FEDERAL STATUTES — WIRETAP ACT — NINTH CIRCUIT HOLDS THAT INTERCEPTING UNENCRYPTED WI-FI BROADCASTS VIOLATES THE WIRETAP ACT. — *Joffe v. Google, Inc.*, 729 F.3d 1262 (9th Cir. 2013), *amended by* No. 11-17483, 2013 WL 6905957 (9th Cir. Dec. 27, 2013).

The Electronic Communications Privacy Act of 1986[1] (ECPA) attempted to modernize Title III of the Omnibus Crime Control and Safe Streets Act of 1968[2] (Wiretap Act) for the digital age by creating new protections for electronic communications such as "voice, data, and video communications, including cellular phones, and email [and] other computer transmissions."[3] However, the rapid expansion of the Internet has given courts the difficult task of applying old law to ever-changing technologies.[4] Recently, in *Joffe v. Google, Inc.*,[5] the Ninth Circuit wrestled with the application of the Wiretap Act to local wireless (Wi-Fi) networks and found that Google could face liability for accessing data from an unencrypted Wi-Fi network.[6] In an opinion filed in September 2013, the panel refused to fit unencrypted data on a Wi-Fi network into the Wiretap Act's safe harbor for electronic communications "readily accessible to the general public."[7] The Ninth Circuit evaluated whether the data was "readily accessible" by examining the geographic range of the network and the skill necessary to intercept it.[8] In December 2013, the Ninth Circuit amended its *Joffe* opinion by omitting the section that addressed whether the data was readily accessible to the general public, leaving the issue for the district court to resolve.[9] Rather than using the factors chosen by the Ninth Circuit in its initial opinion, courts should instead consider employing an "express prohibition" test based on the objective configuration of the network to evaluate whether a network is readily accessible to the general

---

[1] Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[2] Pub. L. No. 90-351, tit. III, 82 Stat. 223 (codified as amended at 18 U.S.C. §§ 2510–2521 (2012), 47 U.S.C. § 605 (2006)).

[3] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1441 (2001).

[4] *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1293 (2004) ("Even with foresight, the law is bound to be lagging behind technological developments, especially given the profound specificity and detail of the current [ECPA] statutory regime.").

[5] 729 F.3d 1262 (9th Cir. 2013), *amended by* No. 11-17483, 2013 WL 6905957 (9th Cir. Dec. 27, 2013).

[6] *Id.* at 1264.

[7] *Id.* at 1277 (quoting 18 U.S.C. § 2511(2)(g)(i) (2012)) (internal quotation marks omitted); *see* 18 U.S.C. § 2511(2)(g)(i).

[8] *See Joffe*, 729 F.3d at 1277–79.

[9] *See Joffe*, 2013 WL 6905957 (granting in part Google's petition for rehearing and amending the opinion such that section III.B, "Wi-Fi Transmissions Are Not 'Readily Accessible to the General Public' under 18 U.S.C. § 2511(2)(g)(i)," and related material from the original opinion are omitted).

public.[10] While the express prohibition test may run counter to public expectations of privacy, it is supported by both the statutory text and the legislative history of the ECPA.

In 2007, Google initiated efforts to add street-level images to its Google Maps service.[11] To create these images, Google drove motor vehicles equipped with cameras down public streets.[12] Many of these vehicles were equipped with Wi-Fi antennas and software that collected basic identifying information about the Wi-Fi networks the vehicles encountered along the way — including wireless network names (SSIDs) and unique hardware numbers (MAC addresses) — to enhance location-based services for mobile devices.[13] In addition, in a practice known as "packet sniff[ing],"[14] Google's Street View cars stored "payload data" — actual data fragments transmitted as part of a "data packet" sent from one device to another — which sometimes contain "personal emails, usernames, passwords, videos, and documents."[15] After several class action lawsuits were filed challenging Google's data-collection practices, the Judicial Panel on Multidistrict Litigation transferred the cases to the Northern District of California.[16] Plaintiffs — individuals whose homes could be seen in Google Maps' Street View and who claimed that Google accessed payload data from their unencrypted Wi-Fi networks — filed a consolidated complaint alleging violations of the Wiretap Act and other statutes.[17] Google filed a motion to dismiss.[18]

The Wiretap Act makes it unlawful to intentionally intercept "any wire, oral, or electronic communication."[19] However, it supplies a

---

[10] *See* Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 101, 130 (2004).

[11] *Joffe*, 729 F.3d at 1263–64. *See generally Google Announces New Mapping Innovations at Where 2.0 Conference*, GOOGLE (May 29, 2007), http://googlepress.blogspot.com/2007/05/google-announces-new-mapping_29.html.

[12] *Joffe*, 729 F.3d at 1264. *See generally Behind the Scenes: Street View*, GOOGLE, http://www.google.com/maps/about/behind-the-scenes/streetview/ (last visited Mar. 1, 2014).

[13] *Joffe*, 729 F.3d at 1264.

[14] *Id.* at 1272. In 2010, Google acknowledged this practice, explained that it was unintentional, apologized, ceased the data collection, and rendered the user payload data it had collected inaccessible. *Id.* at 1264; *see also WiFi Data Collection: An Update*, GOOGLE (June 9, 2010), http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html. For background on how Wi-Fi scanning could inadvertently become packet sniffing, see Robert Graham, *Technical Details of the Street View WiFi Payload Controversy*, ERRATA SECURITY (May 19, 2010), http://blog.erratasec.com/2010/05/technical-details-of-street-view-wifi.html.

[15] *Joffe*, 729 F.3d at 1264.

[16] *Id.*

[17] *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1070 (N.D. Cal. 2011). The plaintiffs also brought suit under the California Business and Professional Code and various state wiretap statutes. *See id.* at 1072.

[18] *Id.* at 1070.

[19] 18 U.S.C. § 2511(1)(a) (2012).

number of exemptions, two of which were alternately implicated in *Joffe*. First, it provides an exemption for intercepting a radio communication that is "readily accessible to the general public,"[20] which in turn is defined as communication that is *not*, among other things, "scrambled or encrypted."[21] The statute does not define "radio communication."[22] Second, the statute provides an exemption for intercepting an electronic communication that is "configured so [as to be] . . . readily accessible to the general public."[23] The statute defines "electronic communication,"[24] but does not define "readily accessible" in this context.[25] Google arguably could have avoided liability under either the radio communication exemption, because the broadcasts were unencrypted and therefore "readily accessible" by statutory definition, or the electronic communication exemption, if the communication was found to be "readily accessible."

The district court granted in part and denied in part the motion to dismiss, allowing the Wiretap Act cause of action to proceed and dismissing all others.[26] Judge Ware concluded that Wi-Fi broadcasts are electronic communication. While the plain meaning and dictionary definitions "fail[ed] to yield a definitive and unambiguous result,"[27] the legislative history demonstrated an intent for radio communication to be limited to "traditional radio services."[28] Judge Ware also found that the statutory definition of "readily accessible to the general public" for radio communication does not apply to the electronic communication exemption.[29] Instead, based on the plain meaning of the statutory language, the court held that payload data on an unencrypted Wi-Fi net-

---

[20] *Id.* § 2511(2)(g)(ii)(II). For the other exemptions for radio communication, see *id.* § 2511(2)(g)(ii)(I), (III), and (IV).

[21] *Id.* § 2510(16)(A). For other factors of what makes radio communication readily accessible to the general public, see *id.* § 2510(16)(B)–(E).

[22] *See id.* § 2510.

[23] *Id.* § 2511(2)(g)(i).

[24] *Id.* § 2510(12) (defining electronic communication as a communication on a "wire, radio, electromagnetic, photoelectronic or photooptical system").

[25] *Id.* § 2510(16).

[26] *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1070 (N.D. Cal. 2011). The court found that the Wiretap Act preempted state wiretap statutory schemes and dismissed the state wiretap statutory causes of action with prejudice. *Id.* at 1085. The court dismissed without prejudice the action under the California Business and Professional Code, holding that California's Proposition 64 — which demands that a plaintiff "establish that he has suffered an 'injury in fact' and has 'lost money or property as a result of such unfair competition'" — creates a "heightened standing requirement[]" that the plaintiffs had not met. *Id.* at 1086 (quoting Hall v. Time Inc., 70 Cal. Rptr. 3d 466, 467 (Ct. App. 2008)). Invasion of privacy is not enough to meet this standing requirement, and the plaintiffs had not alleged lost money or property. *Id.* at 1083.

[27] *Id.* at 1078.

[28] *Id.* at 1080 (internal quotation marks omitted).

[29] *Id.* at 1081. The court thus rejected Google's argument that since 18 U.S.C. § 2510(16)(A) defines "readily accessible to the general public" as not "scrambled or encrypted," the fact that the plaintiffs' networks were unencrypted meant that the data was readily accessible. *Google St. View Litig.*, 794 F. Supp. 2d at 1083.

work is not readily accessible because of the "specially-designed,"[30] "rare,"[31] and "sophisticated packet sniffer technology"[32] necessary to intercept it, and found that Google could be liable under the Wiretap Act.[33]

The Ninth Circuit affirmed.[34] Writing for a unanimous panel, Judge Bybee[35] agreed that Wi-Fi broadcasts are electronic communication rather than radio communication.[36] Next, in the section omitted from the amended opinion,[37] the panel held that unencrypted Wi-Fi transmissions are not "'readily accessible to the general public' under the ordinary meaning of that phrase."[38] Judge Bybee rejected three arguments Google made in favor of classifying Wi-Fi broadcasts as radio communication — a plain meaning argument,[39] a legislative history argument,[40] and an appeal to the rule of lenity[41] — finding them unpersuasive and thus finding the radio communication exemption inapplicable.

In the section omitted from the amended opinion, Judge Bybee further held that the electronic communication exemption did not apply. Google argued that software able to intercept unencrypted Wi-Fi payload data is freely available on the Internet and that, as the Northern District of Illinois had previously held, intercepting unencrypted Wi-Fi network payload data should not be unlawful.[42] Judge Bybee disagreed,

---

[30] *Google St. View Litig.*, 794 F. Supp. 2d at 1082.

[31] *Id.* at 1083.

[32] *Id.* at 1082.

[33] *Id.*; *see also id.* at 1083 ("Plaintiffs plead that the networks were themselves configured to render the data packets, or electronic communications, unreadable and inaccessible without the use of rare packet sniffing software; technology allegedly outside the purview of the general public.").

[34] *Joffe*, 729 F.3d at 1264.

[35] Judge Bybee was joined by Judges Tashima and Stafford.

[36] *Joffe*, 729 F.3d at 1275–76.

[37] *Compare id.* at 1276–79, *with* Joffe v. Google, Inc., No. 11-17483, 2013 WL 6905957, at *13 (9th Cir. Dec. 27, 2013).

[38] *Joffe*, 729 F.3d at 1277 (quoting 18 U.S.C. § 2511(2)(g)(i) (2012)).

[39] Google argued that radio communication plainly means all information transmitted via radio frequencies, *id.* at 1268, but Judge Bybee found that the common meaning of the phrase as well as its use in the statute as a whole confirm that Congress intended only to include "predominantly auditory" radio broadcasts like AM and FM radio, *id.* at 1270–71.

[40] Google pointed to two pieces of evidence: a report of a congressional task force from 1990 and an enactment in 1994 and subsequent repeal in 1996 of a revision to section 2510(16). *Id.* at 1274–75. However, Judge Bybee found neither persuasive, affording no weight to the report of a task force consisting of only fifteen members and finding Google's "series of inferences," *id.* at 1275, about the repeal insufficient. *Id.* at 1275–76.

[41] *Id.* at 1276–77. The rule of lenity was arguably applicable because Google could also face criminal charges under the Wiretap Act. *Id.* at 1277 (citing Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004)). However, Judge Bybee rejected this argument, stating "we do not resort to the rule of lenity every time a difficult question of statutory interpretation arises. . . . Here, the traditional tools of statutory interpretation are sufficient." *Id.*

[42] *Id.* at 1278 n.8 (citing *In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 893 (N.D. Ill. 2012)).

noting in a footnote that "[t]he availability of the technology necessary to intercept the communication cannot be the sole determinant" of accessibility, and analogized packet sniffing technology to keystroke-logging software, which might be easy to download from the Internet but does not make every keystroke "readily accessible."[43] Judge Bybee relied on two factors to determine that the technology was not "readily accessible." First, unencrypted Wi-Fi networks have a small service range compared to broadcasts such as AM or FM radio, making them less available to the public as a spatial matter.[44] Second, the payload data is accessible only with "some difficulty": even on an unencrypted network, devices "communicate via encoded messages" and "sophisticated hardware and software" is required to intercept and decode the messages.[45] To intercept the data, a device has to "initiate a connection" and "send encapsulated and coded data over the network to a specific destination."[46] As Judge Bybee noted "the general public lacks the expertise to intercept and decode payload data"[47] and "do[es] not typically mistakenly intercept, store, and decode data transmitted by other devices on the network."[48] Based on these considerations, Judge Bybee concluded that Wi-Fi transmissions are not readily accessible to the general public and that therefore Google could face liability under the Wiretap Act.

The amended Ninth Circuit opinion correctly removed this analysis, which strayed from the statutory text and the guidance of the legislative history. The statute's electronic communication exemption is for systems "*configured* so that such electronic communication is readily accessible to the general public."[49] The word "configured" has been interpreted to suggest that courts should use an "express prohibition" test that looks at whether the network's configuration actually prevents access[50] — a reading the legislative history supports. When analyzed in this light, an unencrypted Wi-Fi network lacks an express prohibition and thus fits under the electronic communication exemption. While the results may run contrary to the public's expectations of privacy, such a concern is an issue that Congress, and not the courts, should address. In removing this section of the original opinion, the Ninth Circuit wisely gave district courts an opportunity to employ a different test.

---

[43] *Id.*
[44] *Id.* at 1277–78.
[45] *Id.* at 1278.
[46] *Id.*
[47] *Id.*
[48] *Id.* at 1279.
[49] 18 U.S.C. § 2511(2)(g)(i) (2012) (emphasis added).
[50] *See* Kern, *supra* note 10, at 128, 138; *see also, e.g.*, Snow v. DirecTV, Inc., 450 F.3d 1314, 1316 (11th Cir. 2006).

The statutory text focuses on the configuration of the electronic network, which suggests that an "express prohibition" test should be used. An express prohibition test is "an objective test that looks at the network operator's actions to determine whether the operator expressed or implied prohibition on access, which . . . would conclusively show that access was unauthorized."[51] The question then should be whether the "communicator took steps to keep [the communication] private."[52] Since Congress provided "bright line"[53] tests for when the Wiretap Act exempts interception of *radio* communication — such as when such a radio communication is unencrypted[54] — "it is more appropriate to classify the ECPA as a statute that applies the express prohibition test [rather] than the reasonable expectations test"[55] for *electronic* communication as well. The Eleventh Circuit implicitly applied the express prohibition test to an electronic communication in *Snow v. DirecTV, Inc.*,[56] holding that an electronic bulletin board — which required users to create an account and exhorted that certain parties not join[57] — was not configured to be private.[58] While the website operator *intended* to make the website private, the configuration did not effectively do so: "[A]n Internet website must be *configured* in some way so as to limit ready access by the general public."[59]

The legislative history of the ECPA also supports this approach. The Senate Report on the ECPA emphasized that "[t]he term 'configure' is intended to establish an *objective standard of design configuration* for determining whether a system receives privacy protection."[60] This understanding is identical in approach[61] to that in the radio

---

51 Kern, *supra* note 10, at 128.

52 Ehling v. Monmouth-Ocean Hosp. Serv. Corp., Civ. No. 2:11–cv–03305 (WJM), 2013 WL 4436539, at *7 (D.N.J. Aug. 20, 2013) (holding that Facebook wall posts set as "private" are not readily accessible).

53 Kern, *supra* note 10, at 138 (internal quotation marks omitted).

54 *See* 18 U.S.C. § 2510(16).

55 Kern, *supra* note 10, at 138.

56 450 F.3d 1314 (11th Cir. 2006).

57 *Id.* at 1316.

58 *Id.* at 1322.

59 *Id.* (emphasis added); *see also id.* ("To be clear, we do not require a plaintiff to 'plead in grave detail' all of a website's restrictive technical configurations. . . . Here, a short simple statement that the plaintiff screens the registrants before granting access may have been sufficient to infer that the website was not configured to be readily accessible to the general public.").

60 S. REP. NO. 99-541, at 18 (1986) (emphasis added).

61 The Ninth Circuit made a compelling textualist argument that radio and electronic communications are treated differently in the Wiretap Act, noting that the former, unlike the latter, are predominantly auditory. *See Joffe*, 729 F.3d at 1270. However, it does not follow that the *kind* of test used to evaluate the parallel "readily available" exemptions should differ; indeed, given that radio is a type of electronic communication, *see* 18 U.S.C. § 2510(12) (2012), it follows that the two should be evaluated under a similar approach where, as here, that approach is consistent with the statute.

communication exemption, where the statute does define "readily accessible to the general public": the communication is not private when it is not "scrambled or encrypted," transmitted using techniques "withheld from the public," and so on.[62] As such, the configuration of the network, not the intent of the owner, should govern.[63]

Congress's analysis regarding the technology in existence in 1986, the year in which the ECPA was enacted, demonstrates this framework in application.[64] The House Report recognized the growing use of electronic bulletin board systems[65] and noted that "[a] person may reasonably conclude that a communication is readily accessible to the general public" if the "means of access are widely known" and if a user accessing the network does not "encounter any warnings, encryptions, password requests, or other indicia of intended privacy."[66] The test depends on the network's configuration, as understood by the lack of empirical "indicia" that expressly prohibit access. An unencrypted Wi-Fi network is similarly configured to be readily accessible under this standard. The plaintiffs' wireless routers publicly broadcasted their SSIDs and other identifying information so that anyone nearby could see and connect to them, and the plaintiffs did not create a password, enable encryption, or take any affirmative steps to ensure privacy.[67]

The factors applied by the Ninth Circuit in its original opinion strayed from this legislative history and the express prohibition standard embodied in the statute. Neither factor relied upon in the original *Joffe* decision speaks to how the network was "*configured* [to be] . . . readily accessible to the general public."[68] The language employed by the Ninth Circuit suggested instead a concern for whether

---

[62] 18 U.S.C. § 2510(16).

[63] *But see* Orin Kerr, *District Court Rules that the Wiretap Act Does Not Prohibit Intercepting Unencrypted Wireless Communications*, VOLOKH CONSPIRACY (Sept. 6, 2012, 7:08 PM), http://www.volokh.com/2012/09/06/district-court-rules-that-the-wiretap-act-does-not-prohibit-intercepting-unencrypted-wireless-communications ("[T]he text focuses on the intent of the designer — the person who does the *configuring* of the network *so* that it works a particular way — to design the network so that the general public was *supposed* to be able to access them.").

[64] *See* William Jeremy Robison, Note, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1204–05 (2010) ("[The ECPA] is best understood by considering its operation and purpose in light of the technology that existed in 1986. The Act is not built around clear principles that are intended to easily accommodate future changes in technology; instead, Congress chose to draft a complex statute based on the operation of early computer networks. To apply the Act to modern computing, courts need to begin by extracting operating principles from a tangled legal framework.").

[65] An electronic bulletin board system, in this usage, is "a computer program that simulates an actual bulletin board by allowing computer users who access a particular computer to post messages." United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990).

[66] H.R. REP. NO. 99-647, at 62 (1986).

[67] While connecting to a router is fundamentally different from accessing payload data being transmitted, the express prohibition test does not distinguish between the two.

[68] 18 U.S.C. § 2511(2)(g)(i) (2012) (emphasis added).

the public is aware that such an interception could occur,[69] but this concern is not a consideration compelled by the statute.[70]

Applying the express prohibition approach may lead to some unsettling results that contravene public expectations about privacy and technology. For instance, some wireless routers are unencrypted by default and consumers may purchase them without realizing or intending that their network be public. Nevertheless, without express prohibitions, connecting to the network and intercepting data are permitted. While the Fourth Amendment doctrine of reasonable expectation of privacy might prohibit the interception of data on such a network, the Wiretap Act does not.[71] The statutory language mandates this result by suggesting an express prohibition test rather than one that relies on express authorization or expectations.[72] It is Congress's job to adapt the Wiretap Act to remedy this problem, not the job of the courts.

The statutory language and legislative history of the ECPA suggest that courts should use the express prohibition test to evaluate the "readily accessible to the general public" electronic communication exemption. The rapid evolution of technology can undermine both traditional understandings of the law and the expectations of private individuals — making a practice like packet sniffing legal. The Ninth Circuit in the original *Joffe* opinion came to the wrong result by applying the wrong test, and the court's ultimate decision to leave the question open demonstrates that Congress should update the law to match the public's privacy expectations.

---

[69] *See Joffe*, 729 F.3d at 1278–79 ("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. . . . [M]embers of the general public do not typically mistakenly intercept, store, and decode data transmitted by other devices on the network.").

[70] *See In re* Innovatio IP Ventures, LLC Patent Litig., 886 F. Supp. 2d 888, 893–94 (N.D. Ill. 2012) ("Any tension between [the] conclusion [that Wi-Fi packet sniffing on an unencrypted network is permissible under the Wiretap Act] and the public's expectation of privacy is the product of the law's constant struggle to keep up with changing technology. . . . But it is not the court's job to update the law to provide protection for consumers against ever changing technology." *Id.* at 894.).

[71] *See* United States v. Ahrndt, No. 3:08–CR–00468–KI, 2013 WL 179326, at *2–8 (D. Or. Jan. 17, 2013) (holding that the Fourth Amendment reasonable expectation of privacy right was violated when a woman assisted law enforcement officials by connecting to her neighbor's unencrypted Wi-Fi network and accessing child pornography files he was unintentionally sharing through iTunes and Limewire, but finding the woman did "nothing illegal," *id.* at *5).

[72] *See* Kern, *supra* note 10, at 128 (defining the express authorization test as "a test that presumes access by any 'outsider,' . . . to be unauthorized, absent express authorization"; the subjective expectations test as one that "looks at the intent of the network operator to determine whether access is unauthorized"; and the reasonable expectations test as "a more objective test that looks at the reasonable expectations of the network operator to determine whether access was unauthorized, or at the reasonable expectations of a user to determine intent").