SPECTOR ROSEMAN KODROFF & WILLS, PC
Jeffrey L. Kodroff, Esq.
1818 Market St., Ste. 2500
Philadelphia, PA 19103
Tel. 215-496-0300
Fax. 215-496-6611

COHEN MILSTEIN SELLERS & TOLL PLLC
Daniel A. Small, Esq.
1100 New York Avenue, NW, Suite 500W
Washington, DC 20005
Tel. 202-408-4600
Fax. 202-408-4699

Plaintiff Co-Lead Counsel

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Elizabeth J. Cabraser, Esq. (SBN: 083151)
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel. 415-956-1000
Fax. 415-956-1008

Plaintiffs' Liaison Counsel

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)

PLAINTIFFS' RESPONSE TO DEFENDANT GOOGLE, INC.'S MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT

Hearing Date: March 21, 2011
Hearing Time: 9:00 a.m.
Before: Hon. James Ware

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

OTHER AUTHORITIES

RULES

TREATISES

Rather than answer the allegations against it, Google has asked this Court to summarily dismiss the Consolidated Class Action Complaint ("Compl."). *See* Def. Google Inc.'s Mot. to Dismiss Pls.' Consol. Class Action Compl., Dkt. No. 60 ("MTD"). For the reasons set forth below, the Complaint alleges sound claims, and should not be dismissed.

I. STATEMENT OF ISSUES

A. Whether Google must answer the Federal Wiretap Act claims.
B. Whether Google must answer the State Wiretap Act claims.
C. Whether Google must answer the UCL claims.

II. FACTS

Google launched its "Street View" program in 2007, announcing that it would take pictures from streets across the globe. Compl. ¶¶54-55. Secretly, Google equipped its "Street View" vehicles with a wireless data sniffer, which Google had developed in 2006. *Id.* ¶61. As Google's vehicles drove down the streets, its wireless sniffer technology secretly intercepted otherwise unreadable information from WiFi networks, and then decoded and analyzed the data. *Id.* ¶¶ 62-64. Plaintiffs allege that Google surreptitiously intercepted, decoded and stored on its corporate servers the Class Members' communications and data, including personal emails, passwords, videos, audio, documents and Voice over Internet Protocol communications. *Id.* ¶¶4, 65-67. Instead of alerting the public to its planned intrusion, Google told the public that it had gone to great lengths to ensure people's privacy. *Id.* ¶67. Similarly misleading, Google's privacy policy at the time stated that Google "will not collect or use sensitive information … unless we have obtained your prior consent." *Id.* ¶ 68.

III. LEGAL STANDARD

Google's motion tests the legal sufficiency of the claims asserted in the complaint. *See* Fed. R. Civ. P. 12(b)(6). A complaint should not be dismissed "unless the plaintiffs' complaint fails to state a claim to relief that is plausible on its face." *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 989 (9th Cir. 2009) (quotations omitted). The issue is not whether the non-moving party will ultimately prevail but whether plaintiffs are entitled to offer evidence to support the claims asserted. *See Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1100 (9th Cir. 2010). When evaluating a Rule 12(b)(6) motion, the court must accept all material

allegations in the complaint as true and construe them in light most favorable to the non-moving party.[1] *See Johnson v. Riverside Healthcare Sys.*, 534 F.3d 1116, 1122 (9th Cir. 2008).

IV. Plaintiffs Stated a Claim for Violation of the Wiretap Act

A. Google's Interception of Communications Violated the Federal Wiretap Act

"The paramount objective of the Wiretap Act is to **protect effectively the privacy of communications**." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) (emphasis supplied). Although the Act originally protected only wire and oral communications, Congress enacted the Electronic Communications Privacy Act ("ECPA") in 1986 in order to extend the Act's protections to electronic communications. *See Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995). Plaintiffs' communications sent over WiFi systems are "electronic communications," as defined in the Act. *See* 18 U.S.C. § 2510(12); Compl. ¶¶ 1-2.[2] Google intentionally intercepted those electronic communications, using a data collection program designed by Google that "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." Compl. ¶¶ 4, 60-66. Therefore, Google's intentional interception of Plaintiffs' electronic communications violates Section 2511(1)(a) unless another provision of the Act "specifically provide[s]" that Google's intentional interception of those communications is permitted. *See* 18 U.S.C. § 2511(1).

In its defense, Google relies solely upon Section 2511(2)(g)(i) ("exemption G1"), which provides that it is not unlawful to intercept, "an electronic communication made through an electronic communication system that is configured so that such electronic communication system is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i) (emphasis supplied); *see* MTD at 6-12. Google argues that the definition of "readily accessible" radio

[1] Plaintiffs object to Google's attempt to rely on the report from its retained expert, Stroz Friedberg, which was not incorporated into the Complaint. Plaintiffs have filed a separate Motion to Exclude Google's Expert Report, with detailed arguments incorporated herein.

[2] Plaintiffs also allege Google intercepted "voice over internet" ("VoIP") information. *See* Compl. § 4. Such transmissions are "wire communications," not "electronic communications," because they contain the human voice and are in part transmitted by wire or cable. *See* 18 U.S.C. § 2510(1), (18). Accordingly, the exception in Section 2511(2)(g)(i) on which Google relies, which addresses only "electronic communications," cannot apply to VoIP transmissions, and Google has made no argument that its interception was otherwise legal.

communications, which is contained in Section 2510(16), applies to the G1 electronic communication exemption, rendering Plaintiffs' unencrypted electronic communications "readily accessible." The definition on which Google relies applies, by its own express terms, *only* to the exception contained in Section 2511(2)(g)(ii)(II) ("exemption G2")—an exception on which Google does not, and cannot, rely. Because the definition of "readily accessible to the general public" in Section 2510(16) does not apply to exemption G1, it provides no guidance as to the meaning of that phrase in exemption G1. Accordingly, "readily accessible to the general public," as used in exemption G1, must be read in light of the normal meaning of those words. Accordingly, Google's motion should be denied.

1. Google Cannot Rely on Exemption G1 to Immunize Its Unlawful Intentional Interception of Plaintiffs' Communications

As noted above, Google claims that the definition of "readily accessible to the general public" in Section 2510(16) applies to that phrase as used in exemption G1. Google claims further that, because Plaintiffs' electronic communications were "not scrambled or encrypted"—nor came within any of the other sub-provisions of Section 2510(16)—those communications were, by statutory definition, "readily accessible to the general public." 18 U.S.C. § 2510(16)(A). In making this argument, however, Google ignores Congress's express instruction that the statutory definition of "readily accessible to the general public" in Section 2510(16) applies *only* "with respect to a *radio communication*." *Id.* § 2510(16) (emphasis added). Google further ignores that exemption G2—which Congress enacted at the same time as both Section 2510(16) and exemption G1—applies to "intercept[ions] [of] any *radio communication*," *id.* § 2511(2)(g)(ii)(II) (emphasis added), whereas exemption G1 applies to interceptions of "*electronic communications*," *id.* § 2511(2)(g)(i) (emphasis added).

Specifically, exemption G2 provides that it is "not . . . unlawful" to "intercept any radio communication which is transmitted":

> 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*;

Id. § 2511(2)(g)(ii)(II) (emphasis added). The statutory text and structure make clear that the

definition of "readily accessible to the general public" on which Google relies applies only to that phrase as it is used in exemption G2 and does *not* apply to that phrase as used in exemption G1. Instead, the meaning of "readily accessible to the general public" in the context of *electronic communications* (to which exemption G1 applies) must be understood in light of the normal meaning of the words used in that phrase. *See S.D. Warren Co. v. Me. Bd. of Envtl. Prot.*, 547 U.S. 370, 370 (2006) ("since [the term] is neither defined nor a term of art, it should be construed in accordance with its ordinary or natural meaning" (quotation omitted)); *FDIC v. Meyer*, 510 U.S. 471, 476 (1994) ("In the absence of [an applicable statutory] definition, we construe a statutory term in accordance with its ordinary or natural meaning.").

First, as noted above, Congress enacted both exemptions—G1 and G2—as part of ECPA, when it also enacted Section 2510(16). *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, §§ 101(a)(6), (b)(4), 100 Stat. 1848 (1986). Congress thus used the phrase "readily accessible to the general public" *twice*—once with respect to "electronic communications" (G1) and once with respect to "radio communications" (G2)—yet chose to define the phrase *only* "with respect to a *radio communication*." 18 U.S.C. § 2510(16) (emphasis added). Congress did not enact a definition of the phrase with respect to electronic communications generally or even the subset of electronic communications that are transmitted by radio. The natural conclusion is that Congress intended for the definition in Section 2510(16) to apply *only* to exemption G2 but not also to exemption G1. *See, e.g.*, *Lindh v. Murphy*, 521 U.S. 320, 330 (1997).

Second, Google's statutory construction would render exemption G2 surplusage, in violation of the basic principle that courts should "construe statutes, where possible, so as to avoid rendering superfluous any parts thereof." *Astoria Fed. Sav. & Loan Ass'n v. Solimino*, 501 U.S. 104, 112 (1991). Although Congress did not define the term "radio communications" as used in the Act, the legislative history indicates that all radio communications are electronic communications. *See* H.R. Rep. 99-647 at 35 ("all communications transmitted only by radio would be electronic communications"). As a result, on Google's reading, any interceptions of radio communications that exemption G2 permits, because those communications are "readily accessible to the general public" as defined in Section 2510(16), would already have been

permitted by exemption G1. In other words, if the definition in Section 2510(16) applies to exemption G1 with respect to electronic communications transmitted by radio, as Google claims, exemption G2 is rendered entirely superfluous because all of the communications listed therein would already be encompassed within exemption G1.

Third, in contrast to the natural reading of the statute, Google's position would require the phrase "readily accessible to the general public" to have different meanings, depending on the manner in which an electronic communication is transmitted. That is, on Google's view, Section 2510(16) would define when an electronic communication transmitted by radio is "readily accessible to the general public," but would *not* define that phrase in the context of electronic communications transmitted by any other means recognized in the statute—whether "by a wire, . . . electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12). Thus, under Google's approach, the ordinary meaning of the words in the phrase "readily accessible to the general public," rather than the special definition in Section 2510(16), would control only as to electronic communications not transmitted by radio. Basic principles of statutory interpretation preclude reading the words of exemption G1 to have different meanings depending upon the manner in which an electronic communication is transmitted. *See Reno v. Bossier Parish Sch. Bd.*, 528 U.S. 320, 329 (2000) ("As … in the past, we refuse to adopt a construction that would attribute different meanings to the same phrase in the same sentence, depending on which object it is modifying."); *accord Harper v. U.S. Seafoods LP*, 278 F.3d 971, 975-76 (9th Cir. 2002).[3]

2. Google's Interpretation Violates the Purpose and Objectives of the EPCA

The "paramount objective of the Wiretap Act"—to "protect effectively the privacy of communications," *In re Pharmatrak, Inc.*, 329 F.3d at 18—is furthered only by reading the

[3] Although there is also a "natural presumption that identical words used in different parts of the same act are intended to have the same meaning"—where, as here, both exemptions G1 and G2 include the phrase "readily accessible to the general public"—that presumption "is not rigid and readily yields" where, as here, there is reason to "conclu[de] that they were employed in different parts of the act with different intent." *Envtl. Def. v. Duke Energy Corp.*, 549 U.S. 561, 574 (2007) (internal quotation marks omitted). Here, Congress' express statement that its definition in Section 2510(16) applies only "with respect to a radio communication" supplies the necessary reason to conclude that the phrase carries a different meaning in the two exemptions.

statutory exceptions narrowly. Because the Act originally applied only to wire and oral communications, Congress recognized in 1986 that technological advances, including the proliferation of home computers, required an updating of the law.[4] Congress thus enacted the ECPA to extend the Wiretap Act's protections to electronic communications. *See Brown v. Waddell*, 50 F.3d at 289. With the ECPA, Congress made explicit that it intended to protect personal e-mail communications in which it found individuals "likely . . . have a 'reasonable expectation of privacy.'" H.R. Rep. No. 99-647 at 23. This concern has been echoed by the federal courts in related contexts. *See, e.g.*, *United States v. Warshak*, No. 08-3997, 2010 WL 5071766, at *14 (6th Cir. Dec. 14, 2010) (finding a reasonable expectation of privacy in e-mails under the Fourth Amendment); *cf. Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 974 (C.D. Cal. May 26, 2010) (equating a person's personal rights in a profile or inbox on a social networking site to individual's personal rights regarding employment or bank records). The United States Department of Justice also agrees. Its official computer crime manual instructs that the Wiretap Act generally "bars third parties (including the government) from . . . installing electronic 'sniffers' that read Internet traffic,"[5] strongly suggesting that prosecutors must obtain a warrant before intercepting emails from private networks.[6]

---

[4] S. Rep. No. 99-541 at 4 ("The law must advance with the technology to ensure the continued vitality of the fourth amendment."); 132 Cong. Rec. 4039-01, 1986 WL 776505 (1986) (statement of Congressman Kastenmeier) (right to privacy "will evaporate" if protection is not extended to computer services, "which store [citizens'] bank records, credit card data, electronic mail and other personal data").

[5] Computer Crime and Intellectual Property Section, Criminal Division, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, at 167 (2009). *See also id.* at 60 ("[P]rosecutors should pursue cases involving interceptions occurring on computers or internal networks that affect interstate commerce. For example, if an individual installs malicious software on the victim's computer that makes a surreptitious copy every time an email is sent, or *captures such messages as they move on the local area network on their way to their ultimate destination half way around the world*, such cases can be prosecuted under section 2511." (emphasis added)).

[6] One of Congress' goals in passing ECPA was to protect electronic communications from interception by private actors consistent with the privacy expectations arising from the Fourth Amendment. *See* H.R. Rep. No. 99-647 at 16-19. Google's position would deny protection to unencrypted WiFi communications originating in one's own home and emanating only a short distance beyond it, even when such communications would be protected from government seizure. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27 (2001) (holding that Fourth Amendment requires a warrant for police to use a thermal imaging device outside a home to detect heat sources emanating from inside).

By contrast, Google's view that the Act provides a complete exemption to anyone who intercepts an electronic communication sent over an unencrypted radio network is flatly inconsistent with the stated purposes of the ECPA. In fact, Google's position turns the ECPA upside down, transforming it from a statute that vigorously protects electronic communications into one that broadly authorizes the interception of wireless electronic communications. The G2 radio communications exemption addresses the interception of radio communications over a governmental, law enforcement, civil defense, private land mobile, or public safety (including police and fire) communications system. *See* 18 U.S.C. § 2511(2)(g)(ii)(II). Unencrypted communications by such entities are intentionally broadcast to the general public who listen to governmental, safety, or other public information using radios, CB radios, or police scanners—all readily accessible technologies well known to the general public.[7] Google's comparison of these activities to a home user's personal WiFi network is unfounded. By design, a home-based WiFi network is not intended to create a publicly accessible radio broadcast, even if some of the signal leaks beyond the confines of the home. To the contrary, the purpose of such a network is to provide the convenience of allowing the homeowner to use multiple devices on his or her own property untethered by wires and cords. Laptop computers, iPads, and other devices communicate with the WiFi base station for the sole purpose of convenience within the home.

Google's interpretation of the statute also seeks to obscure the true nature of its activities. Google would have the Court believe that what it did was no more invasive than "free-riding" a neighbor's WiFi network to access the Internet without payment. But as the Complaint explains, Google intentionally went far beyond identifying home-based wireless networks or even surfing the Web over them. The fact that Google managed to do it does not demonstrate that the networks it hacked were readily accessible to the general public.

[7] According to the Department of Justice, the exception in Title III permitting the interception of electronic communications that are made through a system configured so that the communication is readily accessible to the general public was also intended to permit the interception of electronic communications posted to public bulletin boards, chat rooms, or newsgroups. *See* Searches Manual at 182; *See also* S. Rep. No. 99-541, at 36 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3590 (discussing bulletin boards).

3. Whether Plaintiffs' Electronic Communications Are Readily Accessible to the General Public Is a Factual Determination That Cannot Be Resolved on a Motion to Dismiss

Google makes no argument that Plaintiffs' WiFi transmissions of electronic communications are "readily accessible to the general public" under the normal meaning of the words in that phrase. Nor could it; Plaintiffs have properly alleged that the communications Google intercepted from their WiFi networks were neither "*readily* accessible" nor readily accessible "to the general public." *See* Compl. ¶¶ 5, 18-38, 55, 60-64, 130, 142 (emphasis added). Any factual disputes Google might raise about the truth of those allegations are not properly resolved on a motion to dismiss.

First, the electronic communications transmitted between Plaintiffs' computers and their WiFi routers are not normally visible or apparent to anyone else who may be connected to their network or in the near vicinity.[8] Such communications can only be intercepted and viewed after using wireless sniffers and processing the intercepted data to make it readable. *See* Compl. ¶ 63-64. Accordingly, the communications are not readily accessible.

Second, the wireless sniffers and processing required to pluck Plaintiffs' data out of the air and to assemble it into readable content requires a level of technical sophistication not possessed by members of the general public. Thus, the sophisticated technology required to access the WiFi data is not available to the "general public," who would not know how to use such equipment even if they could obtain it. *See id.* Additionally, WiFi communications only have a range of approximately 120 feet to 600 feet (under optimal circumstances).[9] Communications sent over such a system therefore cannot be said to be "readily accessible to the general public" on any plain reading of that phrase, given the difficulty of acquiring and reassembling such communications, and when the range of the transmission system being accessed is so limited.

[8] The present situation is distinguishable from *United States v. Ahrndt*, No. 08-cr-468, 2010 WL 373994 (D. Or. Jan. 28, 2010). *See* MTD at 10. In that case, the defendant used the widely available iTunes software program and affirmatively configured it to permit any other person with the same program who connected to his WiFi network to have access to the files shared by iTunes. Affirmatively making files available for perusal and use by others connected to your network is far different than sending communications over a WiFi network that can only be accessed by others with sophisticated and complicated packet sniffing software.

[9] *See* Wi-Fi, https://secure.wikimedia.org/wikipedia/en/wiki/Wi-Fi#Reach (last visited Jan. 25, 2011).

Third, as discussed above, individuals use their home WiFi systems for e-mail, online banking, and other activities of a confidential nature. They are willing to conduct these sensitive activities because they understand the communications to be private. *See*, *e.g.*, *Warshak*, 2010 WL 5071766, at *10 ("Given the often sensitive and sometimes damning substance of his e-mails, we think it highly unlikely that Warshak expected them to be made public, for people seldom unfurl their dirty laundry in plain view."); *Gonzales v. Google*, 234 F.R.D. 674, 687-88 (N.D. Cal. 2006) (noting the potentially sensitive nature of search queries). Such actions strongly demonstrate that individuals do not expect their online activities to be intercepted by others and do not understand them to be readily accessible.

Google briefly addresses these factual allegations in its motion, *see* MTD at 9 & n.5, but does not seriously contest them. Nor could it do so on a motion to dismiss, because whether the communications were "readily accessible to the general public," based on the ordinary meaning of those terms, raises factual questions that cannot be resolved on such a motion.

4. Google Intercepted Encrypted Communications

Furthermore, Google incorrectly assumes that this case only concerns unencrypted communications. To the contrary, Plaintiffs have alleged that Google's interception of "electronic communications sent or received on wireless internet connections" violates the Wiretap Act, and do not limit the Class or its allegations to unencrypted networks. *See* Compl. ¶¶ 1, 60-66, 119. Indeed, Google has stated that it intercepted encrypted communications, but contends it discarded the contents and did not record them to disk. *See* Rubin Decl. Ex. 3, at 2. Google's acknowledged interception of encrypted communications violate the Act.

5. The "Electronic Communications Systems" Were Not Configured Such that Communications are Readily Accessible to the Public.

Finally, the G1 electronic communications exception upon which Google relies applies to an electronic communication made (1) "through" an (2) "electronic communication system" that is (3) "configured" so that such (4) "electronic communication is readily accessible to the general public." "The term 'configure' is intended to establish an objective standard of design configuration for determining whether a system receives privacy protection." S. Rep. No. 541,

reprinted at 1986 USCCAN 3555 at *3577. Thus, it is the design of the communications system that dictates whether the communication is intended to be public.

Here, Plaintiffs are consumers, whose internet access was provided by an internet service provider, or ISP. An ISP is a service that allows only subscribers who contract with it to access to the internet, and disallows all others. By its very nature, an ISP is an exclusive system not configured so that its communications are accessible to the general public. Google seeks to bypass this by noting that, at the point at which it intercepted the communication, the communication was not encrypted, and therefore it must be "readily accessible." Thus, any weak link in the chain transforms the whole system. But, such an approach to the Wiretap Act, has been rejected both in the Legislative History and by the Department of Justice's Cybercrimes Division: "A transfer should include all transmission of the communication from the originator to the recipient." http://www.justice.gov/criminal/cybercrime/ccmanual/02ccma.html (citing legislative history) (last visited Jan. 23, 2011). Individuals speaking over a CB radio understand the statements can be heard by others. However, people sending email from home internet systems do not expect someone outside can intercept the email. The Federal Wiretap Act favors privacy over disclosure. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002).

B. Google's Disclosure and Use of Plaintiffs' Electronic Communications Violates the Wiretap Act

In addition to interception, the Wiretap Act also makes it unlawful for anyone to intentionally use or endeavor to use, or to intentionally disclose or endeavor to disclose to any other person, the contents of any intercepted wire, oral, or electronic communication. 18 U.S.C. § 2511(c) and (d). Google used the intercepted communications when it processed them; associated them with geographic, network, and date information specific to each communication; recorded the now-compiled information; and then transferred the compiled information from its Street View cars to its own corporate computer network. *See* Compl. ¶¶ 4, 6, 61-63, 65-66. Google disclosed the intercepted communications when it transferred the data compilations that contained them to its corporate servers, conduct that made the compilations available to numerous Google employees and resulted in review of the intercepted communications by at least two

employees. *See* Compl. ¶¶ 4, 6, 57-58; Rubin Decl., Ex. 3 at 2.

1. Use and Disclosure of Intercepted Communications Are Not Lawful

The sole exemption upon which Google relies to justify its actions does not insulate Google from liability for *using* or *disclosing* the intercepted communications. To the contrary, the exemption provides only that it "shall not be unlawful . . . to intercept or access" certain electronic communications. 18 U.S.C. § 2511(2)(g)(i). Unlike other exemptions in the Act, this exemption does not make it lawful to *use* or to *disclose* communications that were permissibly intercepted as a result of that exemption. *See, e.g.*, *id.* § 2511(2)(a)(i) (providing that it "shall not be unlawful . . . to intercept, disclose, or use" certain communications). Indeed, exemption G1 stands in stark contrast to Section 2511(2)(b), which provides not only that it "shall not be unlawful" for employees and agents of the Federal Communications Commission "to intercept a[n] . . . electronic communication," but also makes clear that it shall not be unlawful for the employee or agent "to disclose or use the information thereby obtained." *Id.* § 2511(2)(b).

The Sixth Circuit adopted this reading of the exemptions contained in the Wiretap Act in *Cafarelli v. Yancy*, 226 F.3d 492 (6th Cir. 2000). In *Cafarelli*, the plaintiff cab company owner sued a competitor for intercepting and using his radio communications. The plaintiff alleged that the defendant intercepted his dispatch calls, sent by radio, and then used the information obtained to send one of defendant's own cabs to pick up the customer (and the fare) before plaintiff's cab could arrive. *See id.* at 494-95. The defendant argued that, because the radio communications were readily accessible to the general public, their interception was lawful. The court agreed that the defendant's interception was not unlawful, but found that illegal interception was not a prerequisite to a finding of illegal use under Section 2511(1)(d). Relying on the differences in the language of the various statutory exemptions in the Wiretap Act, the Court concluded that:

> because Congress expressly excluded the word "use" or "disclose" from § 2511(2)(g)[], while expressly including those words in other subparts of subsection (2), one cannot conclude that Congress allowed for the use of intercepted messages under § 2511(2)(g)[] without finding Congress' express inclusion of the word "use" in other subparts of subsection (2) superfluous, in violation of basic principles of statutory construction.

Id. at 499. That same conclusion applies here, so that Google's use and disclosure of the

intercepted communications violates Section 2511(1)(c) and (d).

2. Google Used Plaintiffs' Intercepted Communications

Plaintiffs have pled a claim that Google used Plaintiffs' intercepted communications in violation of Section 2511(1)(d).[10] First, an intercepted communication is used when it is actively, rather than passively, employed. *See Dorris v. Absher*, 179 F.3d 420, 426 (6th Cir. 1999) ("Using is best understood as active, while listening is passive."); *Peavy v. Harman*, 37 F. Supp. 2d 495, 513 (N.D. Tex. 1999), *rev'd in part on other grounds*, 221 F.3d 158 (use "connotes active employment of the contents of the illegally intercepted communication for some purpose"). While "merely listening" to the intercepted communication is generally not considered use, recording an intercepted communication or analyzing and compiling relevant portions of it have been considered use. *See Peavy*, 37 F. Supp. 2d at 514 (analyzing recorded interceptions and compiling relevant portions for transcription constitutes use); *Tapley v. Collins*, 41 F. Supp. 2d 1366, 1375 (S.D. Ga. 1999) ("listening to and hand-recording" constitutes "using").

Google went far beyond "merely listening" to the intercepted communications. It affirmatively designed a system that used the intercepted communications to create unique data compilations that tied the communications to the date, time, and physical location where they were intercepted, as well as the name, quality, strength, and transmission speed of the WiFi system from which the communications were intercepted, and then recorded these compilations to computer disk. *See* Compl. ¶¶ 4, 61-63, 66. Google then took the compilations that contained the intercepted communications from the Street View vehicles and stored them on its own corporate servers.[11] *See* Compl. ¶ 6. Google has also sought to patent the process by which it intercepts WiFi communications and creates these compilations. *See id.* ¶ 65. This act of combining the intercepted communications with other information to create new data is inherently active, and

[10] Although the Complaint only makes reference to interception in Count I, *see* Compl. ¶¶ 129-30, it alleges a violation of 18 U.S.C. § 2511 and the facts necessary to support a claim for use of the communications. *See, e.g., Air Line Pilots Ass'n Int'l v. Transamerica Airlines, Inc.*, 817 F.2d 510, 516 (9th Cir. 1987) (regardless of what legal theory is articulated, a complaint "is sufficient if it shows that the plaintiff is entitled to *any* relief which the court can grant, regardless of whether it asks for the proper relief." (quotation omitted, emphasis in original)).

[11] The only point of storing the communications would be in order to use them, and Google could have chosen to intercept the communications without storing them.

thus constitutes "use" of the intercepted communications. It used them to create new data compilations that were then stored on Google's servers for multiple years (and that Google only sought to destroy once its actions came to light).[12]

3. Google Disclosed Plaintiffs' Electronic Communications

Plaintiffs have also pled a claim that Google disclosed Plaintiffs' intercepted communications in violation of Section 2511(1)(c).[13] Google recorded data compilations containing the intercepted communications on multiple Street View cars, and then transferred the information to Google's central corporate servers, where it was accessible to numerous employees. *See* Compl. ¶¶ 4, 6, 57-58. Moreover, Google has admitted that at least two employees—including the employee who designed the system at issue—accessed the data compilations and viewed the intercepted communications. *See* Rubin Decl., Ex. 3 at 2. Notably, because it is virtually certain that neither employee would have been present for the interception of every communication at issue, their accessing and review of the communications necessarily involves disclosure, in violation of Section 2511(1)(c). *See, e.g.*, *Peavy*, 221 F.3d at 176.

V. THE STATE WIRETAP CLAIMS ARE NOT PREEMPTED

Google relies on the doctrines of express, field, and conflict preemption to claim that state laws prohibiting the interception of Plaintiffs' communications are preempted. Google is wrong on all three counts.

A. Plaintiffs' State Wiretap Claims Are Not Expressly Preempted

In enacting the Wiretap Act, Congress made its intent not to displace state law clear: "The scope of the [civil] remedy [for wiretapping offenses] is intended to be both comprehensive and exclusive, *but there is no intent to preempt parallel state law*." S. Rep. No. 90-1097, 1968 U.S.C.C.A.N. at 2196 (emphasis added). *See, e.g.*, *Kearney v. Salomon Smith Barney, Inc.*, 39

[12] Further details about Google's use of the intercepted data are uniquely in Google's possession and must await discovery. Google has already admitted that at least two of its employees accessed the intercepted communications. *See* Rubin Decl., Ex. 3 at 2. Google has repeatedly stated that the intercepted communications have "never been used *in any Google product or service*," *see, e.g.*, *id.* at 2 (emphasis added), but has never claimed that the communications were not used at all.

[13] While Plaintiffs' Complaint only makes reference to interception in Count I, *see* Compl. ¶¶ 129-30, it alleges a violation of 18 U.S.C. § 2511 and the facts necessary to support a claim for disclosure of the communications.

Cal. 4th 95, 137 P.3d 914 (Cal. 2006) (reaffirming 1974 ruling that the Wiretap Act does not preempt state law); see also *Gaeta v. Perrigo Pharmaceuticals Co.*, No. 09-15001, 2011 WL 198420, at *4 (9th Cir. Jan. 24, 2011).

Google, however, claims that Congress, in enacting ECPA, reversed its long-standing intent and expressly preempted state law remedies. Google relies on Section 2518(10)(c), which states that the "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). However, this restrictive language makes clear that only the civil and criminal remedies provided in §2520 are available to redress violations of the Wiretap Act. It does not indicate intent to preempt state civil remedies or other federal remedies. *See In re NSA Telecomms. Records Order Litigation*, 483 F. Supp. 2d 934, 939 (N.D. Cal. 2007). "[W]hen the text of a preemption clause is susceptible to more than one plausible reading, courts ordinarily 'accept the reading that disfavors pre-emption.'" *VP Racing Fuels, Inc. v. General Petroleum Corp.*, 673 F.Supp. 2d 1073, 1079 (E.D. Cal. 2009),

As the Ninth Circuit has recognized, this section—and a parallel section of the Stored Communications Act—simply make clear that the two federal acts are "mutually exclusive statutes (with mutually exclusive remedies)." *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998). Indeed, in enacting Section 2518(10)(c), Congress gave no indication of an intent to preempt state law remedies. On the contrary, in this section, Congress sought to make clear that the statutory suppression-of-evidence rule in the Wiretap Act (which is not found in the Stored Communications Act) does not apply to unlawfully intercepted electronic communications, which could instead be suppressed only pursuant to the Fourth Amendment:

> The purpose of this provision [§ 2518(10)(c)] is to underscore that, as a result of discussions with the Justice Department, the Electronic Communications Privacy Act does not apply the statutory exclusionary rule contained in title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the interception of electronic communications.

S. Rep. No. 99-541 at 23. As the Ninth Circuit has explained, courts "are compelled to adopt a reading of the preemption clause that conforms with the statute's structure as a whole and the

stated legislative purpose." *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1063 (9th Cir. 2009). That purpose was not to preempt state law remedies.

Against this, Google cites only two cases, *see* MTD at 13, but neither can support its claim here. The court in *Bunnell v. Motion Picture Ass'n of America*, 567 F. Supp. 2d 1148 (C.D. Cal. 2007), simply asserted without explanation that "the federal Wiretap Act contains and [sic] express preemption." *Id.* at 1154. In *Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116 (C.D. Cal. 2006), the court was construing the Stored Communications Act and the plaintiff apparently did not respond to the defendant's characterization of the statute as containing an express preemption provision. *See id.* at 1138. Instead, the proper analysis is found in *In re NSA Telecomms. Records Order Litigation*, 483 F. Supp. 2d 934 (N.D. Cal. 2007), in which a court in this district followed the Ninth Circuit's decision in *Smith* and recognized that Section 2518(10)(c) was "added to the ECPA for a limited purposes: to prevent criminal defendants from suppressing evidence based on [intercepted] electronic communications." *Id.* at 939.

B. The Wiretap Act Does Not Preempt the Field

Although Google next asserts, *see* MTD at 14-15, that the Wiretap Act preempts the field, leaving no room for state law to regulate the unauthorized interception, use, and disclosure of communications, the Supreme Court has recently reconfirmed that the "case for federal pre-emption is particularly weak where Congress has indicated its awareness of the operation of state law in a field of federal interest, and has nonetheless decided to stand by both concepts and to tolerate whatever tension there [is] between them." *Wyeth v. Levine*, 129 S. Ct. 1187, 1200 (2009) (internal quotation marks omitted); *see also Ting v. AT&T*, 319 F.3d 1126, 1136 (9th Cir. 2003) (holding that "field preemption is not an issue because state law unquestionably plays a role" under the statutory regime). That principle bars Google's field preemption claim, because the Wiretap Act expressly contemplates state adoption or supplementation of federal wiretap law. For example, pursuant to § 2516(2), orders by a state court authorizing the interception of wire communications are required to be "in conformity with section 2518 . . . *and with the applicable State statute*." 18 U.S.C. § 2516(2) (emphasis added).

The legislative history also demonstrates that Congress anticipated and planned for

parallel state statutes. "The State [wiretap] statute must meet the minimum standards reflected as a whole in the proposed chapter. The proposed provision envisions that States would be free to adopt more restrictive legislation, or no legislation at all, but not less restrictive legislation." *See* S. Rep. No. 90-1097, at 98 (1968). *See also United States v. Mora*, 821 F.2d 860, 863 n.3 (1st Cir. 1987) ("Generally speaking, insofar as wiretapping is concerned, states are free to superimpose more rigorous requirements upon those mandated by the Congress, but not to water down federally-devised safeguards.") (internal citations omitted); *Commonwealth v. Spangler*, 809 A.2d 234, 237 (Pa. 2002) ("The federal legislation authorizes states to adopt coordinate statutes permitting the interception of wire, oral, or electronic communications, see 18 U.S.C. § 2516(2), and to grant greater, but not lesser, protection than that available under federal law.")

When Congress passed the ECPA to amend the Wiretap Act, it re-emphasized that it was not preempting state laws by giving the states needed time to incorporate the newly amended "minimum standards" into their own wiretap laws: "Under chapter 119, the states must enact statutes which are at least as restrictive as the provisions of chapter 119 before they can authorize their state courts to issue interception orders. Because of the substantial changes made by this act it is appropriate to grant the states sufficient time to modify their laws. This special effective date rule gives the states two years to amend their laws to meet the new requirements of chapter 119." S. Rep. No. 99-541, at 35.[14] *See also Lane v. CBS Broad., Inc.*, 612 F. Supp. 2d 623, 637 (E.D. Pa. 2009) (quoting the above language and concluding "rather than leaving no room for supplementary state regulation, Congress expressly authorized states to legislate in this field.").

Against this, Google again cites only *Bunnell* and *Quon*, but neither decision addresses any of these points — or the applicable legal standard — in finding field preemption.[15]

C. Plaintiffs' State Wiretap Claims Are Not Barred by Conflict Preemption

Finally, Google claims, MTD at 15-16, that Plaintiffs' state wiretap claims are preempted because they conflict with federal law. That claim also fails. First, this case implicates the Supreme Court's recognized "presumption against preemption," which applies with particular

[14] This provision was enacted by Pub. L. 99-508, § 111, 100 Stat. 1848 (1986).

[15] Google also cites, *see* MTD at 15, the Supreme Court's decision in *Bartnicki v. Vopper*, 532 U.S. 514 (2001), but that case had nothing to do with preemption or state law remedies.

force here, because this case involves an area of traditional state regulation, namely, those within the police power of the state. *See Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996); *Buckman Co. v. Pls.' Legal Comm.*, 531 U.S. 341, 347 (2001); *United States v. Locke*, 529 U.S. 89, 108 (2000). States have long regulated the interception of electronic communication. Indeed, many of the state laws governing the privacy of electronic communications predate the ECPA.[16]

Second, Google cannot identify any actual conflict that would warrant preemption. Instead, based on its erroneous claim that the Wiretap Act authorized its interception of data on unencrypted WiFi networks, Google claims further that state law prohibiting such unauthorized interception "would thwart the federal policy of encouraging open communications on [unlicensed] spectrum." MTD at 16. As an initial matter, as explained above, Google is wrong: its interception of the communications at issue here is not protected by exemption G1, so there is no conflict between state and federal laws. *See* Section IV.A.1. In addition, Google does not identify any federal policy in favor of the *unauthorized* interception of WiFi communications, let alone the *intentional* deployment of technology to intercept communications that otherwise would have remained entirely private.

Finally, and in all events, Google ignores that Congress has always allowed states to adopt *more restrictive* wiretapping laws, providing greater protection to consumers. *See Mora*, 821 F.2d at 863 n.3; *Gaeta*, 2011 WL 198420 at *1 ("federal law does not preempt state law failure – to-warn claims against generic manufacturer, provided there is no 'clear evidence' that the FDA would not have approved the proposed stronger warning."). Thus, Congress has "decided to tolerate . . . whatever tension there [is] between" the Wiretap Act and more restrictive state law. *Wyeth*, 129 S. Ct. at 1200.[17]

[16] For example, while the Wiretap Act was passed in 1968, Washington first passed a statute related to the interception of telegraph transmissions in 1909. *See* Rev. Code Wash. § 9.73.010.

[17] That Plaintiffs' state wiretap claims would be an obstacle to the ECPA policy of encouraging innovation is absurd. *See* MTD at 15. The goal of innovation was secondary to Congress' principal goals of privacy and law enforcement, as attested by the Act's title: "The Electronic Communications Privacy Act of 1986." H.R. Rep. No. 106-932 at 10 (2000). The text of the House report is even more explicit: "It was the intent of Congress to encourage the proliferation of new communications technologies, but it recognized that consumers would not trust new technologies if the privacy of those using them was not protected." *Id.* (citing: S. Rep No. 99-541, at 5 (1986)); H.R. Rep. No. 99-647, at 19 (1986).

VI. THE 17200 CLAIMS SHOULD NOT BE DISMISSED

A. The Section 17200 Claim Is Not Preempted

As discussed above, the claims under California's Unfair Competition Law ("UCL") are not preempted by the Federal Wiretap Act. Additionally, the UCL claims are not preempted because they are qualitatively different from and contain elements not shared by the Federal Wiretap Act claims. *See Bekaert Progressive Composites Corp. v. Wave Cyber Ltd.*, No 06-cv-2440, 2007 WL 1110736, at *2-3 (S.D. Cal. Apr. 5, 2007); *see also Wang v. Chinese Daily News, Inc.*, 623 F.3d 743, 760 (9th Cir. 2010). The Wiretap Act is narrowly focused on prohibiting the interception, use and disclosure of specific types of communications. In contrast, the UCL broadly prohibits businesses from engaging in any unlawful, unfair or fraudulent business acts or practices. Unlike the relatively limited scope of the Wiretap Act, the UCL implicates a "broad range of claims," and includes "sweeping language to permit tribunals to enjoin on-going wrongful business conduct in whatever context such activity might occur." *Summit Mach. Tool Mfg. Corp. v. Victor CNC Sys, Inc.*, 7 F. 3d 1434, 1440 n.3 (9th Cir. 1993).

Plaintiffs allege that Google violated § 17200 because its conduct, in addition to violating federal and state wiretap acts, was unlawful, unfair, immoral, unethical, oppressive, unscrupulous and/or substantially injurious to the National Class members. *See Compl.* ¶136. Plaintiffs further allege that Google violated § 17200 because it invaded class members' legally protected right to privacy under the California Constitution and other applicable law. *See id*. ¶137. They allege not just that Google intercepted, used and disclosed communications, but that it did so surreptitiously and misled the public and Class Members about its misdeeds. *See id*. ¶¶ 1, 56, 59, 66-70, 76-77.

Google makes no claim that these aspects of the UCL claims are preempted, nor could it succeed in such an argument. The proof supporting the UCL claim is qualitatively different from that required to show an unlawful "interception," "use," or "disclosure" under the Wiretap Act.

B. The Section 17200 Claim Is Sufficiently Pled

The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. Google asserts that its conduct did not violate the Federal Wire Tap Act, and summarily concludes that, therefore, it was not "unlawful" or "unfair" under the UCL.

Aside from the fact that Google is wrong about the lawfulness of its conduct under the Wiretap Act and similar state laws, Google's argument fails because it does not address the other respects in which its actions were unlawful and unfair.

1. Google's Acts Were Unlawful

As explained above, Google violated the Federal Wiretap Act. Its conduct was, thus, unlawful under the UCL. *See Cal-Tech Commc'n, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (Cal. 1999) ("By proscribing 'any unlawful' business practices, section 17200 'borrows' violations of other laws and treats them as unlawful practices that the unfair competition law makes independently actionable." (citations omitted)).

Moreover, Google's conduct was unlawful because it violated the privacy rights set forth in the California Constitution.[18] *See* Cal. Const. art. I, § 1; *see also Ortiz v. L.A. Police Relief Ass'n.*, 98 Cal. App. 4th 1288, 1300 (Cal. Ct. App. 2002). The California Constitution establishes a right to privacy that exists where there is: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 15-20, 39-40 (Cal. 1994). Plaintiffs have alleged that Google's conduct met all three of these elements. *See, e.g.*, Compl. ¶¶ 1-8, 53-77.

Additionally, Google's conduct is prohibited by the UCL, because it violated the common law. An unlawful business practice actionable under the UCL, "is one that violates an existing law, including case law." *See Cmty. Assisting Recovery, Inc. v. Aegis Sec. Ins. Co.*, 92 Cal. App. 4th 886, 891 (Cal. Ct. App. 2002); *see also Cortez v. Global Ground Support, LLC*, No. 09-cv-4138, 2009 WL 4282076, at *2-3 (N.D. Cal. Nov. 25, 2009). For instance, in *In CRST Van Expedited, Inc. v. Werner Enterprises*, the UCL allegations were sufficient because the plaintiff, "adequately alleged that [the defendant] engaged in an 'unlawful' business act or practice, . . . namely, intentional interference with [the plaintiff's] employment contracts." 479 F. 3d 1099,

[18] The Complaint does not need to include invasion of privacy and other tort claims as separate, additional causes of action. *See Chabner v. United of Omaha Life Ins. Co.*, 225 F.3d 1042, 1048 (9th Cir. 2000); *see also Jordan v. Paul Fin., LLC*, No. 07-4496, 2010 WL 3892261, * 10 (N.D.Cal. Sep. 30, 2010).

1107 (9th Cir.2007); s*ee also Clark v. Prudential Ins. Co. of Am.*, No. 08-cv-6197, 2010 WL 352223, at * 23-25 (D.N.J. Sept. 9, 2010).[19]

In this case, Google's actions constituted an unlawful invasion of privacy. *See Marich v. MGM/UA Telecomm., Inc.*, 113 Cal. App. 4th 415, 421 (Cal. Ct. App. 2003) (setting forth elements of a common law cause of action for invasion of privacy: "(1) [intentional] intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person."). Google's conduct also amounted to conversion or wrongful possession of property. *See Terarecon, Inc. v. Fovia, Inc.*, 2006 WL 1867734, * 9-10 (N.D. Cal. July 6, 2006) (finding complaint stated claim of conversion for allegations of converted computer code); *see also A & M Records, Inc. v. Heilman*, 75 Cal. App. 3d 554, 569-70 (Cal. Ct. App. 1977) (California courts recognize conversion claims based on the taking of copies of intangible personal property even where original remains with owner).

Because Google's actions violated the Federal Wiretap Act and similar state law, violated the privacy protections of the California Constitution, violated common law privacy rights and constituted wrongful possession of another's property, Google's conduct was unlawful. The UCL claim should not, therefore, be dismissed.

2. Google's Acts Were Unfair

It is well-established that a practice may be "unfair" in violation of the UCL, even when it does not rise to the level of being, "unlawful." *See Gregory v. Albertson's, Inc.*, 104 Cal. App. 4th 845, 850 (Cal. Ct. App. 2002). That is, of course, precisely the reason the UCL prohibits both "unfair" conduct and "unlawful" conduct. Therefore, even if Google's conduct was lawful (and it is not), it does not follow that its conduct must therefore be deemed fair.

Many courts define "unfair" conduct as conduct that is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers, and weigh those acts against the conduct's

[19] Whether negligence-based claims are unlawful under the UCL is irrelevant because simple acts of negligence are substantively distinct from acts, such as Google's, which constitute the intentional torts of invasion of privacy and conversion. *See, e.g. Klein v. Earth Elements, Inc.*, 59 Cal. App. 4th 965, 969 (Cal. Ct. App. 1997) (holding that "the *unintentional* distribution of a defective product is beyond the scope and policy of the 'unlawful' prong of section 17200" (emphasis added)).

utility. *See Bardin v. DaimlerChrysler Corp.*, 136 Cal. App. 4th 1255, 1260-61 (Cal. Ct. App. 2006); *Lozano v. AT&T Wireless, Servs., Inc.*, 504 F. 3d 718, 736 (9th Cir. 2007). Other courts have held that "unfair" conduct underlying a UCL claim must be "tethered" to a specific constitutional, statutory or regulatory provision. *See Bardin*, 136 Cal. App. 4th at 1260-61. Google's conduct is an "unfair" business practices under either approach.

Google seized personal data and communications from the public; did this without permission; and did this in secret. When launching its Street View program in 2007, Google concealed the fact that its cars had not just cameras—but also "sniffers," intentionally designed by Google to gather what it euphemistically calls "payload data," and which in fact includes personal emails, passwords, photos, videos, documents and other information. *Compl*. ¶¶4-5; 53-68. Google could have announced its plan, and allowed people an opportunity to shield themselves from this intrusion. Instead, Google issued misleading and untruthful statements about its activities, assuring the public that it had "gone to great lengths to ensure . . . privacy." *Id.* ¶67. At the time, Google's widely-circulated privacy policy similarly proclaimed that "we will not collect or use sensitive information for purposes other than those described . . . unless we have obtained your prior consent." *Id.* ¶ 68.

Contrary to its assurances, however, Google methodically gathered the very information it promised it had gone to "great lengths" to safeguard. Considering the personal privacy and information at stake, and especially in light of the surreptitious and misleading nature of Google's acquisition of this data, Google's conduct was, "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." Nor are the injuries in having personal, private data seized and maintained by Google, "conjectural or hypothetical," as Google asserts.[20] Although Google misled the pubic and initially denied its misdeeds, it now admits it seized the class members' communications and information. *See* Compl. ¶¶ 69-75. Google's actions demonstrate how little Google respects these rights, but Google's dismissive attitude does not lessen the real injury

[20] *Spiegler v. Home Depot USA Inc.*, 552 F. Supp. 2d 1036 (C.D. Cal. 2008) is inapplicable. *See* MTD at 18. That case simply held that where the conduct complied with the parties' contract, "the UCL cannot be used to rewrite their contracts or to determine whether the terms of their contracts are fair." *Id.* at 1045-46. There is no such contract here.

inflicted by its misdeeds.

Google's conduct is also "unfair" because it encroached upon privacy and property rights embodied in multiple Constitutional, and federal and state statutory provisions. These rights lie at the heart of civilized society. *See Hill*, 7 Cal. 4th at 23 (Cal. 1994). As explained by the California Supreme Court,

> The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, ... It prevents government and *business interests from collecting and stockpiling unnecessary information about us* and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.
>
> Fundamental to our privacy is the ability to control circulation of personal information.

White v. Davis, 13 Cal. 3d 757, 774 (Cal. 1975) (emphasis added). Because the allegations against Google are "tethered" to Constitutional and statutory provisions, Google's conduct was unfair.

The cases Google cites do not support its claim that if its conduct did not violate the federal Wire Tap Act, then it was "fair" under the UCL. For instance, in *Facebook, Inc. v. Power Ventures, Inc.*, No. 08-cv-5780, 2010 WL 3291750, at *14-15 (N.D. Cal. July 20, 2010), this Court dismissed the UCL claim because it rested solely upon alleged antitrust violations, and the Court had already found that the conduct was not anticompetitive. Similarly, in *Saunders v. Apple Inc.*, 672 F.Supp.2d 978, 989 (N.D. Cal. 2009), the Court dismissed the UCL claim because the plaintiff, "failed to make out a viable claim for fraudulent concealment or other wrongdoing." Neither of these cases supplies grounds for excusing Google's unfair actions.

Because Google's conduct was unfair, the UCL claim should not be dismissed.

C. Plaintiffs have Demonstrated Proposition 64 Standing

Because Plaintiffs have alleged they "suffered injury in fact[21] and . . . lost money or property as a result of the unfair competition," they have standing to bring a UCL claim. Cal. Bus. & Prof. Code § 17204, as amended by Proposition 64.[22]

[21] Google does not challenge that Plaintiffs have alleged injury in fact. *See* MTD at 18-19.

[22] Standing under Proposition 64 must be shown only for class representatives, not for absent class members. *In re Tobacco II Cases*, 46 Cal. 4th 298, 324 (Cal. 2009).

Under Section 17204, a plaintiff must show either "prior possession or a vested legal interest in the money or property allegedly lost." *Multiven, Inc., v. Ciso Sys., Inc.*, 725 F. Supp. 2d 887, 896 (N.D. Cal. 2010) (*citing Walker v. USAA Cas. Ins. Co.*, 474 F. Supp. 2d 1168, 1172 (E.D. Cal. 2007). In this case, Plaintiffs had prior possession of the communications and data that Google surreptitiously seized. Plaintiffs, furthermore, have a vested legal interest in the copies of their communications and data that are retained by Google which is capable of restitution. *See Buckland v. Threshold Enters., Ltd.*, 155 Cal. App. 4th 798, 817 (Cal. App. Ct. 2007). Google admittedly seized personal, private data and communications without authorization. There is a property right in copies of intangible personal property, even when the owner retains an original or copy. *See A & M Records,* 75 Cal. App. 3d at 569-70. The UCL provides Plaintiffs the means to obtain the return of their stolen data. Similar to this case, in *Multiven, Inc. v. Cisco Systems, Inc.*, this Court found UCL standing arising from the unauthorized downloading of copies of software because, among other reasons, returning the software was an appropriate UCL remedy. 725 F. Supp. 2d 887, 897 (N.D. Cal. 2010).

Google argues that because Plaintiffs provided their data and communications to third parties, Plaintiffs lost all rights in it, and Google was free to steal it. *See* MTD at 18. That is not the law. For instance, in *Doe v. AOL, LLC*, No. 06-cv-5866, 2010 WL 2524494, *4-5, 9 (N.D. Cal. June 23, 2010), the Court found that the plaintiffs had standing under the UCL when AOL collected and stored plaintiffs' search queries, which contained confidential information. The Court found that the plaintiffs had suffered a loss from AOL's unauthorized collection and disclosure of this private information, even though the plaintiffs had transmitted the information to others over the internet and had sent their inquiries directly through AOL. Importantly, the Court found that, like Google, AOL misrepresented its activities, assuring the plaintiffs of its commitment to maintaining privacy. *Id.* at *7. Of course, in *AOL* the defendant had already published the unfairly seized information—whereas in this case the Class Members do not yet know all that Google has done or will do with their communications and data. It is axiomatic that, "[t]he intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind." *Restatement (Second) of Torts* § 652B (noting an invasion

occurs when someone opens the private and personal mail or when one "taps" the phone of another to make a record of conversations). Without Court intervention, Google will remain free to use this unfairly gained private data in any way it chooses, and free to collect more.

Likewise, Google's unsupported argument that Plaintiffs broadcasted their communications, and thus had no "plausible expectation of it being returned," is unfounded. *See* MTD at 18. Instead, much like the plaintiffs in *AOL*, the Class Members, in their private homes, communicated with identified third parties, providing personal emails, passwords, videos, audio, documents, and VoIP communications. *Compl.* ¶4. Class Members had no expectation that these private communications would be intercepted by sophisticated equipment and software merely because the communications momentarily emanated a few feet beyond the confines of their home, but Class Members certainly do expect Google to return these communications. Just as in *AOL*, the Class Members have a right to the return or destruction of Google's copies of the private information Google surreptitiously seized.

The loss suffered by Plaintiffs in this case is highlighted when the facts of this case are compared to those in the *Robinson v. HSBC Bank, USA*, No. 10-cv-1494, 2010 WL 3155833 (N.D. Cal. 2010), which is cited by Google. In *Robinson*, the defendant merely took a picture of the plaintiffs' house from the street and then used the photograph in an advertisement. *Id.* at * 1. The plaintiffs clearly had no property interest in the way their house looked from the street. Thus, they suffered no loss of property from the defendant's use of a picture of it. In this case, by contrast, Google surreptitiously developed and deployed sophisticated equipment and software to invade the Class Members' private communications, and then to seize, decode and store them.

Google's reliance on *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121 (N.D. Cal. 2008), is also misplaced. Contrary to the facts in this case, in *Ruiz*, the plaintiff voluntarily gave personal identifying information to Gap, which then had its laptops stolen. *Id.* at 1124. Gap did not steal the information. *Id.* As the R*uiz* Court explained, "[t]here are no allegations of conversion or any other action by Gap that would indicate that Gap sought to unlawfully retain possession of Ruiz's social security number." *Id.* at 1127. Gap did not wrongfully retain stolen information, nor could the UCL serve as a means for Gap to return it. That is far different from Google's intentional,

unauthorized interception, use, and disclosure of private information.

In addition, in working to vindicate their rights, Plaintiffs have invested time and energy investigating claims and have retained counsel to hire computer experts to analyze the depths of Google's misdeeds, and to enjoin Google's use of the information. (*See Compl*. ¶ 6; Dkt. No. 28, "Pls' Notice & Mot. to Appoint Jeffrey Kodroff & Daniel Small as Interim Class & Co-Lead Counsel, & Elizabeth Cabraser as Interim Class & Liaison Counsel," 6). Plaintiffs have thus also suffered lost money sufficient to allege standing under the UCL. S*ee Coupons, Inc. v. Stottlemire*, 588 F. Supp. 2d 1069, 1075 (N.D. Cal. 2008) (denying motion to dismiss and finding plaintiff had sufficient standing for UCL claim based, in part, on the allegations that it was required to expend attorney's fees and costs); *see also Witriol v. LexisNexis Group*, 2006 WL 4725713, *6-7 (N.D. Cal. Feb. 10, 2006) (finding standing because plaintiff incurred costs to monitor and repair damage to credit because defendant's unauthorized release of private information); *S. Cal. Hous. Rights Ctr. v. Los Feliz Towers Homeowners Ass'n*, 426 F. Supp. 2d 1061 (C.D. Cal. 2005) (plaintiff satisfied UCL's standing requirements by presenting evidence of a loss of financial resources in investigating the claim and diversion of staff time).[23]

Plaintiffs have established injury-in-fact and shown a loss of "money or property" to maintain a claim under the UCL, which was drafted with broad language to protect the public from novel misdeeds by creative corporations. Because Plaintiffs have sufficiently pled an injury in fact and a loss of money or property, the UCL claims should not be dismissed.

VII. CONCLUSION

For the foregoing reasons, Google should be required to answer the allegations against it and the Complaint should not be dismissed.

[23] Google is also incorrect that "[t]here are no allegations of subsequent use or disclosure of the payload collected." MTD at 19. Plaintiffs have alleged that Google used and disclosed their intercepted communications in violation of Section 2511(c) and (d) of the Wiretap Act. *See* Section IV.B, above.

Dated: January 25, 2011

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

By: /s/ Elizabeth J. Cabraser
Elizabeth J. Cabraser (SBN: 083151)

275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel. 415-956-1000
Fax. 415-956-1008

Plaintiffs' Liaison Counsel

SPECTOR ROSEMAN KODROFF & WILLS, PC

By: /s/ Jeffrey L. Kodroff
Jeffrey L. Kodroff, Esq.

1818 Market St., Ste. 2500
Philadelphia, PA 19103
Tel. 215-496-0300
Fax. 215-496-6611

COHEN MILSTEIN SELLERS & TOLL PLLC

By: /s/ Daniel A. Small
Daniel A. Small, Esq.
1100 New York Avenue, NW, Suite 500W
Washington, DC 20005
Tel. 202-408-4600
Fax. 202-408-4699

Plaintiff Co-Lead Counsel