cline*, 540 U.S. 581, 595 (2004) (holding that the word "age" carries a different meaning in different sections of the ADEA); *Robinson v. Shell Oil*, 519 U.S. 337, 343 (1997) (holding that the term "employees" carries a different meaning in different sections of Title VII).

Google also leans heavily on a series of amendments to 18 U.S.C. § 2510(16) to argue that Congress impliedly gave the phrase "radio communication" a meaning other than the ordinary one that we adopt here. In 1990, Senator Patrick

Leahy commissioned a task force to study the effect of new technologies, including the precursors to wireless networking, on the statutory scheme created in 1986 by the Electronic Communications Privacy Act. *See* S. Hrg. 103-1022, at 179 (1994). In its report, the task force indicated it was concerned that communications by "'wireless modems' which can transmit data between computers . . . will not be protected unless the user goes to the expense of full data encryption." *Id.* at 183. The section of the report on "Wireless Data Communications" concluded that "[t]he task force recommends appropriate amendments to legally protect digital communications of this type from unauthorized interception." *Id*. In short, the task force was of the opinion that the version of 18 U.S.C. § 2510(16) enacted in 1986 did not adequately protect unencrypted "wireless data communications." The task force must have implicitly decided that "wireless data communications" were a "radio communication" because otherwise it would not have been concerned with § 2510(16), which only applies to "radio communication." *See id*.

In 1994, Congress amended § 2510(16) to add a new category of communication—which it called an "electronic communication"—that it deemed to be a "radio communication" that was not "readily accessible to the general public." In relevant part, the statute provided that "'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). Google claims that Congress added § 2510(16)(F) in 1994 in order to protect from interception new technologies that transmitted data using radio frequencies, including the contemporary versions of wireless networks. There is some support for this proposition in the congressional record. *See*

H.R. Rep. No. 103-827, at 18 (1994) (explaining that the bill "[e]xtends privacy protections of the Electronic Communications Privacy Act to cordless phones and certain data communications transmitted by radio").

The significance of all of this is that Congress repealed 18 U.S.C. § 2510(16)(F) in 1996. Google attempts to draw a series of inferences from the 1994 and 1996 amendments: The 1994 Congress thought that data transmissions across the wireless networks of the day were a type of "radio communication." Otherwise, Congress would not have needed to amend § 2510(16) in order to shield them from interception given that the provision only applies to "radio communication." By deleting § 2510(16)(F), the 1996 Congress removed the sole protection for unencrypted data transmissions over wireless networks by returning § 2510(16) to its pre-amendment form. From Google's perspective, the upshot of this historical narrative is that payload data transmitted over an unencrypted Wi-Fi network is a "radio communication" that is "readily accessible to the general public" before the 1994 amendment and, crucially, after the 1996 repeal.

This evidence of congressional action and inaction is far more equivocal than Google acknowledges. First, the task force's report does not control what the phrase "radio communication" meant to Congress when it enacted § 2510(16) in 1986. The task force's report suggests that it thought that the "wireless data communication" technology that existed in 1991 entailed "radio communication" as the phrase is used in § 2510(16). But the task force's opinion on questions of statutory interpretation has no independent authority; it is not charged with divining congressional intent. The task force's recommendation informs us that in 1991 a

group of fifteen individuals thought that early versions of wireless networks involved "radio communication" under the statute. Their opinion is not indicative of what Congress intended when it included the phrase in the Wiretap Act. It may be considered evidence of the phrase's ordinary meaning. But it does not outweigh the more substantial evidence, discussed at length above, indicating that the ordinary meaning of "radio communication" excludes data transmitted over a Wi-Fi network.

Second, Congress's decision to add § 2510(16)(F) in 1994 does not prove that it thought data transmitted over a Wi-Fi network constituted a "radio communication." The 1994 Congress was certainly concerned about ensuring that "certain data communications transmitted by radio" were protected from interception. But that does not necessarily mean that it was of the view that such communications were a "radio communication" under § 2510(16). Congress might have been forestalling the possibility that evolving technologies would be construed as radio communications, contrary to the ordinary meaning of the phrase.

Third, and perhaps most importantly, there is no reliable indication of what the 1996 Congress intended to accomplish by repealing § 2510(16)(F). Google mines the 1991 task force report and the 1994 congressional record, but it cannot close the loop on its argument because the 1996 Congress did not leave behind the snippets of enactment history that are essential to Google's narrative. Consider two possible rationales for the 1996 repeal of § 2510(16)(F): first, Congress might have deleted the provision because it found it redundant. That is, Congress might have thought that data transmitted over a radio frequency was not a "radio communication," which would render the additional

protection for such communications offered by § 2510(16)(F) unnecessary.

Alternatively, Congress might have (correctly) determined that § 2510(16)(F) made the statute incoherent. Recall that the short-lived provision provided that "'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)(F) (1994). The phrase "electronic communication" has been broadly defined since the Electronic Communications Privacy Act of 1986. In 1994, when § 2510(16)(F) was added, the Wiretap Act provided—as it still does today—that "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce." 18 U.S.C. § 2510(12). As Google stresses in its briefs, and the statute plainly states, "radio communication" is a subset of "electronic communication." Yet § 2510(16)(F) conveyed that a "radio communication" was not "readily accessible to the general public" if it was an "electronic communication," which incoherently implies that the latter was a subset of the former. The repeal of § 2510(16)(F) could, therefore, have been a housekeeping matter designed to resolve this internal tension without affecting the protection afforded "electronic communications, including data" that the 1994 Congress sought to protect.

Neither of these entirely plausible explanations for the amendment and repeal are consistent with Google's assumption that the pre-1994 conception of "radio communication" included data transmitted over a Wi-Fi

network and the 1996 repeal of § 2510(16)(F) sought to restore that conception. The point is that we do not know why the 1996 Congress deleted § 2510(16)(F). We choose to rely on the ordinary meaning of the phrase "radio communication" rather than follow a trail of enactment history that culminates in silence and then speculate as to Congress's unexpressed intent.

Finally, Google's fall back position is that the rule of lenity dictates that we accept its proposed definition of "radio communication." Although this is a civil suit, the Wiretap Act also carries criminal penalties so Google's reliance on the rule of lenity is not unfounded. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) ("Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."). But we do not resort to the rule of lenity every time a difficult question of statutory interpretation arises. 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.'" *Barber v. Thomas*, 130 S. Ct. 2499, 2508 (2010) (citations omitted); *see also Smith v. United States*, 508 U.S. 223, 239 (1993) ("The mere possibility of articulating a narrower construction [ ] does not make the rule of lenity applicable. Instead, that venerable rule is reserved for cases where, '[a]fter "seizing every thing from which aid can be derived,"' the Court is 'left with an ambiguous statute.'") (citations omitted). Here, the traditional tools of statutory interpretation are sufficient. The ordinary meaning of "radio communication" is consistent with the structure of the Act and avoids absurd results without running afoul of any clearly expressed congressional intent. We need not resort to the rule of lenity where, as here, the ambiguity can be fairly resolved.

B. *Wi-Fi Transmissions Are Not "Readily Accessible to the General Public" under 18 U.S.C. § 2511(2)(g)(i)*

In the previous section, we concluded that payload data transmitted over a Wi-Fi network is not a "radio communication" under 18 U.S.C. § 2510(16). As a result, the definition of "readily accessible to the general public" in § 2510(16) does not apply to the exemption for intercepting an "electronic communication" that is "readily accessible to the general public" in § 2511(2)(g)(i). But that does not end the inquiry. Although payload data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public" *by definition* solely because it is an unencrypted "radio communication," it is still possible for a transmission that falls outside of the purview of the § 2510(16) definition to be considered "readily accessible to the general public" under the ordinary meaning of that phrase.[7] We now hold, in agreement with the district court, that payload data transmitted over an unencrypted Wi-Fi network is not "readily accessible to the general public" and,

[7] The phrase "readily accessible to the general public" is only defined insofar as the communication at issue is a "radio communication." *See* 18 U.S.C. § 2510(16) ("'readily accessible to the general public' means, with respect to a radio communication . . ."). The phrase is undefined where, as here, the transmission is an "electronic communication" that is not a "radio communication." Since the term at issue is undefined, we look to its ordinary meaning. *See Hamilton*, 130 S. Ct. at 2471 ("When terms used in a statute are undefined, we give them their ordinary meaning."). Joffe does not dispute that payload data transmitted over a Wi-Fi network is an "electronic communication," which the Act defines as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce" subject to specific exceptions that do not apply here. 18 U.S.C. § 2510(12).

consequently, that Google cannot avail itself of the § 2511(2)(g)(i) exemption.

First, Wi-Fi transmissions are not "readily" available because they are geographically limited and fail to travel far beyond the walls of the home or office where the access point is located. Google was only able to intercept the plaintiffs' communications because its Street View vehicles passed by the street outside of each plaintiff's house. The FCC generally limits the peak output of Wi-Fi broadcasts to 1 watt. *See* 47 C.F.R. § 15.247(b). Meanwhile, AM, FM, and other traditional radio broadcasts typically range from 250 to 100,000 watts. *See* Fed. Commc'n Comm'n, *Encyclopedia – FM Broadcast Station Classes and Service Countours*, *available at* http://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf (last visited Aug. 13, 2013); *see also* Fed. Commc'n Comm'n, *Encyclopedia – AM Broadcast Station Classes; Clear, Regional, and Local*, *available at* http://www.fcc.gov/encyclopedia/am-broadcast-station-classes-clear-regional-and-local-channels (last visited Aug. 13, 2013). As a result, AM radio stations have a service range of up to 100 miles, while individual Wi-Fi access points usually have a range of less than 330 feet. *See* Fed. Commc'n Comm'n, *Encyclopedia – Why AM Radio Stations Must Reduce Power, Change Operations, or Cease Broadcasting at Night*, http://www.fcc.gov/encyclopedia/why-am-radio-stations-must-reduce-power-change-operations-or-cease-broadcasting-night (last visited Aug. 13, 2013); Encyclopedia Brittanica Online, *Wi-Fi*, http://www.britannica.com/ EBchecked/topic/1473553/Wi-Fi (last visited Aug. 13, 2013).

Second, the payload data transmitted over unencrypted Wi-Fi networks is only "accessible" with some difficulty.

Unlike traditional radio broadcasts, a Wi-Fi access point cannot associate or communicate with a wireless device until it has been authenticated. *See* IEEE Computer Soc'y, *IEEE Standard for Information Technology — Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks — Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* 473, Fig. 11-6 (2007). Devices on Wi-Fi networks—even unencrypted networks—communicate via encoded messages sent to a specific destination over the wireless channel. *Id.* Therefore, intercepting and decoding payload data communicated on a Wi-Fi network requires sophisticated hardware and software. To capture this information, a wireless device must initiate a connection with the network and send encapsulated and coded data over the network to a specific destination. If the communications were intercepted by a traditional analog radio device they would sound indistinguishable from random noise. Wi-Fi transmissions are not "readily accessible" to the "general public" because most of the general public lacks the expertise to intercept and decode payload data transmitted over a Wi-Fi network.[8] Even if it is commonplace for

[8] Google argues that unencrypted data transmitted over a Wi-Fi network is "readily accessible to the general public" because the hardware used to intercept the data can be purchased by anyone and the software used to decode the data can be downloaded from the internet. A district court also reached this conclusion in a patent case. *See In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 893 (N.D. Ill. 2012) ("In light of the ease of sniffing Wi–Fi networks, the court concludes that the communications sent on an unencrypted Wi–Fi network are readily accessible to the general public."). The availability of the technology necessary to intercept the communication cannot be the sole determinant of whether it is "readily accessible to the general public" as the phrase is ordinarily understood. A device that surreptitiously logs a computer user's keystrokes can be purchased online and easily installed, but that

members of the general public to connect to a neighbor's unencrypted Wi-Fi network, members of the general public do not typically mistakenly intercept, store, and decode data transmitted by other devices on the network. Consequently, we conclude that Wi-Fi communications are sufficiently inaccessible that they do not constitute an "electronic communication . . . readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i) as the phrase is ordinarily understood.

IV. CONCLUSION

For the foregoing reasons, we affirm the judgment of the district court.

AFFIRMED.

hardly means that every keystroke—whether over a wired or a wireless connection—is "readily accessible to the general public."