2

34

5

7

8

10

11 12

13

14

15 16

18

17

19 20

21

23

22

24

2526

27

28

# IN THE UNITED STATES DISTRICT COURT

### FOR THE NORTHERN DISTRICT OF CALIFORNIA

### SAN FRANCISCO DIVISION

In re Google Inc. Street View Electronic Communications Litigation

NO. C 10-MD-02184 JW

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS WITH LEAVE TO AMEND

## **I. INTRODUCTION**

Plaintiffs<sup>1</sup> bring this putative class action against Google, Inc. ("Defendant"), alleging three causes of action for violation of the federal Wiretap Act, 18 U.S.C. §§ 2511, et seq., violation of Cal. Bus. & Prof. Code §§ 17200, et seq., and violation of various state wiretap statutes. Plaintiffs allege that Defendant intentionally intercepted data packets, including payload data, from Plaintiffs' Wi-Fi networks utilizing specially designed packet sniffer software installed on Defendant's Google Street View vehicles.

Presently before the Court is Defendant's Motion to Dismiss.<sup>2</sup> The Court conducted a hearing on March 21, 2011. Based on the papers submitted to date and oral argument, the Court GRANTS in part and DENIES in part Defendant's Motion to Dismiss.

Plaintiffs are Patrick Keyes, Matthew Berlage, Aaron Linsky, James Fairbanks, Jeffrey Colman, John Redstone, Karl Schulz, Dean Bastilla, Vicki Van Valin, Stephanie and Russell Carter, Danielle Reyas, Bertha Davis, Jason Taylor, Jennifer Locsin, James Blackwell, Rich Benitti, Benjamin Joffe, Lilla Marigza, Wesley Hartline, David Binkley and Eric Myhre.

<sup>&</sup>lt;sup>2</sup> (Defendant Google Inc.'s Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint, hereafter, "Motion," Docket Item No. 60.)

# II. BACKGROUND

### A. <u>Factual Allegations</u>

In a Consolidated Class Action Complaint filed on November 8, 2011,<sup>3</sup> Plaintiffs allege as follows:

Plaintiffs are individuals who reside in various states,<sup>4</sup> and who maintained a Wi-Fi network in their homes that was not readily accessible to the general public and used the Wi-Fi connection to send and receive various types of payload data, including usernames, passwords and personal emails. (CCAC ¶¶ 18-38.) Each of Plaintiffs' homes can be seen depicted on Google Maps and Google Street View. (Id.) Defendant Google develops and hosts a broad range of Internet-based services and is incorporated under the laws of Delaware with its principal place of business in Mountain View, California. (Id. ¶ 39.)

Defendant launched Google Street View on May 25, 2007 in several select cities across the United States. (CCAC ¶ 55.) In the last three years, Google Street View has expanded broadly and now includes more cities and rural areas in the United States, and has expanded worldwide into more than 30 countries. (Id.) Google Street View is a feature embedded within Defendant's Google Maps program that offers panoramic views of various positions along streets using photos taken from a fleet of specially adapted vehicles commonly known as Google Street View vehicles. (Id. ¶¶ 54, 55.) Each Google Street View vehicle is equipped with nine directional cameras to capture 360 degree views of the streets and 3G/GSM/Wi-Fi antennas with custom-designed software for the capture and storage of wireless signals and data. (Id. ¶ 55.) Additionally, Defendant used smaller vehicles, commonly known as Google Trikes, also outfitted with the cameras and Wi-Fi equipment, to capture photo and Wi-Fi data from areas inaccessible to cars. (Id. ¶ 58.) While Defendant issued press releases to the public to disclose its intent to utilize the vehicles in order to

<sup>&</sup>lt;sup>3</sup> (Consolidated Class Action Complaint, hereafter, "CCAC," Docket Item No. 54.)

<sup>&</sup>lt;sup>4</sup> Plaintiffs are citizens and residents of Washington, D.C.; Ohio; Pennsylvania; Nevada; Tennessee; Washington; California; Illinois; and Oregon. (CCAC ¶¶ 18-38.)

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

capture photo data, Defendant failed to disclose its intent to also capture Wi-Fi data. (<u>Id.</u> ¶ 56.)

In 2006, prior to the launch of the Google Street View vehicles, Defendant's employee engineers intentionally created a data collection system that included code that sampled, collected, decoded and analyzed all types of data broadcast through Wi-Fi connections. (CCAC ¶¶ 60-61.) This data collection system is commonly known as a packet analyzer, wireless sniffer, network analyzer, packet sniffer or protocol analyzer. (Id. ¶ 61.) Defendant authorized inclusion of this wireless sniffer technology into its Google Street View vehicles and even sought to patent the process. (Id.  $\P$  65.) The wireless sniffer secretly captures data packets as they stream across Wi-Fi connections and then decodes or decrypts the data packet and analyzes the contents. (Id. ¶ 62.) In order to view the contents of the data packets captured by the wireless sniffer in a readable form, the packets must be stored on digital media and then decoded using crypto-analysis or a similarly complicated technology. (Id. ¶ 63.) As such, the data packets are not readable by the general public absent this sophisticated decoding and processing technology. (Id. ¶ 64.) Defendant has admitted to storing this data on their servers. (Id.  $\P$  6.) The content of the data packets collected by Defendant included Plaintiffs' SSID information (the Wi-Fi network name), MAC address (the ID number of the Wi-Fi network's hardware), usernames, passwords and personal emails. (Id.  $\P\P$  66, 69.)

On April 27, 2010, in response to an inquiry from a European privacy authority, Defendant posted an entry explaining that it had collected SSIDs and MAC addresses. (CCAC ¶ 69.) However, at that time, Defendant claimed to have not collected any payload, or content data from the packets. (Id. ¶ 70.) On May 14, 2010, following a request by the privacy authority to audit packet data collected by Defendant, Defendant admitted to collecting "fragmentary" samples of "publicly broadcast" payload data from open (i.e., non-password-protected) Wi-Fi networks and that, through this conduct, it had collected about 600 gigabytes of data from more than 30 countries. (Id. ¶¶ 71-72, 110.) Prior to May 14,

18

19

20

21

22

23

24

25

26

27

28

1

2

3

4

5

6

7

8

9

2010, Plaintiffs were unaware of and could not have discovered the existence of Defendant's unlawful conduct. (Id. ¶¶ 100-10.) On June 9, 2010, Defendant admitted that it had been collecting Wi-Fi data in the United States via Google Street View vehicles since 2007. (Id. ¶ 80.) On July 9, 2010, Defendant issued an apology on its Official Google Australia Blog where it admitted to intercepting the data in an attempt to improve Defendant's locationbased services, e.g., search and maps. (Id. ¶ 100.) In October 2010, Defendant was forced to admit, following continuing investigations, that it had intercepted whole emails, usernames, passwords and other private data. (Id. ¶ 77.)

On the basis of the allegations outlined above, Plaintiffs allege three causes of action: (1) violation of the federal Wiretap Act, 18 U.S.C. §§ 2511, et seq.; (2) violation of Cal. Bus. & Prof. Code §§ 17200, et seq.; and (3) violation of various state wiretap statutes. (CCAC at 28-31.)

### В. **Procedural History**

On August 17, 2010, the United States Judicial Panel on Multidistrict Litigation transferred eight pending actions to this Court pursuant to 28 U.S.C. § 1407. (See Docket Item No. 1.) On October 18, 2010, the Court appointed Jeffrey Kodoff of Spector Roseman Kodroff & Willis, P.C. and Daniel Small of Cohen Milstein Sellers & Toll, PLLC as Interim Class and Co-Lead Counsel and Elizabeth Cabraser of Lieff Cabraser Heimann & Bernstein, LLP as Interim Class and Liaison Counsel. (See Docket Item No. 47.) On November 8, 2010, Plaintiffs filed their Consolidated Class Action Complaint. (See CCAC.)

On March 21, 2011, the Court conducted a hearing on Defendant's Motion to Dismiss. That same day, the Court issued an Order directing the parties to submit supplemental briefs addressing three questions: (1) what "radio communication" means within the purview of the Wiretap Act; (2) whether wireless home internet networks are "radio communications" within the purview of the Wiretap Act's usage of that term; and (3) whether cellular telephone calls constitute "radio communications" as intended by Congress when drafting the Wiretap Act and, if so, whether such technology properly fits within any of the five enumerated exceptions to the definition of "readily accessible to the general public" as outlined in Section 2510(16). (See Docket Item No. 73.) On

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

April 11, 2011, the parties timely filed their Supplemental Briefs. (See Docket Item Nos. 79, 80.) Also on April 11, 2011, the Electronic Privacy Information Center filed a Brief for Amicus Curiae in support of Plaintiffs. (See Docket Item No. 80.)

Presently before the Court is Defendant's Motion to Dismiss.

### III. STANDARDS

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a complaint may be dismissed against a defendant for failure to state a claim upon which relief may be granted against that defendant. Dismissal may be based on either the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory. Balistreri v. Pacifica Police Dep't, 901 F.2d 696, 699 (9th Cir. 1990); Robertson v. Dean Witter Reynolds, Inc., 749 F.2d 530, 533-34 (9th Cir. 1984). For purposes of evaluating a motion to dismiss, the court "must presume all factual allegations of the complaint to be true and draw all reasonable inferences in favor of the nonmoving party." Usher v. City of Los Angeles, 828 F.2d 556, 561 (9th Cir. 1987). Any existing ambiguities must be resolved in favor of the pleading. Walling v. Beverly Enters., 476 F.2d 393, 396 (9th Cir. 1973).

However, mere conclusions couched in factual allegations are not sufficient to state a cause of action. Papasan v. Allain, 478 U.S. 265, 286 (1986); see also McGlinchy v. Shell Chem. Co., 845 F.2d 802, 810 (9th Cir. 1988). The complaint must plead "enough facts to state a claim for relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). A claim is plausible on its face "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009). Thus, "for a complaint to survive a motion to dismiss, the non-conclusory 'factual content,' and reasonable inferences from that content, must be plausibly suggestive of a claim entitling the plaintiff to relief." Moss v. U.S. Secret Serv., 572 F.3d 962, 969 (9th Cir. 2009). Courts may dismiss a case without leave to amend if the plaintiff is unable to cure the defect by amendment. Lopez v. Smith, 203 F.3d 1122, 1129 (9th Cir. 2000).

26

27

28

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

### IV. DISCUSSION

Defendant moves to dismiss Plaintiffs' Complaint on the grounds that: (1) Plaintiffs have failed to plead that their Wi-Fi broadcasts were not "readily accessible" and thus, Defendant is entitled to exemption from liability under 18 U.S.C. § 2511(2)(g)(i), one of the Wiretap Act's exemptions ("exemption G1"); (2) Plaintiffs' claims based on state law wiretap statutes are preempted by the Wiretap Act and, alternatively, fail to state a claim; and (3) Plaintiffs' "unlawful" and "unfair" Cal. Bus. & Prof. Code §§ 17200 claims are also preempted by the Wiretap Act and, alternatively, fail to state a claim or plead standing under Proposition 64. (Motion at 5-19.) Plaintiffs respond that dismissal is improper as: (1) the Wiretap Act's statutory definition of "readily accessible" relied on by Defendant solely applies to "radio communications" under § 2511(2)(g)(ii) ("exemption G2") and is, thus, inapplicable to "electronic communications" under exemption G1 and the ordinary meaning of "readily accessible" should be used; (2) additionally, exemption G1 only applies to unlawful interception and access, and Plaintiffs allege that Defendant further used and disclosed the intercepted communications; (3) the state wiretap statutes are not preempted by the Wiretap Act either expressly, by field preemption, or by conflict; and (4) claims under Cal. Bus. & Prof. Code §§ 17200, et seq., are not preempted by the Wiretap Act as they are qualitatively different and are properly pleaded. (Opp'n at 3-25.) The Court addresses each ground in turn.

## A. Wiretap Act

Defendant contends that Plaintiffs' Wi-Fi broadcasts were "readily accessible to the general public," per the statutory definition provided in Section 2510(16) of the Wiretap Act, such that exemption G1 obviates Defendant's liability for any alleged interceptions. (Motion at 5-12.) Plaintiffs respond that the Section 2510(16) definition of "readily accessible to the general public" applies solely to "radio communications," as specified, and thus would only apply to exemption G2 ("radio communications") and not exemption G1 ("electronic communications"). (Opp'n at 2-10.)

The Wiretap Act, 18 U.S.C. § 2511(1) provides a private right of action against:

(1) Except as otherwise specifically provided in this chapter any person who-

27

28

2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

(a)	intentionally intercepts, endeavors to intercept, or procures any other person
	to intercept or endeavor to intercept, any wire, oral, or electronic
	communication:

- (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
- (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; . . . .

However, Section 2511(2) provides exemptions to Section 2511(1)'s private right of action:

- (g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--
  - (i) 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;
  - (ii) to intercept any radio communication which is transmitted--
    - (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles or persons in distress;
    - (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
    - (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
    - (IV) by any marine or aeronautical communications system; . . .

Section 2510(16) provides the sole definition in the Wiretap Act for "readily accessible to the general public":

- (16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not--
  - (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 communication by radio; . . . .

18 U.S.C. § 2510.

The matter before the Court presents a case of first impression as to whether the Wiretap Act imposes liability upon a defendant who allegedly intentionally intercepts data packets from a

wireless home network. The case also presents a novel question of statutory interpretation as to how the definition in Section 2510(16) of "readily accessible to the general public" modifies exemption G1, if at all.

In establishing the standard principles of statutory construction, the Supreme Court has held that the starting point at which courts should discern congressional intent is always the existing statutory text. Lamie v. U.S. Trustee, 540 U.S. 526, 534 (2004). Unless a court finds the existing statutory text such that a plain meaning interpretation would lead to absurd results, the court is bound to enforce the existing text according to its terms. Id. (citing Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A., 530 U.S. 1, 6 (2000)). "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." K-Mart Corp. v. Cartier, Inc., 486 U.S. 281, 291 (1988). One measure of ambiguity is that the statutory text at issue is fairly capable of more than one interpretation. Chickasaw Nation v. United States, 534 U.S. 84, 90 (2001). Should a court find the statutory text ambiguous or should a plain text reading fail to yield a definitive interpretation, a court may then turn to the legislative history in order to add context to the statute. SEC v. McCarthy, 322 F.3d 650, 655 (9th Cir. 2003).

### 1. Plain Text Reading

In this case, Congress has not expressly declared its intent as to how Section 2510(16) should apply to exemption G1 in the plain text of the statute, nor has Congress defined "radio communication" anywhere within the Act. As Congress has not provided a definition for "radio communication" within the confines of the Act, the Court first attempts to discern the ordinary and plain meaning of the term from the context of its use, from dictionary references and from Congress' use of similar terms within the Act.

### a. Statutory Text

Section 2510(16) defines "readily accessible to the general public" as it pertains specifically to "radio communication" by first establishing a presumption of ready accessibility and then defining five types of radio communications which would be expressly excluded from that

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

presumption. Notably, none of the five express exemptions from ready accessibility under Section 2510(16) specifically address wireless internet technologies, as the list predominantly addresses radio broadcast technologies. See 18 U.S.C. §§ 2510(16)(A)-(E). In addition to Section 2510(16), the Act uses the term "radio communication" on three other occasions. First, Section 2511(2)(g), which provides five exceptions to liability for intentional interception of wire, oral or electronic communications, makes it lawful to intentionally intercept:

[A]ny radio communication which is transmitted—

- by any station for the use of the general public, or that relates to ships, aircraft, (I)vehicles, or person in distress;
- by any governmental, law enforcement, civil defense, private land mobile, or public (II)safety communications system, including police and fire, readily accessible to the general public;
- by a station operating on an authorized frequency within the bands allocated to the (III)amateur, citizens band, or general mobile radio services; or
- by any marine or aeronautical communications system; . . . . (IV)

18 U.S.C. § 2511(2)(g)(ii). Second, Section 2511(2)(g) also makes it lawful "for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted." 18 U.S.C. § 2511(2)(g)(v). Finally, Section 2511(5)(a)(i)(B) makes unlawful and authorizes a right of action for the federal government to bring suit in federal court for the interception of "a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain." 18 U.S.C. § 2511(5)(a)(i)(B). Title 47, part 74 of the rules of the Federal Communications Commission pertains to "Experimental Radio, Auxiliary, Special Broadcast and Other Program Distributional Services." 47 C.F.R. § 74. Subpart D of part 74 regulates "Remote Pickup Broadcast Stations." Id. Remote pickup broadcast stations are defined under the regulations as either a mobile or fixed "pickup broadcast transmitter, and its associated accessory equipment necessary to the radio communication function." 47 C.F.R. § 74.401.

19

20

21

22

23

24

25

26

27

28

1

2

3

4

5

The drafting of these provisions predated the spread of wireless internet technologies and, thus, the lack of any explicit reference to wireless internet technologies does not itself preclude an interpretation of "radio communications" that would include these later-developed technologies. However, the usage of "radio communication" throughout the Act does not lend itself to a broad interpretation of the term. In particular, references to "radio communication" throughout the Act predominantly pertain to and are drafted for the particular design of radio broadcast technologies, and do not address other communications technologies that transmit using radio waves. For example, Section 2511(2)(g) makes it lawful to intentionally intercept any radio communication that "that relates to ships, aircraft, vehicles, or person in distress," without reference to whether such radio communication was readily accessible to the general public and not scrambled or encrypted. Should the Court interpret radio communication so broadly within the Act to include such technologies as wireless internet and cellular phones, this exception could lead to absurd results. Specifically, pursuant to this interpretation, an unauthorized intentional monitoring of a cellular phone call could be lawful should the content of the communication relate to vehicles or persons in distress, but unlawful otherwise. Further, Section 2511(2)(g) makes it lawful to intentionally intercept any radio communication transmitted by "any marine or aeronautical communications system," which could lead to equally arbitrary results when applying the exception to communications technologies other than radio broadcast technologies, e.g., a Wi-Fi network aboard an airplane.

### b. Dictionary Reference

Gleaning a plain meaning reading of "radio communication" from dictionary references is equally as inconclusive. The Oxford Dictionaries Online ("ODO") defines "radio" as "[t]he transmission and reception of electromagnetic waves of radio frequency, especially those carrying sound messages." Further, the ODO lists a number of more specific definitions for "radio": (1) "the activity or industry of broadcasting sound programs"; (2) "radio programs"; (3) "an apparatus for receiving radio programs"; (4) "an apparatus capable of both receiving and transmitting radio messages between individuals, ships, planes, etc."; (5) "... a broadcasting station or channel." The ODO defines "communication," in pertinent part, as "the imparting or exchanging of information or

news." However, the ODO, Merriam-Websters and the Oxford English Dictionary do not contain any definition for "radio communication" and, thus, fail to provide an authoritative interpretation for the compound formulation of the two words. On one hand, Congress could have intended "radio communication" to simply combine the definition of "radio" with the definition of "communication," thereby creating a compound that incorporates all communications transmitted using radio waves. Yet, on the other hand, Congress could have intended the compound of "radio" and "communication" to denote communications that involved a radio apparatus or a communication that solely involved the transmission of sound over radio waves. Moreover, should Congress have intended the compound term "radio communication" to mean simply "communication by radio waves," it could have so specified. Rather, Congress chose to use the compound term, "radio communication," a term that shares a likeness with other compound terms used throughout the Act that prefix "communication" with reference to a particular form of media; each of which are provided specialized definitions within the Act. The Court now examines the statutory text to discern how Congress intended compound terms to modify the independent meaning of each word, if at all.

### c. Compound Terms

While the ECPA does not define the compound term "radio communication," the Act does provide definitions for three other compound terms that combine a form of media with the term "communication": "wire communication," "oral communication" and "electronic communication." A "wire communication," as defined by the Act, means:

[A]ny aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

<sup>&</sup>lt;sup>5</sup> <u>See</u> 18 U.S.C. § 2510(1).

<sup>&</sup>lt;sup>6</sup> <u>See</u> 18 U.S.C. § 2510(2).

<sup>&</sup>lt;sup>7</sup> <u>See</u> 18 U.S.C. § 2510(12).

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

or

18 U.S.C. § 1210(1). The Act defines "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 1210(2). Finally, an "electronic communication" is defined as:

[A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

- any wire or oral communication; (A)
- (B) any communication made through a tone-only paging device;
- any communication from a tracking device (as defined in section 3117 of this title); (C)
- (D) electronic funds transfer information stored by a financial institution in a communication system used for the electronic storage and transfer of funds . . . . 18 U.S.C. § 1210(12).

In defining these compound terms, Congress intended more refined definitions than simply combining the independent meanings of each word into a unified whole, e.g., electronic communication is not defined as any communication transmitted by electronic means. Rather, Congress provided nuanced definitions of each compound term; in part, to mitigate confusion in light of the inevitable overlap between terms. For example, electronic communication expressly includes electronic communications transmitted in whole or in part by wire, but excludes wire communications. Moreover, Congress did not define "wire communication" as any communication transmitted by wire, but limited the definition to incorporate solely "aural communications" transmitted by wire. Congress also expressly included communications transmitted in whole or in part by radio as a form of electronic communication, such that an interpretation of the compound "radio communication" as all communications by radio would render all communications technologies that transmit using radio waves electronic communications. An interpretation of "radio communication" that presumptively included all technologies that transmit over radio waves, such as cellular phones, under the purview of electronic communications and held that technology bound by Section 2510(16)'s definition of "readily accessible to the general public," would contravene Ninth Circuit precedent holding that cellular phone communications are wire communications for purposes

of the Wiretap Act.<sup>8</sup> The Ninth Circuit based its holding on the legislative history of the Act, finding that, despite the apparent wireless nature of cellular telephones, Congress intended cellular phone technology to fall into the meaning of wire communication based on the fact that cellular phones transmit the communications over wire at some point during the course of the transmission. <u>Id.</u> at 1138, n.12. Rather than a simply interpret "wire communications" as all communications by wire, the Ninth Circuit found that Congress intended compound terms that prefixed "communication" with a type of media to have specialized and, at times, counter-intuitive definitions. In this case, Congress did not provide a specialized definition of "radio communication," unlike wire, oral and electronic communication. However, such an omission does not preclude a finding that Congress intended a more sophisticated compound meaning and, as consequence, the meaning of "radio communication" remains open to multiple interpretations.

Thus, the Court finds that a plain reading of "radio communication" from the statutory text, as well as reading the text in the context of the structure and purpose of the Act, fails to yield a definitive and unambiguous result. The Court now turns to the legislative history for clarification.

### 2. Legislative History

The ECPA was passed by Congress in 1986 to amend the Omnibus Crime Control and Safe Streets Action of 1968, commonly known as the Wiretap Act, in order to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986). Prior to the amendment, Title III of the Omnibus Crime Control and Safe Streets Act provided a private right of action for interception of communications, however, the statute was expressly limited to unauthorized aural interception of wire or oral communications. <u>Id.</u> at 2. In 1986, the statute was, in the words of Senator Leahy, one of the senators who introduced the amendment, "hopelessly out of date." <u>Id.</u>

In particular, Congress intended the 1986 amendment to bring the statute in line with "technological developments and changes in the structure of the telecommunications industry." S. Rep. No. 99-541, at 2 (1986). Congress explicitly acknowledged the new privacy concerns faced by

<sup>&</sup>lt;sup>8</sup> In the Matter of the Application of the United States for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d 1132 (9th Cir. 2003).

individuals and businesses in light of developments in the personal and commercial computing
industries. <u>Id.</u> Developments of particular interest to the Senate Committee included the protection
of privacy rights in offsite data storage, the computer-to-computer transmission of this data, and
electronic mail. <u>Id.</u> In fact, the initial development of the amendment came on the heels of a 1984
interaction between Senator Leahy and the Attorney General where the Senator asked the Attorney
General if electronic mail and computer-to-computer communications were covered by the Wiretap
Act. Id. In response, the Department of Justice expressed concern that in areas of rapid
technological development, "distinctions such as [whether or not a reasonable expectation of privacy
exists] are not always clear or obvious." <u>Id.</u> at 3. To this end, Congress amended the Wiretap Act in
order to provide statutory privacy protection and a civil right of action for interceptions of electronic
communications, including, inter alia, computer-to-computer transmissions and electronic mail;
contexts in which Congress suspected the Fourth Amendment may only dubiously apply. <u>Id.</u>

Another matter of importance to Congress in the drafting of the amendment was to address concerns expressed by radio hobbyists and users of radio scanners that the amendment would impose liability upon the innocent act of scanning radio broadcast frequencies in order to reach public communications, should the hobbyist inadvertently encroach upon protected communication that shares the same spectrum, for instance a cellular phone. S. Rep. No. 99-541, at 4-5 (1986). An earlier version of the amendment, the Electronic Communications Privacy Act of 1985, S. 1667, did not include the Section 2510(16) definition of "readily accessible to the general public" and applied both exemptions G1 and G2 to "electronic communication," without any use of the term "radio communication." 131 Cong. Rec. S. 11795, at 4. Following a year of hearings, at which concerns were raised by radio hobbyists, Senator Leahy, joined by Senator Mathias, introduced a superseding version of the bill that incorporated explicit mention of "radio communication," including Section 2510(6) and reference in exemption G2, as well as a heightened mens rea requirement from "willful" to "intentional" to find criminal liability for interception. S. Rep. No. 99-541, at 3, 5 (1986); 132 Cong. Rec. S7987-04, at 18 ("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.").

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1

2

3

4

It was in light of these dual considerations that Congress drafted the text that became Sections 2510 and 2511. Section 2510(12) defines "electronic communication" as a broad category that includes "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 . . . ." 18 U.S.C. § 2510(12). As defined in the statute, a communication transmitted by radio is a specific type of electronic communication, such that exemption G1—which exempts from liability any interception of an electronic communication that is readily accessible to the general public—would exempt communications transmitted by radio as well, should those communications be "readily accessible to the general public." 18 U.S.C. § 2511(2).

However, to clarify that "intercepting traditional radio services" was not a violation of the Act in order to quiet the concerns raised by radio hobbyists, Congress added, inter alia, Section 2510(16). See, e.g., 132 Cong. Rec. S7987-04, at 18. Section 2510(16) provides a definition for "readily accessible to the general public" with respect to "radio communication" that establishes a presumption of accessibility, should the communication not fit within one of five delineated exceptions. 18 U.S.C. § 2510(16). Notably, each of the five exceptions, as well as the presumption of accessibility, are drafted for the particular technology of traditional radio broadcast mediums and do not address any broader radio-based communications technology of the time, including cellular phones. The first exception to the Section 2510(16) is for "scrambled or encrypted" communications, which the Senate Report describes as "to convert the signal into unintelligible form by means intended to protect the contents of a communication from unintended recipients." 18 U.S.C. § 2510(16)(A); S. Rep. No. 99-541, at 11 (1986). The second exception is for communications that have been "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). The Senate Report clarified that "paragraph (B) refers to spread spectrum radio communications," which was a technology that allowed for the transmission of a signal on "different frequencies where the receiving station must possess the necessary algorythm [sic] in order to reassemble the signal." S. Rep. No. 99-541, at 11 (1986). The third exception is for communications "carried on a subcarrier or other signal subsidiary to a radio

transmission," which, according to the Senate Report, included "data and background music services carried on FM subcarriers." <u>Id.</u> at 11-12. The fourth exception is for communications that are "transmitted over a communication system provided by a common carrier," excluding "tone only paging system communication." 18 U.S.C. § 2510(16)(D). The fifth exception was for communications that were transmitted on frequencies allocated under the Rules of the Federal Communications Commission for: (1) Part 25 ("Satellite Communications"); (2) subparts of Part 74 ("Experimental Radio, Auxiliary, Special Broadcast and Other Program Distributional Services"); and (3) Part 94 ("Microwave Services"). 18 U.S.C. § 2510(16)(E); 47 C.F.R. § 47(24), (74), (94).

Although the ECPA never explicitly defines "radio communication," what the legislative history and the context of the term's use in Section 2510(16) make clear is that Congress intended "radio communication" to include "traditional radio services," such that public-directed radio broadcast communication, as the technology was understood at the time, would be clearly excluded from liability under the Act. What the legislative history also reveals, however, is that Congress did not intend "radio communications" to be defined so broadly such that it would encompass all communications transmitted over radio waves. This was made explicit in the Senate Report's consideration of cellular phone technology, which also uses radio waves to transmit communications, and the clear intent to include such technology under the protections of the Act as a "wire communication" without any express limitation by Section 2510(16). S. Rep. No. 99-541, at 6, 11 (1986) ("Thus, a wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fiber optic cable or by radio—as in the case of cellular telephones . . . .").

As the legislative history demonstrates, despite the insistence of radio scanning enthusiasts, Congress stopped short of including a full exception to liability under the Act for the willful monitoring of cellular telephone calls. S. Rep. No. 99-541, at 6 (1986). According to the Senate Report, this hesitation was based on two considerations. Id. First, Congress had made willful

<sup>&</sup>lt;sup>9</sup> 132 Cong. Rec. S7987-04, 1986 WL 776264, at \*18 ("Under this revised Electronic Communications Privacy bill, cellular phones, private and public microwave services and voice or display pagers are protected against interception.").

monitoring of telephone calls illegal in the original 1968 Wiretap Act should at least part of the call
pass through a wire. <u>Id.</u> Second, the design of the cellular phone technology made intentional
monitoring of the communication more difficult than other signals commonly scanned. <u>Id.</u> Rather
than exclude cellular phone communications from the protections of the act, the Senate Committee
highlighted the possibility that the Federal Communications Commission should consider labeling
cellular phone and radio scanning equipment to alert the user that such technologies are "radio-based
communications" and, as such, intentional interception of the communication could violate the
Wiretap Act. Id.

The presumption of accessibility established in Section 2510(16) for traditional radio broadcast technology was an appropriate response to the balance being struck between particular electronic forms of communication that were designed to be public, like traditional radio broadcast, and others that were designed to be private, like cellular phone technology. <u>Id.</u> However, to apply the presumption to all communications transmitted using radio technology by interpreting "radio communication" broadly would contravene congressional intent to provide protection for technology like cellular phones, which use radio waves to transmit communications, but are architected in such a way as to be private.

Thus, the Court finds that the legislative history and text of the statute demonstrate congressional intent to apply Section 2510(16)'s definition of "readily accessible to the general public" to exemption G1, and not merely to limit the application of Section 2510(16) to "radio communications" in exemption G2. However, in light of the legislative history and text of the statute, the Court also finds that Section 2510(16)'s presumption of accessibility and the requirement that a communications technology must fit within one of five exceptions were solely intended to apply to "traditional radio services." To interpret Section 2510(16) so broadly as to apply its strict presumption of accessibility to all communications technology that uses radio waves, regardless of the technology's design, would disregard explicit congressional intent to include cellular phone technology within the protections of the Act and clear Ninth Circuit precedent, holding that cellular

For the Northern District of California

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

phone technologies are, in fact, "wire communications." Rather, for all electronic communications that could not be fairly classified as "traditional radio services," or radio broadcast technology, regardless of the technology's use of radio waves as the medium of transmission, the Court finds that Congress did not intend Section 2510(16)'s narrow definition of "readily accessible to the general public" to apply for purposes of exemption G1. The Court now turns to examine the sufficiency of the pleadings in light of these findings.

### **3. Sufficiency of the Pleadings**

Here, Plaintiffs allege in pertinent part:

Defendant intentionally intercepted electronic communications sent or received on wireless internet connections ("WiFi connections") by the Class from at least May 25, 2007 through the present . . . (CCAC ¶ 1.) Defendant intercepted the Class members' electronic communications with its Google Street View vehicles. (Id. ¶ 2.) When Defendant's engineers created the data collection system for its Google Street View vehicles, most commonly known as a packet analyzer or wireless sniffer, they intentionally included computer code in the system that was designed to and did sample, collect, decode, and analyze all types of data sent and received over the WiFi connections of class members. (Id.  $\P 4.)$ 

This data included Class members' unique, secret WiFi network identifiers (known as Service Set Identifier or SSID) and unique WiFi router numbers (Media Access Control or MAC addresses). (CCAC ¶ 4.) The data also included all or part of any personal emails, passwords, videos, audio, documents, and Voice Over Internet Protocol ("VOIP") information (collectively, "payload data") transmitted over Class members' WiFi networks in which plaintiffs had a reasonable expectation of privacy. (Id.) The WiFi networks from which the Google Street View vehicles collected payload data were not configured so that such data were reasonably accessible by the general public. (Id. ¶ 5.) Indeed, the data, as captured by the wireless sniffer, are not even readable by members of the public absent use of sophisticated decoding and processing technology. (Id.)

Based on the allegations above, the Court finds that Plaintiffs plead facts sufficient to state a claim for violation of the Wiretap Act. In particular, Plaintiffs plead that Defendant intentionally created, approved of, and installed specially-designed software and technology into its Google Street View vehicles and used this technology to intercept Plaintiffs' data packets, arguably electronic communications, from Plaintiffs' personal Wi-Fi networks. Further, Plaintiffs plead that the data packets were transmitted over Wi-Fi networks that were configured such that the packets were not readable by the general public without the use of sophisticated packet sniffer technology. Although Plaintiffs fail to plead that the wireless networks fall into at least one of the five enumerated

<sup>&</sup>lt;sup>10</sup> In the Matter of the Application of the United States for an Order Authorizing the Roving Interception of Oral Communications, 349 F.3d at 1138, n.12.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

exceptions to Section 2510(16)'s definition of "readily accessible to the general public" for radio communications, the Court finds that the wireless networks were not readily accessible to the general public as defined by the particular communication system at issue, wireless internet networks, which are not "radio communications," as the term was intended by Congress in drafting Section 2510(16).

Rather, application of the Section 2510(16) definition of "readily accessible to the general public" as narrowly defined for traditional radio broadcast technology, would be inapplicable to the determination of whether Plaintiffs' allegedly intercepted data packets from their Wi-Fi networks are readily accessible to the general public for purposes of exemption G1, despite the fact that wireless networks transmit data using radio waves. As the Court has found, Congress intended Section 2510(16)'s definition to resolve the issue of radio scanning devices used to intercept radio broadcasts by establishing a presumption that traditional radio services were "readily accessible to the general public," in accord with the design of the medium as one where most communications over that medium are intended to be public. Unlike in the traditional radio services context, communications sent via Wi-Fi technology, as pleaded by Plaintiffs, are not designed or intended to be public. Rather, as alleged, Wi-Fi technology shares a common design with cellular phone technology, in that they both use radio waves to transmit communications, however they are both designed to send communications privately, as in solely to select recipients, and both types of technology are architected in order to make intentional monitoring by third parties difficult. S. Rep. No. 99-541, at 6 (1986).

Further, applying Section 2510(16)'s narrow definition of "readily accessible to the general public" to wireless networks, a technology unknown to the 99th Congress who drafted and passed the ECPA, would contravene the primary stated purpose of the amendment, which was to update the Wiretap Act to include within the Act specific protections against intentional interceptions of computer-to-computer communications and so-called "electronic mail" or email; data Plaintiffs plead was included in the data packets intercepted by Defendant. Interpreting the ECPA such that the statute provides obscure limitations on the protection of emails and other computer-to-computer communications based on the particular medium that transmitted the electronic communication

would render the Wiretap Act, and the efforts of the 99th Congress to provide such protections, absurd. Under such an interpretation, the Act would provide a private civil right of action, and even impose criminal liability, for the interception of emails transmitted over an ethernet cable through a wired network, but would stop short at protecting those very same emails should they pass momentarily over radio waves through a Wi-Fi network established to transmit data within a home. Such an interpretation cannot pass muster in the face of an explicit limitation that Section 2510(16)'s specialized definition of "readily accessible to the general public" solely apply to "radio communications," a term undefined within the statutory text, and where the legislative history of the Act makes plain that Congress intended "radio communications" to mean traditional radio services or broadcast radio.

Defendant's contention that Plaintiffs fail to state a claim for violation of the Wiretap Act, as Plaintiffs plead that their networks were "open" and "unencrypted," is misplaced. (Motion at 8-11.) While Plaintiffs plead that their networks, or electronic communications systems, were configured such that the general public may join the network and readily transmit electronic communications across that network to the Internet, 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. Thus, the Court finds that Plaintiffs plead facts sufficient to support a claim that the Wi-Fi networks were not "readily accessible to the general public," such that exemption G1 would not apply.

Defendant's interpretation of <u>United States v. Ahrndt</u><sup>11</sup> as standing for the principle that all unencrypted wireless networks are readily accessible to the general public and, thus, any interceptions from those networks are obviated from liability under exemption G1, unduly extends the doctrine. (Motion at 10-11.) In <u>Ahrndt</u>, a neighbor was connected to the Internet via her own wireless network when her network malfunctioned and her computer automatically logged in to another open wireless network operated by the defendant. <u>Id.</u> at \*1. The defendant had administered his iTunes software as set to "share," such that other users on the same network would

<sup>&</sup>lt;sup>11</sup> No. 08-468, 2010 WL 373994 (D. Or. Jan. 28, 2010).

10 For the Northern District of California 11 12 13 14 15 16 17

1

2

3

4

5

6

7

8

9

18

19

20

21

22

23

24

25

26

27

28

be able to access all files that the defendant had stored in his iTunes libaries. Id. After being automatically logged into the defendant's wireless network, the plaintiff in Ahrndt began using her own iTunes program and noticed that the defendant's iTunes library was accessible. Id. In accessing the defendant's iTunes library, the plaintiff located a number of files containing child pornography in a subfolder within the shared directory. Id. Based on these facts, Judge King held that the plaintiff's interception was not illegal and was, in fact, "expressly lawful" under the Wiretap Act as the defendant's network and iTunes software were configured to be readily accessible to the general public. <u>Id.</u> at \*8. However, the court did not base its holding merely on the fact the defendant's network was unencrypted. <u>Id.</u> Rather, Judge King found that "defendant's conduct in operating his iTunes software with the preferences set to share, in conjunction with maintaining an unsecured wireless network router, diminished his reasonable expectation of privacy to the point that society would not recognize it as reasonable." <u>Id.</u> at \*8. Unlike in <u>Ahrndt</u>, here, Plaintiffs plead that, although the networks themselves were unencrypted, the networks were configured to prevent the general public from gaining access to the data packets without the assistance of sophisticated technology. (CCAC ¶ 5.) Thus, the Court finds that, without more, merely pleading that a network is unencrypted does not render that network readily accessible to the general public and serve to remove the intentional interception of electronic communications from that network from liability under the ECPA.

Accordingly, the Court DENIES Defendant's Motion to Dismiss Plaintiffs' First Cause of Action for violation of the Federal Wiretap Act, 18 U.S.C. §§ 2511, et seq.

### В. **State Wiretap Statutes**

Defendant moves to dismiss Plaintiffs' Third Cause of Action for violation of various state wiretap statutes on the grounds that claims under state wiretap statutes are preempted by the Federal Wiretap Act on express, field and conflict preemption grounds. (Motion at 12-16.)

"Pursuant to the Supremacy Clause of the United States Constitution, federal law can preempt and displace state law through: (1) express preemption; (2) field preemption (sometimes referred to as complete preemption); and (3) conflict preemption." Ting v. AT&T, 319 F.3d 1126, 1135 (9th Cir. 2003) (citations omitted). "Express preemption exists where Congress enacts an

explicit statutory command that state law be displaced." <u>Id.</u> (citations omitted). "Absent explicit preemptive text, we may still infer preemption based on field or conflict preemption . . . ." <u>Id.</u> A court may find that federal law displaces state law on field preemption grounds "when the federal statutory scheme is sufficiently comprehensive to infer that Congress left no room for supplementary regulation by the states." <u>Public Utility Dist. No. 1 of Grays Harbor Cty. Washington v. Idacorp.</u> <u>Inc.</u>, 379 F.3d 641, 647 (9th Cir. 2004) (citations and quotations omitted). "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." <u>Id.</u> (citations and quotations omitted). However, "[i]n all cases, congressional intent to preempt state law must be clear and manifest." <u>In re Cybernetic Services, Inc.</u>, 252 F.3d 1039, 1046 (9th Cir. 2001).

Here, the Court finds that, while the ECPA contains no express preemptive statement on the part of Congress, 12 the ECPA was intended to comprehensively regulate the interception of electronic communications such that the scheme leaves no room in which the states may further regulate. See Bunnell v. Motion Picture Ass'n of America, 567 F. Supp. 2d 1148, 1154-55 (C.D. Cal. 2007). In particular, the ECPA was enacted, in part, to provide legal certainty to users and developers of innovative communications technologies with bright line rules for liability. S. Rep. 99-541 at 4. In so regulating, Congress struck a balance between the right to the privacy of one's electronic communications against the ability of users to access communications technologies without fear of liability for inadvertent interception. S. Rep. 99-541 at 5-6. State regulation acting in addition to the ECPA might serve to obscure the legislative scheme surrounding innovative communications technologies that Congress intended to clarify through the Act, or could serve to upset the fragile balance considered by Congress between those who transmit electronic

The Court finds that Defendant's interpretation of Section 2518(10)(c) as an express preemption clause misinterprets the provision. (Motion at 13.) The legislative history supports the proposition that the provision was appended to the ECPA solely to address suppression of evidence by criminal defendants. In re NSA Telecomms. Records Order Litigation, 483 F. Supp. 2d 934, 939 (N.D. Cal. 2007) (Walker, J.) (holding that Section 2518(10)(c) was drafted with the limited intent to prevent "criminal defendants from suppressing evidence based on electronic communications or customer records obtained in violation of ECPA's provisions"). Accordingly, the Court declines to adopt Defendant's position.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

communications and those who may inadvertently intercept those communications. Further, the statute provides for criminal penalties, as well as a civil right of action for violation of its provisions, such that the statute provides broad protections for interceptions under the Act. Thus, the Court finds that the federal Wiretap Act preempts state wiretap statutory schemes.

Accordingly, the Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Third Cause of Action for violation of various state wiretap statutes with prejudice.

### C. Cal. Bus. & Prof. Code §§ 17200, et seq.

Defendant moves to dismiss Plaintiff's Second Cause of Action for violation of Cal. Bus. & Prof. Code §§ 17200, et seq., on the grounds that claim is preempted by the Federal Wiretap Act on express, field and conflict preemption grounds; and (2) assuming arguendo that the claim is not preempted, Plaintiffs fail to state a claim and fail to plead Proposition 64 standing. (Motion at 17-19.) The Court addresses each ground in turn.

### 1. **Preemption**

At issue is whether Plaintiffs' claims for violation of Cal. Bus. & Prof. Code §§ 17200, et seq., is preempted by the federal Wiretap Act.

Here, unlike in the context of the state wiretap statutes, Cal. Bus. & Prof. Code §§ 17200, et

seq., does not seek to regulate the same field as the federal Wiretap Act. Rather, the statute was intended to broadly enable "tribunals to enjoin wrongful business conduct in whatever context such activity might occur." Barquis v. Merchants Collection Ass'n., 7 Cal. 3d 94, 111 (Cal. 1972). To this end, Section 17200's prohibition of "unlawful" acts does not proscribe specified conduct; rather, the statute incorporates violations of other substantive law as the basis for imposing liability in order to address the added harm to the marketplace of undertaking such violations in a business context. Cal-Tech Comm'ns, Inc. v. Los Angeles Cellular Tel. Co., 20 Cal. 4th 163, 180 (Cal. 1999). Further, the Federal Wiretap Act provides no additional protection or particular civil right of action for interceptions that result in anticompetitive conduct or harm to the market, nor do such additional protections conflict with the stated purpose of the ECPA.

Thus, the Court finds that Plaintiffs' Second Cause of Action for violation of Cal. Bus. & Prof. Code §§ 17200, et seq., is not preempted by the federal Wiretap Act.

# 2. Proposition 64 Standing

At issue is whether Plaintiffs have properly pleaded Proposition 64 standing sufficient to support their Second Cause of Action for violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.* 

To have standing to state a claim for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, as amended by the 2004 passage of Proposition 64, a plaintiff must establish that he has suffered an "injury in fact" and has "lost money or property as a result of such unfair competition." Hall v. Time Inc., 158 Cal. App. 4th 847, 852 (Cal. Ct. App. 2008). Further, allegations of an invasion of privacy are insufficient to invoke Proposition 64 standing. Ruiz v. Gap, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008).

Here, Plaintiffs allege in pertinent part:

Plaintiffs and National Class members have suffered injury in fact and lost property as a result of the unfair and unlawful business practices.

(CCAC ¶ 138.)

Based on the allegations above, the Court finds that Plaintiffs fail to plead facts sufficient to support Proposition 64 standing. In particular, interception of data packets that a plaintiff has sent over a wireless network are not lost property for purposes of determining Proposition 64 standing. Such an indefinite claim of lost property would circumvent the intent of voters, when passing the amendment, to increase the pleading requirements to state a claim for Section 17200 violation. Further, Plaintiffs contentions that merely incurring attorney fees and expenses as a result of bringing a Section 17200 claim are equally inapposite, <sup>13</sup> and would effectively eviscerate the heightened standing requirements of Proposition 64.

Accordingly, the Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Second Cause of Action for violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*, without prejudice to Plaintiffs to amend their pleadings to add facts sufficient to support Proposition 64 standing, if so desired.<sup>14</sup>

<sup>&</sup>lt;sup>13</sup> (Opp'n at 25.)

<sup>&</sup>lt;sup>14</sup> In amending its UCL claim, Plaintiffs must also allege more than a loss of personal information. A plaintiff's "personal information" does not constitute property under the UCL. <u>Thompson v. Home Depot, Inc.</u>, No. 07cv1058 IEG, 2007 WL 2746603, at \*3 (S.D. Cal. Sept. 18, 2007).

# For the Northern District of California

	~~~	$\sim$ -		
V	CON	( 'I	.1 (\$1	

The Court GRANTS in part and DENIES in part Defendant's Motion to Dismiss as follows:

- (1) The Court DENIES Defendant's Motion as to Plaintiffs' First Cause of Action for violation of the Federal Wiretap Act, 18 U.S.C. §§ 2511, et seq.;
- (2) The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Third Cause of Action for violation of various state wiretap statutes with prejudice; and
- The Court GRANTS Defendant's Motion to Dismiss Plaintiffs' Second Cause of (3) Action for violation of Cal. Bus. & Prof. Code §§ 17200, et seq., with leave to amend.

On or before August 1, 2011, Plaintiffs shall file an Amended Complaint consistent with the terms of this Order.

Dated: June 29, 2011

United States District Chief Judge

# THIS IS TO CERTIFY THAT COPIES OF THIS ORDER HAVE BEEN DELIVERED TO: 1 2 John A. Macoretta jmacoretta@srkw-law.com David H. Kramer dkramer@wsgr.com 3 Bart Edward Volkmer bvolkmer@wsgr.com Bobbie Jean Wilson BWilson@perkinscoie.com Caroline Elizabeth Wilson cwilson@wsgr.com 4 Michael H. Rubin mrubin@wsgr.com 5 Susan D. Fahringer sfahringer @perkinscoie.com Aaron Michael Zigler azigler@koreintillery.com Robert A. Curtis rcurtis@foleybezek.com 6 Michael James Aschenbrener maschenbrener@edelson.com 7 Jay Edelson jedelson@edelson.com Eric H. Gibbs ehg@girardgibbs.com Reginald Von Terrell reggiet2@aol.com 8 9 Dated: June 29, 2011 Richard W. Wieking, Clerk 10 11 By: /s/ JW Chambers Susan Imbriani 12 **Courtroom Deputy** 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27