DAVID H. KRAMER, State Bar No. 168452
MICHAEL H. RUBIN, State Bar No. 214636
BART E. VOLKMER, State Bar No. 223732
CAROLINE E. WILSON, State Bar No. 241031
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, CA 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100
Email: mrubin@wsgr.com

Attorneys for Defendant Google Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE INC. STREET VIEW ELECTRONIC COMMUNICATIONS LITIGATION	CASE NO.: 5:10-md-02184 JW (HRL) **DEFENDANT GOOGLE INC.'S MOTION TO DISMISS PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT** Hearing Date: March 21, 2011 Time: 9:00 a.m. Before: Honorable James Ware

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

RULES

MISCELLANEOUS

NOTICE OF MOTION & MOTION DISMISS

Please take notice that on March 21, 2011, at 9:00 a.m., before the Honorable James Ware, Defendant Google Inc. ("Google") will and hereby does move to dismiss with prejudice plaintiffs' Consolidated Class Action Complaint ("CCAC"). Google's motion is based on this notice, the accompanying memorandum of points and authorities, the declaration of Michael H. Rubin, the pleadings on file in these actions, arguments of counsel and any other matters that the Court deems appropriate.

STATEMENT OF ISSUE TO BE DECIDED

Does the CCAC state a claim for which relief can be granted under Rule 12(b)(6)?

MEMORANDUM OF POINTS & AUTHORITIES

I. INTRODUCTION

This case concerns Google's acquisition of radio broadcasts sent over open, unencrypted Wi-Fi networks. Google, like many other companies, collects and uses the presence of Wi-Fi networks to offer "location aware" services, like Google Maps. By allowing individuals to pinpoint their location using the identified Wi-Fi networks around them, Google can provide those people with directions and other location-specific information. Prior to mid-May 2010, Google collected the publicly available identifying information that Wi-Fi networks broadcast by using radio antennae mounted to cars that drove down public streets. If, at the instant Google drove by, a user was broadcasting data over an identified network and the network was configured to be open and unencrypted, Google also collected the data (known as "payload data") that was being broadcast.

Shortly after Google announced that it had collected this payload data, lawyers from across the country rushed to file more than a dozen putative class-action lawsuits alleging that Google violated the federal Wiretap Act and other laws. These lawsuits are misguided: it is not unlawful under the Wiretap Act to receive information from networks that are configured so that communications sent over them are "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). Because plaintiffs have already represented that their broadcasts took place over open, unencrypted networks, any broadcasts that Google acquired were, by the Wiretap Act's

plain language, "readily accessible to the general public." For that reason, Google did not violate the Wiretap Act by collecting payload data.[1]

Plaintiffs' parallel state wiretap claims fail for the identical reason, and because the federal Wiretap Act preempts those claims. Plaintiffs' claim under Section 17200 of the California Business and Professions Code is also preempted, and fails because plaintiffs have not sufficiently alleged the "actual injury" and "loss of money or property" that the statute requires.

In sum, the CCAC does not state a claim upon which relief can be granted and should be dismissed with prejudice.

II. FACTUAL BACKGROUND

A. Wi-Fi Technology.

Wi-Fi is a wireless communications protocol that uses radio waves to broadcast information pursuant to the IEEE 802.11 standard. *See* Rubin Dec., Ex. 4 at ¶ 9[2]; *see also Fujitsu Ltd. v. Netgear Inc.*, 620 F.3d 1321, 1325 (Fed. Cir. 2010). Wi-Fi is commonly used to connect computers and mobile devices to routers providing Internet access. *See* Rubin Dec., Ex. 3 at 1; *Fujitsu*, 620 F.3d at 1325. Each Wi-Fi-compliant device is assigned by its manufacturer a unique number called a MAC address. *See* Rubin Dec., Exs. 1, 2, 3, 4 at ¶ 8. In addition, wireless access points like routers are assigned alpha-numeric names called service set identifiers ("SSIDs"). *Id*., Exs. 1, 2, 3, 4 at ¶ 16. Most mobile phones and computers can detect a router's MAC Address and SSID. *Id*.

B. Google's Geo-Location Services.

Google has long used vehicles to drive down public streets in order to take photographs of their surroundings for use in its Street View service. For a time, those vehicles also collected

---

[1] As it has stated repeatedly, Google does not want the payload data it collected, did not and will not use the payload data in any product or service, and has taken steps to ensure that payload data is not collected again. But Google's acknowledgement that the collection was an error does not render Google's conduct unlawful, nor excuse plaintiffs from the pleading requirements mandated by the unambiguous language of the Wiretap Act.

[2] Rubin Declaration Exhibits 1, 2, 3, and 4 are all incorporated by reference into the CCAC. *See, e.g.*, CCAC ¶¶ 66, 69-72, 80. Accordingly, this Court may consider them. *See Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005).

identifying information regarding available Wi-Fi networks. CCAC ¶¶ 2, 4. To accomplish this, the vehicles were outfitted with readily available open source software and radio antennae. Rubin Dec., Ex. 4 at ¶¶ 23-28. The process by which Google identified available networks is similar to what happens when a person turns on his laptop or mobile phone to find Wi-Fi networks at a hotel, a coffee shop, or anywhere else. Because the presence of any Wi-Fi network acts as a unique landmark, knowing which combination of networks is nearby at a given time allows Google to help people determine their approximate locations based on which networks they can detect. The collection of publicly broadcast Wi-Fi network identification information is a common practice, and plaintiffs take no issue with it.

C. Google's Payload Collection.

On April 27, 2010, Google published a blog post stating that its Street View cars had been collecting SSID and MAC address information about Wi-Fi networks, but not payload data. CCAC ¶ 69; Rubin Dec., Ex. 1. Shortly thereafter, Google determined that its Street View vehicles were also collecting payload data that was publicly broadcast over open, unencrypted networks at the moment Google's vehicles drove by. CCAC ¶ 71; Rubin Dec., Ex. 2. Google quickly corrected its prior post and described the scope of the payload collection. CCAC ¶ 71; Rubin Dec., Ex. 2.

On June 9, 2010, Google released a report from an independent security firm that had analyzed, among other things, how Google collected public Wi-Fi radio broadcasts. Rubin Dec., Exs. 2, 4. The report describes how Google used freely available open-source software to passively collect radio broadcasts from Wi-Fi networks as its cars traveled down the road. By cycling through Wi-Fi channels five times per second, the software limited any single data-acquisition to two-tenths of one second. *Id*., Ex. 4 at ¶ 28. The report confirmed that only payload data that was broadcast over open, unencrypted networks was collected. *Id*., Ex. 4 at ¶ 20.

D. The Putative Class Action Lawsuits.

Since mid-May 2010, 19 putative class-action lawsuits have been filed across the country concerning Google's acquisition of payload data. The complaints collectively included the

following claims for relief: (1) the federal Wiretap Act; (2) the federal Computer Fraud and Abuse Act; (3) the federal Stored Communications Act; (4) Section 705 of the federal Communications Act; (5) state wiretap statutes; (6) common law privacy torts; (7) state data protection statutes; (8) conversion; (9) unjust enrichment; (10) trespass; (11) unfair competition; (12) accounting; and (13) California Penal Code Section 502. Most of plaintiffs' original complaints premised liability on Google's alleged acquisition of payload data broadcast over "open" or "open [and] unencrypted" networks. None of the plaintiffs named in the CCAC have alleged that they configured their Wi-Fi network to be closed or encrypted.[3] *See* Appendix A (chart detailing plaintiffs' prior statements that their networks were open and unencrypted, including (i) plaintiffs' core allegations in their original complaints, and (ii) the first joint case management statement in this action).

The parties filed motions with the Judicial Panel on Multidistrict Litigation ("MDL Panel") to have the extant cases transferred to a single court for pre-trial activities. On August 17, 2010, the MDL panel concluded that transfer was appropriate because the cases were predicated on the shared factual allegation that Google had acquired information from "class members' *open, non-secured wireless networks*." *See* MDL August 17, 2010 Transfer Order at 1 (emphasis added), Docket No. 1. Eight other cases were transferred by related case orders issued by this Court. Docket Nos. 17, 31, 48; Rubin Dec., Ex. 5. Two other cases were conditionally transferred by the MDL Panel. Docket Nos. 32, 59. All of these actions are consolidated for pre-trial purposes before this Court. *See* Docket No. 53.

On November 8, 2010, plaintiffs filed a consolidated complaint. The CCAC contains only three claims for relief: (1) the federal Wiretap Act; (2) state law wiretap statutes; and (3) California's Business and Professions Code Section 17200. Plaintiffs allege that Google's Street View vehicles used "packet sniffers" to collect "all types of data sent and received over

[3] Notably, the group of plaintiffs in the *Berlage* case had amended their complaint to add a new plaintiff, Denise Bergin, who alleged that she used a "closed or encrypted wireless network and internet connection." Rubin Dec., Ex. 11 (Berlage First Am. Compl. at ¶¶ 8, 15). Of the *Berlage* plaintiffs, Ms. Bergin alone was chosen to be excluded from the case upon filing of the CCAC.

the Wi-Fi connections." CCAC ¶ 4. Plaintiffs do not allege that Google used Wi-Fi payload data in any product or service. Instead, they plead that Google merely "stored the data on its servers." *Id*. at ¶ 6.

III. ARGUMENT

Under Rule 12(b)(6), a complaint should be dismissed when it "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "[O]nly a complaint that states a plausible claim for relief survives a motion to dismiss." *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1950 (2009). While the Court accepts as true all material allegations in the complaint, it need not accept the truth of conclusory allegations or unwarranted inferences, nor should it accept legal conclusions as true merely because they are cast in the form of factual allegations. *Id*. at 1949. ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice."); *Schmier v. U.S. Court of Appeals*, 279 F.3d 817, 820 (9th Cir. 2002). On a motion to dismiss, the Court may consider "documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007).

Here, the CCAC fails to state a claim upon which relief can be granted. Because plaintiffs cannot cure the CCAC's pleading deficiencies through amendment, the CCAC should be dismissed with prejudice.

A. Plaintiffs Have Failed To State A Federal Wiretap Act Claim.

The federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, prohibits the intentional interception of wire, oral, or electronic communications. 18 U.S.C. § 2511(1)(a). Plaintiffs' Wiretap Act claim here is based on the allegation that Google acquired "electronic communications" sent over "WiFi networks." CCAC ¶¶ 1, 18-38, 129. The radio waves broadcast by those Wi-Fi networks ("Wi-Fi Radio Broadcasts") are the "electronic communications" at issue in this case. *See* 18 U.S.C. § 2510(10) (defining "electronic communication" to include those that occur "in whole or in part" by radio). But, as noted, plaintiffs have admitted that their Wi-Fi networks were configured to be "open," or "open [and] unencrypted." *See* Appendix A. That is fatal to their wiretapping allegations. It is not unlawful under the Wiretap Act to acquire information

from networks configured in a way that makes communications sent over them "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i); *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1320-21 (11th Cir. 2006) ("Congress did not intend to criminalize or create civil liability for acts of individuals who 'intercept' or 'access' communications that are otherwise readily accessible by the general public."). Plaintiffs' Wi-Fi Radio Broadcasts were "readily accessible to the general public" under the Wiretap Act. That is confirmed by the plain text of the statute, its structure, and the case law.

1. Plaintiffs Have Failed To Plead Facts Showing That Their Wi-Fi Radio Broadcasts Were Not "Readily Accessible To The General Public."

To state a claim under the Wiretap Act, a plaintiff must plead facts showing that their communications were not "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i) ("It shall not be unlawful … to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public"); *see Snow*, 450 F.3d at 1321 (describing pleading requirements and stating: "the requirement that the electronic communication not be readily accessible by the general public is material and essential to recovery").

All radio broadcasts, including plaintiffs' Wi-Fi Radio Broadcasts, are by statutory definition "readily accessible to the general public" unless they are:

> (A) scrambled or encrypted;
>
> (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
>
> (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
>
> (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
>
> (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74

> that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

18 U.S.C. § 2510(16)(A)-(E) (defining what "readily accessible to the general public" means with respect to radio communications). Thus, a radio broadcast is "readily accessible to the general public" unless the plaintiff has pled facts to support one of the five exceptions set forth above.

A clear policy animates the statute: anyone may freely receive radio broadcasts as a matter of course unless the broadcast is scrambled or encrypted, uses particular modulation techniques, or is transmitted using specified non-public systems or frequencies. S. Rep. No. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 ("Radio communications are considered readily accessible to the general public unless they fit into one of five specified categories."). These are objective technical standards; the subjective beliefs or expectations of the broadcaster concerning public accessibility are irrelevant. S. Rep. No. 99-541, at 18 (Section 2511(2)(g)(i) creates "an objective standard of design configuration for determining whether a system receives privacy protection").

Plaintiffs do not even attempt to plead facts showing that their Wi-Fi Radio Broadcasts fall within one of the five narrow exceptions to the "readily accessible" presumption for radio broadcasts. Without a single supporting fact, plaintiffs merely recite the bare legal conclusion that their Wi-Fi Radio Broadcasts were "not readily accessible to the general public." CCAC ¶¶ 18-38, 130, 142. That is insufficient. *See Ashcroft*, 129 S. Ct. at 1949 ("A pleading that offers 'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action will not do.'") (citations omitted); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007); *Snow*, 450 F.3d at 1321 (conclusory allegation that website was not readily accessible insufficient); *Birdsong v. Apple, Inc.*, No. 06-2280, 2008 WL 7359917, at *3 (N.D. Cal. June 13, 2008) ("Plaintiffs' legal conclusion . . . is insufficient. Rather, a plausible set of facts must either be alleged or be apparent to the Court upon which Plaintiffs could prevail."). These plaintiffs must plead *facts*, which, if taken as true, would bring their broadcasts within Section 2510(16). *Snow*, 450 F.3d at 1321 ("To survive a motion to dismiss, [plaintiff] must have alleged, at a minimum, facts from

which we could infer that his electronic bulletin board was not readily accessible to the general public."). They have not done so and their Wiretap Act claim should be dismissed. *See, e.g.*, *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1009 (9th Cir. 2006) (affirming dismissal of ECPA case under Rule 12(b)(6) based on the plain language of the statute); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1265-72 (N.D. Cal. 2001) (dismissing under Rule 12(b)(6) a putative class action brought under the Wiretap Act and ECPA).

2. Plaintiffs Cannot Plead Facts Supporting A Claim That Their Wi-Fi Radio Broadcasts Were Not "Readily Accessible To The General Public."

Plaintiffs would not be able to cure the pleading defects in the CCAC by amendment because the exceptions to the "readily accessible" presumption are at odds with the facts plaintiffs have pled and the central premise of their case. Accordingly, no leave to amend should be granted. *See, e.g.*, *Leadsinger, Inc. v. BMG Music Publ'g*, 512 F.3d 522, 532 (9th Cir. 2008) (leave to amend should not be granted when doing so would be futile).

a. Plaintiffs Cannot Plead Facts Alleging That Their Wi-Fi Radio Broadcasts Were "Scrambled Or Encrypted."

Plaintiffs have not alleged in the CCAC that they configured their Wi-Fi networks to be "scrambled or encrypted." 18 U.S.C. § 2510(16)(A). Nor could they given their repeated admissions that they broadcast using *open, unencrypted* wireless networks:

- Each plaintiff "used and maintained at all times relevant and material hereto an unencrypted wireless internet connection at his home." Berlage First Am. Compl. ¶¶ 5-7 (Rubin Dec., Ex. 10).
- "During all relevant times [plaintiffs] used an open Wi-Fi network at their residence." Carter Compl. ¶ 6 (Rubin Dec., Ex. 9).
- "During all times relevant herein, [plaintiff] used and maintained an open wireless internet connection at his home which he shares with his wife and family." Colman Compl. ¶ 5 (Rubin Dec., Ex. 7).
- Plaintiffs "maintained and used an open wireless internet connection." Van Valin Compl. ¶¶ 4-5 (Rubin Dec., Ex. 6).

See also Appendix A.

Instead of asserting that they scrambled or encrypted their networks, plaintiffs allege that it takes sophisticated technology to acquire their publicly available Wi-Fi Radio Broadcasts. *See, e.g.*, CCAC ¶ 55. Regardless of whether that allegation is true, it is entirely beside the point. The Wiretap Act is clear that all radio broadcasts are open to the public unless the system over which they are sent scrambles or encrypts them. *See* 18 U.S.C. § 2511(2)(g)(i); 18 U.S.C. § 2510(16)(A). The legislative history confirms this plain meaning and instructs that anyone wishing to invoke the "scrambled or encrypted" exception for radio networks must configure their networks to convert their "signal[s] into unintelligible form." S. Rep. No. 99-541, at 15. The encryption inquiry does not turn on the sophistication of radio receivers, but on the technical network configuration steps that one must take to render a radio broadcast unintelligible to the public. *Id.*[4] Plaintiffs here have not alleged that they configured their networks to encrypt or scramble their Wi-Fi Radio Broadcasts. They have alleged the opposite – that their networks were open and unencrypted – and that permanently dooms their wiretap claim. *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, 138 (2004) (the definition of "readily accessible" with respect to radio broadcasts "removes all Wi-Fi networks that do not use encryption from the ECPA's protection.").[5]

---

[4] The Senate Report leaves no room for debate about what constitutes scrambling or encryption: "These terms are used in their technical sense. To 'encrypt' or to 'scramble' means to convert the *signal* into unintelligible form by means intended to protect the contents of a communication from unintended recipients. Methods which merely change the form of a plaintext message, e.g., a device which converts an analog signal to a digital stream, does not provide 'encryption' within the meaning of this bill." S. Rep. No. 99-541 at 15 (emphasis added).

[5] Plaintiffs include a smattering of allegations in the CACC about the alleged scarcity of devices that could acquire their Wi-Fi Radio Broadcasts. Such incorporeal allegations offer no future salvation. The notion that alleged scarcity of receiving devices is relevant to the encryption or scrambling analysis is foreclosed not only by the statute itself, but also by the rule of lenity. That canon of statutory interpretation "requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them." *United States v. Santos*, 553 U.S. 507, 514, 523 (2008) (rule applies to statutes like the Wiretap Act that have both civil and criminal applications). And the rule would be violated by an interpretation of "scrambled or encrypted" that allowed liability to be found one day based on a supposed scarcity of receiving devices, but not the next when such devices passed some undefined threshold of prevalence. *See id*. at 514 (the rule of lenity ensures that "no citizen should be held accountable for a violation of a statute whose commands are

(continued...)

Given that plaintiffs did not scramble or encrypt their Wi-Fi Radio Broadcasts, there is no doubt that those broadcasts were "readily accessible to the general public" under §2510(16)(A) of the Wiretap Act. Indeed, in a similar case, the district court in Oregon recently held just that. *See United States v. Ahrndt*, No. 08-468, 2010 WL 373994 (D. Or. Jan. 28, 2010). In *Ahrndt*, a woman logged on to her neighbor's open Wi-Fi network and accessed an iTunes folder on his personal computer that appeared to contain child pornography. *Id*. at *1. She alerted the police, and an officer came to her house and duplicated her steps. *Id*. That led to search warrants and the defendant's arrest. *Id*. at *1-*2. The defendant moved to suppress on the ground, *inter alia*, that the officer violated the Wiretap Act by using the defendant's open Wi-Fi network to access the computer files at issue. The Court rejected that position because "defendant's wireless network system was configured so that any electronic communications emanating from his computer via his iTunes program were readily accessible to any member of the general public with a Wi-Fi enabled laptop." *Id*. at *8.

The logic of *Ahrndt*—that files accessed directly *on* the defendant's home computer were "readily accessible to any member of the general public" because his Wi-Fi network was configured to be open and unsecured—compels the conclusion that the Wi-Fi Radio Broadcasts in this case are likewise "readily accessible to the general public" under the statute. *See id.* at *1, *8. Indeed, the defendant's files in *Ahrndt* were far *less* accessible to the general public than plaintiffs' Wi-Fi Radio Broadcasts were here. The materials in that case resided on the defendant's personal computer in his home and were not broadcast onto the street over radio waves. To access the materials at issue in *Ahrndt*, the police needed to take a number of volitional steps: (1) logging on to the defendant's network; (2) accessing his iTunes library; (3) viewing the folder structure; (4) opening a folder; and (5) opening a file. In sharp contrast, plaintiffs base their Wiretap claim on Google's passive, non-targeted collection of Wi-Fi Radio

---

(...continued from previous page)
uncertain, or subjected to punishment that is not clearly prescribed."); *Facebook, Inc. v. Power Ventures, Inc*., No. C 08-05780, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010) (rejecting statutory interpretation under rule of lenity that would allow liability to be predicated on web sites' malleable user agreement as that "would create a constitutionally untenable situation in which criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use").

Broadcasts transmitted publicly over open, unencrypted networks as Google Street View vehicles passed by.

* * *

Given plaintiffs' prior admissions about their use of open, unencrypted Wi-Fi networks, it would be futile to provide them an opportunity to try to plead that the Wi-Fi Radio Broadcasts were not "readily accessible to the general public" because they were "scrambled or encrypted." 18 U.S.C. § 2510(16)(A).

b. Plaintiffs Cannot Plead Facts Alleging That Their Wi-Fi Radio Broadcasts Meet Any Other Exception To The "Readily Accessible" Presumption.

It would be equally futile to allow plaintiffs to try to plead that their Wi-Fi Radio Broadcasts were not readily accessible based on one of the other provisions of 18 U.S.C. § 2510(16)(B-E).

First, plaintiffs cannot plead that their Wi-Fi Radio Broadcasts were "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication." 18 U.S.C. § 2510(16)(B). Unencrypted Wi-Fi communications are transmitted pursuant to detailed parameters set forth in federal regulations and using a standard—802.11—that has been publicized widely and discussed in patents, industry groups, business literature, and the press. *See* 47 C.F.R. § 15 *et seq*.; *Fujitsu*, 620 F.3d at 1325. The point of having a standard govern Wi-Fi broadcasts is so that businesses and individuals may know precisely how the protocol works to enable them to build and use interoperable devices and systems. *See, e.g.*, *Fujitsu*, 620 F.3d at 1325 ("Products in this industry adhere to standards to ensure interoperability."). Because the standard is by design open to the public, plaintiffs cannot meet this exception.

Second, plaintiffs cannot allege that their Wi-Fi Radio Broadcasts were "carried on a subcarrier or other signal subsidiary to a radio transmission." 18 U.S.C. § 2510(16)(C). Subcarrier and subsidiary radio transmissions relate to collateral information that accompanies commercial radio and television broadcasts; they have nothing to do with Wi-Fi. *See* S. Rep. No. 99-541, at 15 ("this category includes, for example, data and background music services carried

on FM subcarriers. It also includes data carried on the Vertical Blanking Interval (VBI) of a television signal.").

Third, plaintiffs cannot allege that their Wi-Fi Radio Broadcasts were "transmitted over a communication system provided by a common carrier." 18 U.S.C. § 2510(16)(D). Plaintiffs are natural persons who plainly do not qualify for common-carrier status. Nor would some new allegation that their Wi-Fi networks were "provided by" an Internet Service Provider ("ISP") change the result. ISPs that offer enhanced services like Internet access are not regulated as common carriers. *See Howard v. America Online, Inc.*, 208 F.3d 741, 752 (9th Cir. 2000); *McKinney v. Google, Inc.*, No. 10-01177 JW, slip op. at 13-14 (N.D. Cal. Nov. 16, 2010) ("Internet Service Providers are generally not common carriers.").

Fourth, plaintiffs could not claim that their Wi-Fi Radio Broadcasts were sent over the specific non public radio frequencies referenced in 18 U.S.C. § 2510(16)(E). Wi-Fi transmissions do not use those frequencies. And this subsection of the Wiretap Act shows that Congress knows how to place entire radio frequencies off-limits from consumption by the general public. If Congress had wanted to create a blanket prohibition on the acquisition of Wi-Fi transmissions, it had an easy and ready mechanism to do so. But it did not. Hence, unencrypted Wi-Fi radio broadcasts are readily accessible to the general public.

* * *

The plain text and structure of the Wiretap Act make clear that the radio broadcasts at issue in this case were "readily accessible to the general public." Under Section 2511(2)(g)(i), there can be no Wiretap Act liability.

B. Plaintiffs' State Law Wiretap Claims Fail.

In addition to the federal Wiretap Act, plaintiffs have asserted claims under the wiretap laws of Arizona, Hawaii, Minnesota, Nebraska, Ohio, South Carolina, Utah, Tennessee, Missouri, Washington, Pennsylvania, Nevada and Texas. CCAC ¶ 141. Plaintiffs allege that these statutes are "substantially similar to 18 U.S.C. § 2511." *Id*. These claims must be dismissed for the same reason that plaintiffs' federal Wiretap Act claim fails: plaintiffs' Wi-Fi Radio Broadcasts were

"readily accessible to the general public." Regardless, the state wiretap claims should be dismissed based on federal preemption.

Federal law may preempt state law in three ways: (1) expressly; (2) by pervasive regulation demonstrating implicit intent to displace state law in a particular field; or (3) where there is a conflict between state law and federal law and enforcement of the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Silvas v. E*Trade Mortg. Corp.*, 514 F.3d 1001, 1004 (9th Cir. 2008) (quoting *Bank of Am. v. City & Cnty. of S.F.*, 309 F.3d 551, 558 (9th Cir. 2002)). All three doctrines of preemption bar plaintiffs' state wiretap claims here.

1. Plaintiffs' State Wiretap Claims Are Expressly Preempted.

The Wiretap Act contains an express preemption clause: "[t]he remedies and sanctions described in this chapter with respect to the interception of electronic communications are the *only* judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications." 18 U.S.C. § 2518(10)(c) (emphasis added). Yet plaintiffs assert state wiretap law claims because they allegedly "provide a remedy *in addition* to the Federal Wiretap Statute." CCAC ¶ 144 (emphasis added). The federal statute is unambiguous, and any "additional remedies" that plaintiffs seek from state laws are preempted. *See Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253-54 (1992) ("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there."); *Bunnell v. MPAA*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (holding federal Wiretap Act expressly preempts parallel state law claims); *Quon v. Arch Wireless*, 445 F. Supp. 2d 1116, 1138 (C.D. Cal. 2006) ("Only those remedies outlined in the [statute] are the ones, save for constitutional violations, that a party may seek for conduct prohibited by the [statute]."), *rev'd on other grounds*, 529 F.3d 892 (9th Cir. 2008).[6]

[6] Some courts have ruled that the Wiretap Act's preemption clause operates only to prevent the exclusion of evidence in a criminal proceeding. *See, e.g.*, *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 483 F. Supp. 2d 934, 938-39 (N.D. Cal. 2007); *Bansal v. Russ*, 513 F. Supp. 2d 264, 282-83 (E.D. Pa. 2007). Those constructions should be rejected because they conflict with the plain language of the Wiretap Act, which precludes all other remedies. *See* 18 U.S.C. § 2518(10)(c).

2. Plaintiffs' State Wiretap Claims Are Barred Based On Field Preemption.

In addition to being expressly preempted, plaintiffs' state wiretap claims also fail based on field preemption. That doctrine applies where federal law "is sufficiently comprehensive to infer that Congress left no room for supplementary regulation by the states. When the federal government completely occupies a given field or an identifiable portion of it . . . the test of preemption is whether the matter on which the state asserts the right to act is in any way regulated by the federal government." *Pub. Util. Dist. No. 1 of Grays Harbor Cnty. Washington v. IDACORP Inc.*, 379 F.3d 641, 647 (9th Cir. 2004) (internal quotation marks and citations omitted). This is the case here.

The federal Wiretap Act, as amended by ECPA in 1986, comprehensively regulates privacy claims concerning electronic communications. *See* 18 U.S.C. §§ 2510-22.[7] As a matter of law, this detailed regulatory scheme setting forth privacy standards for electronic communications leaves no room for supplementary state regulation. *See Bunnell*, 567 F. Supp. 2d at 1154-55 (dismissing plaintiff's state wiretap act claims because "[t]he scheme of the ECPA is very comprehensive: it regulates private parties' conduct, law enforcement conduct, outlines a scheme covering both types of conduct and also includes a private right of action for violation of the statute. As such, it is apparent to this Court that Congress left no room for supplementary state regulation.") (internal quotation marks and citations omitted); *cf. Quon*, 445 F. Supp. 2d at 1138 (holding that ECPA preempts state law invasion of privacy and constitutional law claims because "[t]he intricacies of the regulatory scheme crafted by the ECPA (and the SCA) are fairly

[7] Section 2511 proscribes the circumstances in which private parties and government officials may intercept, disclose or use electronic communications. 18 U.S.C. § 2511(1). The Act also sets forth in detail numerous instances where interception is lawful, notwithstanding the prohibitions contained in Section 2511(1). 18 U.S.C. § 2511(2). Violators of Section 2511 face criminal penalties, *see* 18 U.S.C. § 2511(4), and suit by the federal government for the interception of certain satellite and radio communications, *see* 18 U.S.C. § 2511(5). Sections 2512 and 2513 regulate the manufacture and possession of interception devices. *See* 18 U.S.C. §§ 2512-13. Sections 2515 through 2519 describe the manner in which electronic communications may be lawfully intercepted and used by government officials. *See* 18 U.S.C. §§ 2515-19. And Section 2520 provides a private right of action for any person whose electronic communication has been unlawfully intercepted. *See* 18 U.S.C. § 2520.

comprehensive: Regulating private parties' conduct, law enforcement efforts to uncover stored electronic communications, and devising a fairly complicated scheme to accomplish both, including a private right of action for violations of the statute's provisions.").

The original Wiretap Act was Congress's response, "in a comprehensive fashion," to an evolving need to provide for the security of communications while also authorizing certain interceptions. S. Rep. No. 99-541, at 2. When it enacted ECPA in 1986, Congress extended the Wiretap Act to include a pervasive legal regime governing electronic communications, including radio communications. *See Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001). Congress could not have intended to allow the states to disrupt that effort by enforcing their own disparate—and conflicting—set of laws and remedies regarding electronic-communications privacy. [8] And because the patchwork of state laws plaintiffs assert here do just that, the claims based on those laws should be dismissed with prejudice under the doctrine of field preemption.

3. Plaintiffs' State Wiretap Claims Are Barred Based On Conflict Preemption.

Plaintiffs' state wiretap claims are also barred based on conflict preemption. The federal government authorized the unlicensed radio spectrum for public use to encourage innovation in wireless communications technology without governmental interference. Plaintiffs' state wiretap claims would erect an "obstacle to the accomplishment and execution of the full purposes and objectives" of that policy. *Silvas*, 514 F.3d at 1004 (citation omitted). For many years, the FCC prohibited public use of unlicensed radio frequencies altogether. Rubin Dec., Ex. 16 (FCC Docket No. 81-413 at 1). But in 1985, the FCC opened up three bands of the spectrum for unlicensed use, including the 2.4 GHz band over which Wi-Fi network routers broadcast. *Id*. at 9. The Commission did so to encourage "rapid development" of civilian wireless technologies with minimal governmental interference. *Id*. at 11. The following year, Congress decided that all

[8] Some of the state laws vary the available civil remedies. *See* M.S.A. § 626A.01, *et seq*.; Ohio R.C. § 2933.51, *et seq*.; SC St. § 17-30-10, *et seq*.; 18 Pa C.S.A. § 5703, *et seq*. And still others are antiquated and mirror the pre-ECPA federal Wiretap Act. *See* MO St. § 542.200, *et seq*.; N.R.S. § 200.610, *et seq*.; Tex. Civ. Prac. & Rem. § 123.001, *et seq*.

radio transmissions, including those sent over unlicensed bands should be considered "readily accessible to the general public" unless one of five specific exceptions applied. 18 U.S.C. § 2511(2)(g)(i); 18 U.S.C. § 2510(16)(A)-(E). Congress easily could have prohibited the acquisition of radio broadcasts sent over unlicensed radio bands, but elected not to.

Given this framework, a state may not make unlawful the acquisition of unencrypted broadcasts sent over the unlicensed spectrum. To do so would thwart the federal policy of encouraging open communications on that spectrum, without technology-stifling government intrusion. Indeed, Congress understood that a balance needed to be struck between open, free radio networks and communication privacy. To resolve those competing interests, Congress made clear that users of the public spectrum who desired privacy needed to configure their systems in a manner to make their broadcasts "not readily accessible" by using encryption, scrambling, or non-public modulation techniques. That careful balance would be undone by state laws that make unlawful the very acts that Congress has approved. *See Buckman Co. v. Plaintiffs' Legal Comm.*, 531 U.S. 341, 353 (2001) (state laws preempted because they "would exert an extraneous pull on the scheme established by Congress"); *Quon*, 445 F. Supp. 2d at 1137 (finding "great appeal" in argument that a defendant "cannot be held liable for something . . . that is specifically condoned" by ECPA).

***

Plaintiffs' state wiretap claims fail based on express, field, and conflict preemption. They should be dismissed with prejudice.

C. Plaintiffs' Section 17200 Claim Should Be Dismissed.

Section 17200 prohibits unlawful, unfair, or fraudulent business practices. "A plaintiff alleging unfair business practices under Section 17200 must state with reasonable particularity the facts supporting the statutory elements of the violation." *Quintero Family Trust v. OneWest Bank, F.S.B.*, No. 09-cv-1561, 2010 WL 392312, at *12 (S.D. Cal. Jan. 27, 2010) (internal citations and quotation marks omitted). Plaintiffs' Section 17200 claim should be dismissed for three independent reasons: (1) federal law preempts plaintiffs' state law claims; (2) plaintiffs

have failed to plead facts stating a substantive Section 17200 violation; and (3) plaintiffs have not alleged adequately the loss of "money or property" to demonstrate Proposition 64 standing.

1. Plaintiffs' Section 17200 Claim Is Preempted.

Just like the state wiretap claims, plaintiffs' Section 17200 claim is preempted by federal law because it concerns the alleged interception of radio communications. Federal law provides the exclusive avenue for such claims. *See, supra*, Section III.B.

2. Plaintiffs Have Not Stated A Section 17200 Claim.

In any event, plaintiffs have failed to plead facts to support a Section 17200 claim. Plaintiffs assert claims under the "unlawful" and "unfair" prongs of California's unfair competition law ("UCL"). CCAC ¶¶ 136-37. The "unlawful" prong necessarily fails because, for the reasons stated above, Google's collection of Wi-Fi Radio Broadcasts from open, unencrypted Wi-Fi networks was not unlawful. *See Kariguddaiah v. Wells Fargo Bank, N.A.*, No. C 09-5716, 2010 WL 2650492, at *7 (N.D. Cal. July 1, 2010) (dismissing § 17200 claim due to plaintiff's failure to state a claim for either breach of contract or wrongful foreclosure upon which the § 17200 claim was based); *Berryman v. Merit Property Mgmt. Inc.*, 152 Cal. App. 4th 1544, 1554 (2007) ("Thus, a violation of another law is a predicate for stating a cause of action under" the "unlawful" prong).

The basis for plaintiffs' invocation of the "unfair" prong is difficult to discern, and that is reason enough to dismiss their UCL claim. *See Schulken v. Washington Mut. Bank*, No. 09-02708, 2009 WL 4173525, at *8 (N.D. Cal. Nov. 19, 2009) ("the Court finds that Plaintiffs' UCL claim fails because Plaintiffs have not alleged sufficient facts to give Defendants notice of what fraudulent or unfair conduct is being asserted against them"). Regardless, the CCAC does not remotely plead facts that would support a UCL claim under that theory.

The law is unsettled regarding how to evaluate the "unfair" prong. Some courts have held that a plaintiff must plead facts showing a violation of a public policy that is "tethered to specific constitutional, statutory, or regulatory provisions." *Bardin v. Daimlerchrysler Corp.*, 136 Cal. App. 4th 1255, 1260-61 (2006). Other courts have articulated a more amorphous test under which conduct that is "immoral, unethical, oppressive, unscrupulous or substantially injurious to

consumers" may support liability. *Id*. at 1260. It does not matter which test the court employs here because plaintiffs have not stated a claim under either one.

Google's conduct was lawful under the Wiretap Act. It therefore cannot be immoral, unethical, oppressive, unscrupulous or violative of public policy. *See, e.g.*, *Facebook, Inc.*, 2010 WL 3291750, at *15; *Sanders v. Apple Inc.*, 672 F. Supp. 2d 978, 989 (N.D. Cal. 2009). That leaves a single issue: whether the CCAC alleges facts supporting a claim that Google's actions were "substantially injurious to consumers." It does not. Plaintiffs merely allege that Google collected and stored payload data sent from open, unencrypted Wi-Fi networks and for a time stored that data on its servers. They do not claim that Google used that information or disclosed it to anyone. The CCAC does not describe any injury to consumers, let alone a substantial one. *See, e.g.*, *Spiegler v. Home Depot U.S.A., Inc.*, 552 F. Supp. 2d 1036, 1044-47 (C.D. Cal. 2008); *Birdsong*, 2008 WL 7359917, at *6 (rejecting "conjectural or hypothetical" injury claims under Section 17200). Plaintiffs' Section 17200 claim should be dismissed for failing to plead facts that would support liability.

3. Plaintiffs Have Not Demonstrated Proposition 64 Standing.

Plaintiffs' UCL claim also fails based on their failure to demonstrate Proposition 64 standing. Section 17200 "requires a plaintiff to establish that it has 'suffered injury in fact *and* has lost money or property.'" *Walker v. Geico Gen. Ins. Co.*, 558 F.3d 1025, 1027 (9th Cir. 2009) (quoting Cal. Bus. & Prof. Code § 17204) (emphasis added); *Robinson v. HSBC Bank USA*, -- F. Supp. 2d --, 2010 WL 3155833, at *9 (N.D. Cal. Aug. 9, 2010) (dismissing with prejudice Section 17200 claim where plaintiffs "have not and cannot allege lost 'money or property' and thus have no standing."). The CCAC does not allege facts meeting this requirement.

Plaintiffs do not assert that they lost money, but plead in conclusory fashion that they lost "property." CCAC ¶ 138. The only "property" referenced in the CCAC is the data that plaintiffs broadcast over open, unencrypted Wi-Fi networks. Plaintiffs voluntarily sent out that information over a radio network without any plausible expectation of it being returned. Those broadcasts have not been "lost" under any definition of the term. *See Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (rejecting claim of "loss of property" under Section 17200 over

personal information contained on a stolen laptop and noting the lack of authority for the proposition that the "unauthorized release of personal information constitutes a loss of property"). Nor is plaintiffs' claim of entitlement to statutory damages sufficient to confer Section 17200 standing. *See Butler v. Adoption Media, LLC*, 486 F. Supp. 2d 1022, 1062 (N.D. Cal. 2007). Plaintiffs have not demonstrated the loss of "money" or "property," and their Section 17200 claim therefore should be dismissed.

Finally, plaintiffs would not be able to demonstrate the loss of "money" or "property" in an amended pleading. Their basic contention is that Google acquired payload data from open, unencrypted Wi-Fi networks. There are no allegations of subsequent use or disclosure of the payload collected. Nor is there any allegation from any plaintiff of actual injury resulting from Google's conduct. On these facts, it would be impossible for plaintiffs to assert that they somehow lost "money" or "property" because their Wi-Fi transmissions were collected and sat on Google's servers. *See Bell v. Acxiom Corp*., No. 4:06CV00485, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006) (dismissing privacy class action where plaintiff failed to allege any tangible injury resulting from access to database containing consumer information); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684 (S.D. Ohio 2006) (same). Accordingly, their Section 17200 claim should be dismissed with prejudice. *See, e.g.*, *Birdsong v. Apple, Inc.*, 590 F.3d 955, 961-62 (9th Cir. 2009).

IV. CONCLUSION

For the foregoing reasons, Google respectfully requests that the Court dismiss the CCAC with prejudice and enter judgment in Google's favor.

Dated: December 17, 2010

Attorneys for Defendant Google Inc.

By: /s/ Michael Rubin

David H. Kramer
Michael H. Rubin
Bart E. Volkmer
Caroline E. Wilson
Wilson Sonsini Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100
Email: mrubin@wsgr.com

APPENDIX A

Appendix A: Plaintiffs' Prior Statements Regarding Their Use of Open, Unencrypted Wi-Fi Networks

Rubin Dec. Ex. No.	Court Filing in which state-ment was made	Plaintiff Name	Statement
6	*Van Valin Complaint* (filed 5/17/10) D. Or. Case No: 3:10-cv-00557-MO	Van Valin, Vicki	¶4: "During the class period, Van Valin used and maintained and used [sic] an open wireless internet connection ('WiFi connection') at her home."
7	*Colman Complaint* (filed 5/26/10) D.D.C. Case No.: 1:10-cv-00877-JDB	Colman, Jeffrey	¶5: "During all times relevant herein, Colman used and maintained an open wireless internet connection at his home . . ."
8	*Keyes Complaint* (filed 5/28/10) D.D.C. Case No.: 1:10-cv-00896-JDB	Keyes, Patrick	¶1: "Defendant intentionally intercepted electronic communications sent or received on open wireless connection ("WiFi connections") by the Class . . ."
9	*Carter Complaint* (filed 6/2/10) E.D. Pa. Case No.: 2:10-cv-02649-JHS	Carter, Stephanie & Russell	¶6: "Plaintiffs Stephanie and Russell Carter, husband and wife, are residents of Philadelphia, PA. During all relevant times they used an open Wi-Fi network at their residence." ¶7: "Plaintiffs used their open, unencrypted internet connection to transmit and receive personal and private data."
10	*Berlage First Amended Complaint* (filed 6/3/10) N.D. Cal. Case No.: 5:10-cv-02187-JW (PVTx)	General Allegations	¶15: "[P]laintiffs Berlage, Linsky, and Fairbanks maintained open wireless network and internet connections at their residences, while plaintiff Bergin maintained a closed or encrypted wireless network and internet connection."[1]
		Berlage, Matthew	¶5: "Mr. Berlage used and maintained at all times relevant and material hereto an unencrypted wireless internet connection at his home . . . As used herein, 'unencrypted' is intended to mean that a 'key' was not needed to decode intercepted communications . . ."
		Linsky, Aaron	¶6: "Mr. Linsky used and maintained at all times relevant and material hereto an unencrypted wireless internet connection at his home . . . As used herein, 'unencrypted' is intended to mean that a 'key' was not needed to decode intercepted communications . . ."
		Fairbanks, James	¶7: "Mr. Fairbanks used and maintained at all times relevant and material hereto an unencrypted wireless internet connection at his home . . . As used herein, 'unencrypted' is intended to mean that a 'key' was not needed to decode intercepted communications . . ."

[1] Plaintiff Denise Bergin was excluded from the Consolidated Class Action Complaint ("CCAC").

Appendix A: Plaintiffs' Prior Statements Regarding Their Use of Open, Unencrypted Wi-Fi Networks

Rubin Dec. Ex. No.	Court Filing in which state-ment was made	Plaintiff Name	Statement
11	*Locsin Complaint* (filed 7/26/10) N.D. Cal. Case No: 5:10-cv-03272-PVT	General Allegations	¶31: "At all relevant times, Plaintiffs have used open Wi-Fi network at their place of residence which are the type of networks susceptible to unauthorized access by Google Street View vehicles."
		Locsin, Jennifer	¶10: "Plaintiff Jennifer Locsin is a resident of Contra Costa County, California. During all relevant times, she used an open Wi-Fi network at her residence . . ."
		Blackwell, James	¶11: "Plaintiff James Blackwell is a resident of Alameda County, California. During all relevant times, he used an open Wi-Fi network at his residence . . ."
12	*Joffe Complaint* (filed 9/9/10) N.D. Cal. Case No.: 5:10-cv-04007-JW	Joffe, Benjamin	¶3: "During all times relevant herein, Plaintiff used and maintained an open, unencrypted wireless internet connection at his home."
13	*Marigza Complaint* (filed 9/10/10) N.D. Cal. Case No.: 5:10-cv-04084-JW	General Allegations	¶21: "Plaintiffs Lilla Marigza, Wesley Hartline, David Binkley, and Blake Carter (collectively 'Class and Subclass Representative Plaintiffs') each consistently maintained an open wireless network at their homes since and through the time Google began collecting individuals' payload data with its GSV vehicles."
		Marigza, Lilla	¶3: "Plaintiff Lilla Marigza is an individual residing in Davidson County, Tennessee. During the class period, Mrs. Marigza used and maintained an open wireless connection ('WiFi connection') at her home."
		Hartline, Wesley	¶4: "Plaintiff Wesley Hartline is an individual residing in Davidson County, Tennessee. During the class period, Mr. Hartline used and maintained an open wireless connection ('WiFi connection') at his home."
		Binkley, David	¶5: "Plaintiff David Binkley is an individual residing in Davidson County, Tennessee. During the class period, Mr. Binkley used and maintained an open wireless connection ('WiFi connection') at his home."
14	*Davis Complaint* (filed 9/10/10) N.D. Cal. Case No.: 5:10-cv-04079-JW	General Allegations	¶31: "At all relevant times, Plaintiffs have used an open Wi-Fi network at their place of residence . . ."
		Davis, Bertha	¶10: "Plaintiff BERTHA DAVIS is a resident of Solano County, California. During all relevant times, she used an open Wi-Fi network at her residence . . ."
		Taylor, Jason	¶11: "Plaintiff JASON TAYLOR is a resident of Alameda County, California. During all relevant times, he used an open Wi-Fi network at his residence . . ."

Appendix A: Plaintiffs' Prior Statements Regarding Their Use of Open, Unencrypted Wi-Fi Networks

Rubin Dec. Ex. No.	**Court Filing in which state-ment was made**	**Plaintiff Name**	**Statement**
15	*Myhre First Amended Complaint* (filed 9/17/10) W.D. Wa. Case No. 2:10-cv-01444-JPD	Myhre, Eric	¶19: ""Plaintiff Eric Myhre is a United States citizen and resident of Seattle, Washington. Plaintiff used and maintained an unencrypted wireless internet connection at his home . . ."
Dkt. No. 18 (not included in Rubin Dec.)	*Joint Case Management Statement* (filed 9/3/10) N.D. Cal. Case No. 10-md-02184 -JW	Plaintiffs	¶2: "As the JPML stated in its Transfer Order, the principal factual issues 'aris[e] out of allegations that Google intentionally intercepted electronic communications sent or received over class members' open, non-secured wireless networks.'"