RANDALL W. EDWARDS (S.B. #179053) redwards@omm.com
BRYNLY R. LLYR (S.B. #235926) bllyr@omm.com
JEAN B. NIEHAUS (S.B. #254891) jniehaus@omm.com
O'MELVENY & MYERS LLP
Two Embarcadero Center, 28th Floor
San Francisco, CA 94111-3823
Telephone: (415) 984-8700
Facsimile: (415) 984-8701

Attorneys for Defendant
Google Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

JASON WEBER, an individual, on behalf of himself and all others similarly situated,

Plaintiff,

v.

GOOGLE INC., a Delaware Corporation,

Defendant.

Case No. 5:10-cv-05035-LHK

CLASS ACTION

GOOGLE INC.'S MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT PURSUANT TO RULES 12(b)(1) AND 12(b)(6)

Hearing Date: June 23, 2011
Time: 1:30 p.m.
Place: Courtroom 4, 5th Floor
Judge: Hon. Lucy H. Koh

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on June 23, 2011, at 1:30 p.m., or as soon thereafter as this motion may be heard in the above-entitled court, located at 280 South First Street, San Jose, California, in Courtroom 4, Defendant Google Inc. will, and hereby does, move the Court for an order dismissing the First Amended Complaint filed by Plaintiff Jason Weber. Google's Motion to Dismiss is made pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). The Motion is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the Declaration of Brynly R. Llyr and attached Exhibit, and such other matters, both oral and documentary, as may properly come before the Court.

Google seeks an order, pursuant to Federal Rule of Civil Procedure 12(b)(1), dismissing Plaintiff's Complaint for lack of subject matter jurisdiction. Google also seeks an order dismissing each of the Complaint's four causes of action for failure to allege facts sufficient to state a claim upon which relief can be granted, pursuant to Federal Rule of Civil Procedure 12(b)(6).

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

In his first Complaint, Plaintiff Jason Weber attempted to force-fit his claims regarding Google's Toolbar into an inapplicable framework of statutes intended to cover computer hacking, wiretapping, product sales, and other activities entirely unrelated to his allegations. As shown in Google's initial Motion to Dismiss, these deficiencies were fatal: Plaintiff failed to plead facts sufficient to show he suffered any injury in fact or to establish critical elements of each of his claims. In response to Google's motion, Plaintiff filed his First Amended Complaint ("FAC"), which abandoned his claim under the California Consumers Legal Remedies Act but did nothing to cure the substantive and fatal remaining deficiencies. In short, the FAC remains as deficient as the original.

This case is about Google Toolbar, a free browser tool with features including Internet search, spell checking, and web page language translation. Toolbar also offers users the option of

enabling enhanced features—features that require sending certain information to Google. Toolbar users were not exposed to the hacking or wiretapping targeted by the statutes Plaintiff cites; to the contrary, the proposed class of users voluntarily downloaded Toolbar, received disclosures regarding the transmission of information associated with its enhanced features, and then affirmatively opted-in to enable those features.

The FAC focuses on a specific alleged grievance: that for approximately two months when users purportedly disabled Toolbar through certain Internet Explorer commands, Google purportedly knew that Toolbar continued to transmit information as though enhanced features were enabled until the user exited or restarted his or her browser. But even on his second try, Plaintiff does not plead facts establishing that he was a user affected by the alleged continued collection of information or that he suffered any actual injury. Plaintiff attempts to fabricate standing, notwithstanding the fact that Toolbar is free, by concocting a theory of "value-for-value" exchange, in which users trade purportedly "personal" information—a category he entirely fails to define—for the right to use Toolbar. This theory relies on the legally-unsupported notion that the undefined category of "personal" information has economic value. Furthermore, even if such a theory were legally viable, Plaintiff does not—and cannot—allege facts that establish that he or other users agreed with Google to exchange, or did in fact exchange, "personal" information for the right to use Toolbar. Because Plaintiff does not meet the threshold requirement of Article III standing, the entire FAC should be dismissed.

In addition to his standing problems, Plaintiff's factual allegations fail to satisfy the elements of the claims he asserts. Plaintiff cannot shoehorn his claim into the two federal statutes he claims were violated—the Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*, or the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030 *et seq*. Both statutes were designed to address specific unlawful activity: (1) using specially employed devices to surreptitiously intercept communications; and (2) criminal computer hacking. The facts alleged do not fit either statute. Even under Plaintiff's allegations, users knowingly installed Toolbar, were given notice of the types of information that would be collected, and affirmatively enabled Toolbar's enhanced features. Plaintiff does not allege the most basic facts necessary to establish the key elements of

these two claims: that Google either employed an interception device to intercept Plaintiff's communications or that Google accessed Plaintiff's computer without authorization.

Plaintiff's state law claims also fail. As a threshold matter, the Wiretap Act's plain language preempts state-law claims premised on the same conduct. Further, to the extent Plaintiff's state-law claims challenge the adequacy of Google's disclosures surrounding Toolbar and its enhanced features, Plaintiff's factual allegations about his own experience do not state a claim. Plaintiff never alleges that he did not understand what information was collected, and he has not identified what Toolbar disclosures (if any) he actually read. Even assuming Plaintiff reviewed the more recent version of the Toolbar enhanced features dialog box described in the FAC and the 2009 version of the Toolbar Privacy Notice—the only disclosures attacked as inadequate—the plain language of those disclosures refutes any contention that Google failed to disclose the collection of data required by Toolbar's enhanced features.

Finally, additional independent grounds exist to dismiss the UCL claim, including Plaintiff's lack of standing under the UCL due to his failure to allege facts showing that he has lost any money or property. Further, Plaintiff's unjust enrichment claim fails because no such cause of action exists under California law.

Because these fatal deficiencies were not cured, and cannot be cured by further re-pleading, Plaintiff's FAC should be dismissed with prejudice.

FACTUAL ALLEGATIONS[1]

Toolbar is software that users can download from Google and install on their computers to help them search and browse the Internet. (FAC ¶¶ 1, 14.) Once installed on a user's computer, Toolbar appears in the Internet browser (*i.e.*, Internet Explorer or Firefox), and assists users with such tasks as Internet search, spell-checking, and web page language translation. (*Id.* ¶¶ 14, 17.) Plaintiff does not (and cannot) allege that users pay any money to Google for downloading or using Toolbar.

Toolbar routinely transmits certain information to Google, including cookie information

[1] Google assumes the factual allegations to be true for purposes of this motion only.

and IP addresses. (*Id*. ¶ 18.) The FAC does not challenge these routine transmissions. When a user downloads Toolbar, he or she is given the option of enabling Toolbar's enhanced features. (*Id.* ¶ 35.) For some of Toolbar's enhanced features such as PageRank and Sidewiki to work properly, Toolbar must collect additional information regarding the sites users visit, including the URL. (*Id*. ¶¶ 37, 38(a).) Google clearly discloses this fact: the dialog box that offers users the choice to enable enhanced features discloses that "[f]or enhanced Toolbar features to work, Toolbar has to tell us what site you're visiting by sending Google the URL." (*Id.* ¶ 37; *id.* Fig. 5.)

Immediately beneath this disclosure in the enhanced features dialog box is a hyperlink to the Google Toolbar Privacy Notice, dated December 9, 2009, which also states explicitly that enhanced features "operate by sending Google the addresses and other information about the sites at the time you visit them." (*Id*. ¶ 38(a); *see also* Declaration of Brynly R. Llyr, Ex. 1 at 2.)[2] The Toolbar Privacy Notice further states that the operation of Sidewiki requires Toolbar to collect "the URL of the relevant page, the type of action you performed and the text related to that action" and the operation of PageRank requires "knowing which web page you are viewing." (Llyr Decl., Ex. 1 at 2.) In the same dialog box, beneath the "Privacy Policy" hyperlink and the explicit disclosure that transmission of URLs is necessary for enhanced features to work, users are given the option to enable enhanced features by clicking a button, labeled "enable enhanced features" in bold type, or pressing the Enter key or space bar when that button is selected. (FAC ¶ 38(d).)

Despite these disclosures, the FAC alleges that the "installation disclosures" fail to notify users of what Plaintiff characterizes as "privacy-affecting Toolbar functions." (*Id.* ¶ 40.) Presumably Plaintiff is attacking the more recent enhanced features dialog box described in the FAC because he states that the notice given by an earlier version of Toolbar's enhanced features dialog box was conspicuous, clear and robust. (*Id*. ¶¶ 33, 40.) Yet Plaintiff concedes that users consent to the collection of information related to "users' communications with other websites"

[2] Under the doctrine of incorporation by reference, the Court may consider on a Rule 12 motion those documents whose contents are referred to or alleged in the complaint and whose authenticity no party questions. *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001); *Cooper v. Pickett*, 137 F.3d 616, 622 (9th Cir. 1997).

until users attempt to disable Toolbar (*id*. ¶ 55; *see also id*. ¶ 63), and he does not allege what disclosures (if any) he reviewed when installing Toolbar, even though he alleges that the enhanced features dialog box changed over time (*see id*. ¶ 40), and that he has used Toolbar and PageRank for years (*see id*. ¶ 61).

Plaintiff's FAC is premised on alleged improper data collection, which Plaintiff characterizes as "interception" that violates federal statutes. (*See id.* ¶¶ 52, 55.) That claim focuses on one narrow issue: that for a very limited time Toolbar allegedly continued to transmit the same URL information to Google as it routinely transmitted with enhanced features activated after Internet Explorer users used one of three Internet Explorer commands, purportedly intending to disable Toolbar: (1) clicking the "X" button; (2) using Internet Explorer 8's Manage Add-Ons tool; or (3) using Internet Explorer 8's View-Toolbars or right-click options. (*Id*. ¶¶ 46-48.) Plaintiff concedes that, even for this subset of Internet Explorer users, data collection ceased after those users disabled Toolbar and then exited their current Internet browsing session. (*Id*. ¶ 48.) Furthermore, Plaintiff alleges that Google became aware of this data-collection property in approximately November 2009 but that by January 2010 such collection had ceased. Thus, he has not even alleged that Google acted knowingly outside of this limited period. (*Id*. ¶¶ 50, 54.) Plaintiff's allegations as to users generally are therefore only concerned with the purportedly knowing collection of data (1) from Internet Explorer users; (2) who used certain Internet Explorer functions to disable Toolbar during an active browser session; (3) and who then continued browsing without restarting their browser; (4) between approximately November 2009 and January 2010.

As to himself, Plaintiff's allegations are limited to the following: that he "has used Toolbar for a number of years, with PageRank enabled," and that during the Class Period, he "thought he was disabling Toolbar's data transmission functions by clicking the 'X' symbol on the Toolbar display and selecting the option to disable Toolbar operation in the current browser window." (FAC ¶¶ 61-62.) Plaintiff never alleges that he continued to browse the web after he disabled Toolbar, but before he exited his current browser session, and thus he fails to allege that Toolbar ever collected URL information even when Plaintiff purportedly thought he had disabled

Toolbar's "data transmission functions." (*See id.* ¶ 62). Furthermore, even assuming he continued to browse the web in the current browser session, Plaintiff does not allege that Google improperly used or disclosed to any third party any of his information that was allegedly collected. Nor does Plaintiff ever allege that he actually tried to uninstall Toolbar—that is, to remove Toolbar from his computer.

Where the FAC purports to lay out allegations of harm, it does so as to Toolbar users generally. (*See* FAC ¶¶ 64-81.) Toolbar is free, and Plaintiff cannot allege that he paid any money to Google for the product. To skirt this fact and in response to Google's initial Motion to Dismiss, Plaintiff developed a novel and unsupported theory that so-called "personal" information—a category of information that Plaintiff does not define—has economic value. (*Id.* ¶¶ 64-74.) Furthermore, Plaintiff's theories of harm are all factually deficient. Plaintiff never alleges that he ever used Toolbar in a way that resulted in any such "personal" information appearing in the URL or that URLs or search terms themselves constitute "personal" information. Further, the FAC never alleges that Plaintiff or any other user actually entered into an agreement with Google to exchange "personal" information for the right to use Toolbar, or that users believed they were entering into such an agreement—indeed, Plaintiff alleges that he was "unaware of [Toolbar's] collection properties." (*Id.* ¶ 63.) Further, the only "support" for Plaintiff's flawed "value-for-value" theory is a section of Google's Terms of Service that describes a different exchange altogether: the exchange of Google's services for Google's right to place advertising on those services. (*Id.* ¶ 67.) Therefore, Plaintiff offers no facts showing, even if his "personal" information had value that could stand in the place of real money, that he agreed to exchange that information for the use of Toolbar, that he ever actually made such an exchange, or that such information lost any value.

The FAC's other allegations of harm are equally deficient. Plaintiff theorizes that Toolbar users are harmed because they lose the opportunity to enter into similar exchanges with other web publishers and advertisers, and that they lose the ability they would otherwise have had to "exercise[] their rights to utilize the economic value of their information by . . . foregoing online offerings entirely." (FAC ¶¶ 68-70.) Plaintiff also asserts conclusory allegations that, as a result

of Toolbar's operation, users expended time and money investigating and attempting to mitigate the operation of Toolbar, and suffered the compromised integrity of their computers. (*Id*. ¶¶ 76-77.) But Plaintiff does not allege that he or any other users have ever tried and failed to exchange "personal" information with any "online providers and advertisers." (*Id.* ¶ 72.) Plaintiff fails even to allege when he learned of Toolbar's purported undisclosed or inadequately disclosed collection properties, or that he spent a single minute or dollar investigating or attempting to mitigate Toolbar's operation.

ARGUMENT

I. PLAINTIFF LACKS STANDING FOR ANY CLAIMS BECAUSE HE DOES NOT ALLEGE INJURY IN FACT, AS REQUIRED UNDER THE U.S. CONSTITUTION.

Plaintiff has not pled an injury in fact sufficient to confer Article III standing. Article III, Section 2 of the United States Constitution limits federal jurisdiction to actual cases and controversies. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Plaintiff bears the burden of establishing that he suffered an "injury in fact"—that is, an invasion of a legally protected interest that is (a) concrete and particularized, not merely abstract, and (b) actual and imminent, not conjectural or hypothetical. *Id*. (citations omitted). That he attempts to bring a class action makes no difference. The named plaintiff must establish that he "personally, ha[s] been injured" and thus has standing to bring the cause of action. *Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F.3d 1018, 1022 (9th Cir. 2003) (citation omitted); *see generally Lujan*, 504 U.S. at 561 n.1 ("[T]he injury must affect the plaintiff in a personal and individual way.").

The FAC's conclusory assertions of harm are factually and legally deficient even as to the putative class, but especially as to Plaintiff. Toolbar is free, and Plaintiff never alleges that he or any other user paid money to use it. Instead, he casts about for some proxy to compensate for the fact that no money ever changed hands. His first attempt is to allege that users engage in a "value-for-value exchange" with Google, trading their "personal" information for the right to use Toolbar. (*See* FAC ¶¶ 64-65.) Relying on this theory, Plaintiff alleges that Toolbar users did "not receive the full value of their exchange" when Toolbar allegedly "engage[d] in undisclosed [or] inadequately disclosed data collection." (FAC ¶ 68.) However, Plaintiff's attempt to

substitute "personal" information for money fails as a matter of law. Google is unaware of any case that has allowed Article III's injury in fact requirement to be satisfied by this type of so-called "value-for-value" exchange. *Cf. In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) ("There is . . . no support for the proposition that an [individual's] personal information has or had any compensable value in the economy at large.").

Moreover, Plaintiff's "value-for-value" theory assumes that users agree to exchange some set amount of "personal" information for the use of Toolbar, so that the collection of additional information constitutes a "raise[d] ticket price for Toolbar." (FAC ¶ 68.) This assumption is flawed in at least two respects. First, as noted in the Factual Allegations section above, the FAC merely alleges that Google's Terms of Service contain a section that never mentions personal information, but instead conditions use of Toolbar on Google's right to show advertising. (*Id.* at ¶ 67.) Moreover, Plaintiff's theory is based on flawed logic: the collection of more or less information cannot constitute a change in "price" because users do not promise to provide any particular amount of information by searching and browsing, and thus there is no set "price" to begin with.

In addition to this flawed "value-for-value" theory, the FAC contains conclusory allegations that users suffer injury in the form of opportunity costs, costs associated with investigation and mitigation, and diminished value of their computers and personal information, and further speculates upon possible harms associated with disclosure of personal information to third parties. (*Id.* ¶¶ 26-27, 69-77.) But the FAC contains no factual allegations that Plaintiff himself has suffered any actual injury or faces a risk of imminent, palpable injury. *See, e.g.*, *Birdsong v. Apple, Inc.*, 590 F.3d 955, 960 n.4 (9th Cir. 2009) (affirming dismissal of action where plaintiff alleged only a hypothetical injury and failed to allege any actual injury); *Whitson v. Bumbo*, No. C 07-05597, 2009 WL 1515597, at *5-6 (N.D. Cal. Apr. 16, 2009) (dismissing claim for lack of Article III standing). Plaintiff's only allegations as to himself are that he "used Toolbar for a number of years" and "thought he [disabled] Toolbar's data transmission functions." (FAC ¶¶ 61-62.) Thus, even assuming that any of the FAC's alleged injuries are legally viable as to users, Plaintiff fails to establish that he himself has been injured in any of

those ways. *See Gaos v. Google Inc.*, No. C 10-04809 (JW) (N.D. Cal. April 7, 2011) (dismissing claims for failure to allege injury consistent with Article III standing requirements). Plaintiff never alleges that he understood that he was providing "personal" information in exchange for the use of Toolbar or its enhanced features. Nor does Plaintiff allege that he (1) entered any "personal" searches into Toolbar; (2) visited any URLs containing "personal" information while using Toolbar; or (3) ever continued to browse online after using Internet Explorer's functions to disable Toolbar but before restarting his browser. Finally, Plaintiff never alleges that he personally took any action to investigate or mitigate Toolbar's operation, that his own personal information was disclosed to third parties, or that he was unable to use other parties' products or directly market his own personal information as a result of his use of Toolbar. Plaintiff thus offers no facts to show that the operation of Toolbar caused any injury "that is 'distinct and palpable' as opposed to merely 'abstract,' and . . . actual or imminent, nor 'conjectural' or 'hypothetical.'" *Whitmore v. Arkansas*, 495 U.S. 149, 155-56 (1990) (internal citations omitted). Because Plaintiff fails to allege injury in fact sufficient to confer Article III standing, the FAC should be dismissed in its entirety.

II. PLAINTIFF FAILS TO STATE A CLAIM FOR ANY OF HIS CAUSES OF ACTION.

The FAC also should be dismissed under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. Although factual allegations in Plaintiff's FAC are assumed to be true for purposes of this motion, "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment]' to relief requires more than labels and conclusions." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). An unadorned recitation of the elements of the claims will not suffice, and the court need not assume the truth of conclusory allegations unsupported by facts. *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1950 (2009). Rather, the FAC must allege a factual basis for each element of each cause of action. *Moss v. U.S. Secret Serv.*, 572 F. 3d 962, 969 (9th Cir. 2009).

A. Plaintiff's Claim Under The Wiretap Act Fails As A Matter Of Law.

Plaintiff's Wiretap Act claim fails because he does not plead adequate facts to establish an unlawful "interception" under the terms of the Act. The Wiretap Act is primarily a criminal statute, although it provides for a private right of action in certain limited circumstances. 18

U.S.C. § 2520(a). Plaintiff alleges Google violated two sections of the Wiretap Act: (1) Section 2511(1)(a), which provides for liability, subject to exceptions, for "any person who . . . intentionally intercepts [or] endeavors to intercept . . . any . . . electronic communication" (FAC ¶ 95); and (2) Section 2511(1)(d), which provides for liability, subject to exceptions, for "any person who . . . intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] . . . electronic communication in violation of [Subsection 2511(1)]" (*Id.* ¶ 96). Plaintiff does not claim that users' initial download of Toolbar or the election to enable Toolbar's enhanced features violate the Wiretap Act. Rather, his claim appears to focus solely on data transmissions that allegedly occurred after users utilized certain Internet Explorer functions "purporting to disable Toolbar." (*Id.* ¶ 55.)

The FAC fails to state a claim under either Section 2511(1)(a) or Section 2511(1)(d). An "interception" requires the use of a defined device. 18 U.S.C. § 2510(4). Neither Toolbar nor "Google's system," (*see* FAC ¶ 53), is a "device" for purposes of the Wiretap Act. According to the allegations of the FAC, Toolbar and "Google's system" are equipment used by Google in the ordinary course of its business. (*Id.* ¶¶ 1, 16, 19, 37-38). But the Wiretap Act expressly excludes from its definition of "device" any equipment used by a provider of an "electronic communication service" in the ordinary course of business, and without identification of a "device" that was used to acquire the contents of a communication, no interception occurred in violation of the Act. 18 U.S.C. § 2510(5).

Nor can Plaintiff establish an "interception" in violation of the Wiretap Act by alleging legal conclusions to meet the required elements: that Toolbar and "Google's system"—a vague term he fails to define—are "devices and apparatuses used to intercept, retain, and transcribe in-transit electronic communications" (FAC ¶ 53); that Toolbar "intercept[ed] and transmit[ted] users' activities" after those users employed certain Internet Explorer functions "purporting to disable Toolbar" (*id.* ¶ 55); and that "Google's interception and eavesdropping was not in its normal course of business" (*id.* ¶ 56). These conclusory assertions fail to meet the minimum pleading requirements established in *Twombly* and *Iqbal*, and they directly contradict the factual

allegations that show Plaintiff has not pled a "device" covered by the Wiretap Act because Google is alleged to be an electronic communications service provider (*id*. ¶ 51), and Toolbar and "Google's system" are used in the ordinary course of Google's business (*id*. ¶¶ 1, 19, 37-38, 53).

The "ordinary course" exclusion applies to devices that are routinely used for a legitimate business purpose. *See, e.g.*, *Hall v. Earthlink Inc.*, 396 F.3d 500, 504-05 (2d Cir. 2005); *United States v. Friedman*, 300 F.3d 111, 122 (2d Cir. 2002). Plaintiff's own allegations establish that the exclusion applies here. The collection of user data is routine. Plaintiff admits that Toolbar "routinely transmits to Google certain information," including cookie information and IP address (FAC ¶ 18), and that Toolbar's enhanced features require the transmission of certain user information, including the URL of each web page the user requests (*id*. ¶¶ 1, 19, 37-38). Plaintiff also acknowledges that the collection of user data is for a legitimate business purpose, as Toolbar's collection and transmission of users' URLs is necessary to provide the enhanced features that some users choose to install. (*Id*. ¶¶ 1, 37-38.) Indeed, Plaintiff's allegations establish that data transmission via Toolbar is not only within the ordinary course of Google's business, it is essential for Toolbar to function. (*Id.*)

The Second Circuit's decision in *Hall* is especially instructive as to why the ordinary course exclusion applies here. In *Hall*, plaintiff opened an account with defendant Earthlink Network Inc., an Internet Service Provider, for Internet services, including a personal email account. 396 F.3d at 502. Suspicious that the email account was being used to send "spam" emails, defendant terminated plaintiff's access to the account, but continued to receive emails sent to plaintiff's account. *Id.* Plaintiff alleged that defendant's continued receipt of emails constituted illegal "interceptions" under the Wiretap Act. *Id.* The court, however, held that the Wiretap Act did not apply because the alleged "devices"—routers, servers, and other equipment—were used "as part of [defendant's] e-mail service to all customers . . . in the ordinary course of its business." *Id.* at 505. The continued receipt of emails after termination of Plaintiff's account access did not transform the equipment at issue into an "electronic, mechanical, or other device," for purposes of the Wiretap Act. *Id.* at 504.

This case closely parallels *Hall*. Despite alleging facts that establish that Toolbar and

"Google's system" are used in the ordinary course of Google's business, Plaintiff argues that the intervening act of disabling Toolbar by using Internet Explorer's features somehow transformed Toolbar into a "device" under the Wiretap Act whenever user information continued to be collected in the current browser session. Like the plaintiff in *Hall*, Plaintiff is wrong. The case law does not support such an expansive interpretation of "device." *See id.* at 505 (termination of single user's access to account did not transform servers, routers, and other equipment into "devices" covered by Wiretap Act). Further, any such interpretation would be the type of "surprising and novel" interpretation of a criminal statute that is strongly discouraged under the rule of lenity. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2001) (cautioning against interpreting criminal statutes in a civil context in ways that would "impose unexpected burdens" on defendants). Plaintiff's Wiretap Act claim must be dismissed because he does not and cannot allege facts establishing that Toolbar or "Google's system" are intercept "devices" outside the ordinary course exclusion.

B. Plaintiff Fails To State A Claim For Violation Of The CFAA.

The CFAA does not fit Plaintiff's allegations at all. The CFAA was enacted to prevent computer hackers from accessing computers to steal information or to disrupt or destroy computer functionality. *See LVRC Holdings*, 581 F.3d at 1130-31. Although the CFAA is primarily a criminal statute, it creates a limited civil right of action. *Id.* at 1131; *see also* 18 U.S.C. § 1030(g). The FAC does not identify the provisions specifically, but Plaintiff appears to predicate his CFAA claim on three types of offenses: (1) unauthorized access to a protected computer and thereby obtaining information, § 1030(a)(2)(C); (2) unauthorized access with intent to defraud, § 1030(a)(4); and (3) unauthorized transmission of a program or code, § 1030(a)(5)(A). Plaintiff's CFAA claim fails because he lacks standing to bring a civil claim and because the facts as alleged show that Google did not violate the statute.

1. Plaintiff Cannot Meet The Jurisdictional Threshold Required For A Civil Claim Under The CFAA.

To have standing under the CFAA, Plaintiff must allege actual "loss," as that term is defined by the statute. 18 U.S.C. § 1030(e)(11). The loss suffered by reason of the CFAA

offense must involve the conduct set forth at 18 U.S.C. § 1030(c)(4)(A)(i)(I)-(V). The only subclause of the statute alleged by Plaintiff covers conduct resulting in "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). (*See also* FAC ¶ 103.) The statute defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

Plaintiff does not allege that he spent any money responding to the alleged violations, spent any money conducting a damage assessment, spent any money restoring the data, program, system or information to its condition before the offense, or that he incurred any other economic damages due to Google's alleged conduct. Although Plaintiff does make the conclusory allegation that he and the proposed class sustained an aggregated loss of $5,000, there are no alleged facts that Plaintiff himself incurred any loss at all. (*See* FAC ¶¶ 78, 103.) Likewise, the allegation that Google's conduct caused "users to expend money, time, and resources" fails to allege that Plaintiff himself expended money or resources. (*See id*. ¶ 76.) Plaintiff cannot state a claim without alleging individual loss. 18 U.S.C. § 1030(g) (providing right of action for persons who suffer "damage or loss"). The assertion of a class claim does not change this: "[n]amed plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.'" *Lewis v. Casey*, 518 U.S. 343, 357 (1996). Plaintiff's admission that he "would have" taken remedial measures, "had he known" of Google's alleged conduct (FAC ¶ 63), is inconsistent with any claim that he was among the "users" who allegedly were injured because of "their efforts investigating and attempting to mitigate" the data transmissions that occurred after users disabled Toolbar through Internet Explorer but before they closed their current browsing sessions (*id*. ¶ 76).

In addition, Plaintiff cannot satisfy the $5,000 loss requirement by trying to aggregate alleged loss by him related to his computer with alleged loss by other users, presumably related to

their own computers. *See Lyons v. Coxcom, Inc*., No. 08-CV-02047, 2009 WL 347285, at *8 (S.D. Cal. Feb. 6, 2009) ("Plaintiff attempts to aggregate losses of the entire class in order to meet the $5000 requirement; however, under the language of the statute, only federal prosecutors may aggregate losses across multiple protected computers from a related course of conduct."), *vacated on other grounds by Lyons v. Coxcom, Inc*., 718 F. Supp. 2d 1232 (S.D. Cal. 2009); *In re Pharmatrak, Inc. Privacy Litig.*, 220 F. Supp. 2d 4, 15 (D. Mass. 2002), *rev'd on other grounds by In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001); *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934 (9th Cir. 2004) (noting in non-class case that statute looks at "how much damage or loss there is to the victim"); *but see In re Apple & ATTM Antitrust Litig*., 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008). Because Plaintiff lacks standing to bring a CFAA claim, Plaintiff's claim under the CFAA must be dismissed.

2. Google Has Not Acted Without Authorization, Or In A Manner That Exceeded Authorization.

As a matter of law, Plaintiff cannot stretch the scope of the CFAA to encompass Google's alleged collection of information following Plaintiff's voluntary decision to download Toolbar and to opt-in to Toolbar's enhanced features. The Ninth Circuit has narrowly construed the CFAA to apply only when a defendant has not been authorized ***at all*** to obtain access to a protected computer or certain types of information, but nevertheless obtains access to such computer or information. *LVRC Holdings*, 581 F.3d at 1133-35; *AtPac, Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1180 (E.D. Cal. 2010) (recognizing Ninth Circuit's guidance that the CFAA should be read narrowly). Plaintiff's voluntary installation of Google Toolbar (FAC ¶ 14), and voluntary enabling of the enhanced features (*see id*. ¶ 61), shows that his claims are counter to the CFAA's intended scope of addressing criminal computer hacking. *See LVRC Holdings*, 581 F.3d at 1134 (stating that the CFAA cannot be interpreted in surprising or novel ways because it is primarily a criminal statute). Google did not access or transmit program or codes to Plaintiff's computer without authorization, nor did Google covertly install or operate Toolbar on Plaintiff's computer; Google did so openly at Plaintiff's prompting.

A CFAA violation for accessing or transmitting information "without authorization" occurs only where "the person has not received the permission to use the computer for any purpose." *Id.* at 1135. Because Plaintiff admitted to voluntarily downloading Toolbar and opting into Toolbar's enhanced features, Plaintiff cannot maintain a claim that Google acted "without authorization." *See id*. at 1133; *see also In re Apple & ATTM Antitrust Litig.*, No. C-07-05152, 2010 WL 3521965, at *7 (N.D. Cal. July 8, 2010) (voluntary installation of program negates "without authorization" element). The "without authorization" provision applies to outsiders, such as third-party computer hackers, who do not have permission to access the computer ***at all***. *See, e.g.*, *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 964 (D. Ariz. 2008); *AtPac*, 730 F. Supp. 2d at 1180 ("Simply put, a person cannot access a computer 'without authorization' if the gatekeeper has given them permission to use it."). To maintain such a claim, Plaintiff would have had to allege that Google had "no rights, limited or otherwise," to access or transmit to his personal computer. *LVRC Holdings*, 581 F.3d at 1133. But Plaintiff repeatedly has conceded that he granted Google access to his computer with respect to Toolbar, and even its enhanced features. (FAC ¶¶ 14, 61). Because Plaintiff's allegations show that Google did not act "without authorization," he cannot maintain claim for either unauthorized transmission under 18 U.S.C. § 1030(a)(5)(A) or "access without authorization" under §§ 1030(a)(2)(c) and (a)(4).[3]

Likewise, Plaintiff does not and cannot allege facts sufficient to show that Google violated §§ 1030(a)(2)(c) or (a)(4) by "exceed[ing] authorized access," as defined by the CFAA. *See* 18 U.S.C. § 1030(e)(6). The Ninth Circuit has interpreted "exceed[ed] authorized access" to cover "a person who . . . has permission to access the computer, but accesses information on the computer that the person is not entitled to access." *LVRC Holdings*, 581 F.3d at 1133. This requires the violator to access information or data ***beyond*** the information or data for which access was granted. "[T]he plainest and common-sense understanding of the definition of the term 'exceeds authorized access' is one that simply examines whether the accessor was entitled to

[3] Whereas sections 1030(a)(2)(c) and (a)(4) of the CFAA require that the defendant either act "without authorization" or "exceed authorized access," section 1030(a)(5)(A) requires that the defendant act "without authorization," and does not prohibit actions that exceed authorized access.

access the information for any purpose." *AtPac*, 730 F. Supp. 2d at 1181. In *LVRC Holdings*, the Ninth Circuit held that an employee who accessed his employer's documents for the purpose of stealing those documents, did not "exceed authorized access" because the employee was permitted access to the documents at issue albeit for a different purpose. 581 F.3d at 1135 n.7. This is because the CFAA, a criminal statute designed to deter computer hacking, is concerned solely with the rights of access, not the misuse of access to the information. *See Lewis-Burke Assoc. LLC v. Widder*, 725 F. Supp. 2d 187, 194 (D.D.C. 2010); *Bell Aerospace Servs., Inc. v. U.S. Aero Servs., Inc.*, 690 F. Supp. 2d 1267, 1272-73 (M.D. Ala. 2010).

In this case, Google had been granted permission to access information or data on Plaintiff's computer regarding Plaintiff's Internet browsing activities. By using Toolbar and its enhanced features, Plaintiff permitted Google to access "the addresses and other information about sites at the time you visit them." (FAC ¶ 38(a).) While Plaintiff never alleges facts sufficient to show that Google obtained any of his communications after he disabled Toolbar, Plaintiff maintains that Google exceeded its authorized access by "obtaining users' confidential Internet communications" at times after users disabled Toolbar but before they exited the current browsing session. (*Id.* ¶¶ 48, 59.) Even if Plaintiff had alleged that his own information was collected after he disabled Toolbar, those "confidential Internet communications"—that is, the URLs and other information related to websites visited by Plaintiff—are the very type of information that Plaintiff granted Google access to when he opted-in to enhanced features. There is no allegation that Google used its authorized access to obtain other types of information that it was not entitled to access. *See Univ. Sports Publ'ns Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010) (limiting "exceeds authorized access" to require allegation that violator accessed information to which it had no access rights at all).

Plaintiff maintains that by clicking the "X" symbol, Plaintiff "did not consent to data collection" after he disabled Toolbar but before he restarted his browser. (*See* FAC ¶¶ 62-63.) Nowhere does Plaintiff allege he permanently uninstalled, or attempted to uninstall, Google Toolbar from his computer. At most, he complains of Google's access to data for a limited time until the browser was closed after disabling Toolbar. Again, Plaintiff does not allege that he

continued to browse before exiting or restarting his browser. Regardless, the collection of data during the user's current browsing session is not remotely similar to the hacking that is the focus of the CFAA. Any limits Plaintiff attempted to place as to when Toolbar could collect or somehow use that information cannot transform the claim to one under the CFAA; any allegation that he did not consent to Toolbar "collecting" information after he clicked the "X" (*id.* ¶¶ 62-63), is irrelevant. *See AtPac*, 730 F. Supp. 2d at 1181 ("Plaintiff admits that . . . Nevada County had permission to access the AtPac directories and source code . . . What Nevada County chose to do once it accessed the AtPac directors . . . is irrelevant."); *Univ. Sports Publ'ns*, 725 F. Supp. 2d at 385 (holding that defendant does not "exceed authorized access" by collecting information that he was entitled to access but not collect). Plaintiff's complaint that Toolbar purportedly failed to stop collecting users' information at the precise moment users believed it had stopped does not transform the operation of Toolbar into computer hacking.

Moreover, any purported deficiency in Google's disclosures regarding the operation of Toolbar's enhanced features also cannot provide a basis for CFAA liability under any section of that statute. (FAC ¶¶ 59, 99-100.) As noted above, the CFAA is solely concerned with access to the information at issue, not the parameters or limits parties may place on the time, manner or intent of access. Thus, the CFAA does not encompass or incorporate the alleged exploitation or breach of private agreements between parties. *AtPac*, 730 F. Supp. 2d at 1182 (finding that liability under the CFAA will not reach alleged violation of licensing agreement); *United States v. Zhang*, No. CR-05-00812-RMW, 2010 WL 4807098, at *4 (N.D. Cal. Nov. 19, 2010) (finding that breach of private contract cannot be construed to constitute a violation of the CFAA); *Univ. Sports Publ'ns*, 725 F. Supp. 2d at 385 (finding that violation of confidentiality agreements does not support a CFAA claim). Under the CFAA, the relevant inquiry is whether Plaintiff allowed Google access to the computer system or information at issue, irrespective of whether Plaintiff would have revoked permission if he understood Google's alleged intent or knew about Google's alleged conduct. *See Accenture, LLP v. Sidhu*, No. C 10-2977, 2010 WL 4691944, at *4 (N.D. Cal. Nov. 9, 2010) (dismissing with prejudice claim that employee acted "without authorization" or "exceeded authorized access" where employer would have terminated employee or revoked

permission had it known employee's intent in accessing documents).

The CFAA's plain language, and the cases interpreting the CFAA, do not support Plaintiff's attempt to stretch the CFAA to cover the facts alleged. This statute was designed to address third-party computer hackers. It does not apply to the facts Plaintiff alleged, and thus the Plaintiff's claim under the CFAA must be dismissed.

C. Plaintiff's State-Law Claims Are Preempted By The Wiretap Act.

The federal Wiretap Act contains an express preemption clause: "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) (emphasis added). Federal law may, of course, expressly preempt state-law claims. *Silvas v. E*Trade Mortg. Corp.*, 514 F.3d 1001, 1004 (9th Cir. 2008). Thus, under the Act, only "those remedies outlined in the [statute] are the exclusive ones a party may pursue in court for conduct covered by the statute." *Bunnell v. Mot. Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2007) (holding that the Wiretap Act preempts state law claims; *citing Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1138 (C.D. Cal. 2006), *rev'd on other grounds by Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008)).[4]

All the state-law claims asserted here are preempted to the extent that they seek to impose liability based on the same conduct alleged with respect to the Wiretap Act. Plaintiff alleges that Google violated the Wiretap Act through its alleged "interception of electronic communications." (*See* FAC ¶¶ 51-57, 93-97.) The state-law claims incorporate the same allegations as the Wiretap Act claim. (*Id.* ¶¶ 105, 120.) For the UCL claim, Plaintiff alleges that Google violated Plaintiff's privacy by allegedly intercepting his communications and that Google misled the public and failed to disclose its alleged interceptions. (*Id.* ¶¶ 108, 111, 118.) Plaintiff's unjust enrichment claim is also based on the same conduct. (*Id.* ¶ 120.) Thus, at the core of all the claims are the allegations that Google purportedly intercepted Plaintiff's communications. Because federal law

[4] Furthermore, the detailed regulatory scheme set forth in the Wiretap Act leaves no room for supplementary state regulation. *See Bunnell*, 567 F. Supp. at 1154-55.

is the exclusive avenue for any claims regarding such conduct, the state-law claims are preempted.[5] *See Bunnell*, 567 F. Supp. 2d at 1154 (holding that Wiretap Act expressly preempted claim under California Privacy Act). Even if Plaintiff ultimately is unable to state a claim under the Wiretap Act, the state claims still are preempted. *Id.* (holding that state-law claim was preempted by Wiretap Act despite finding no violation of Act).

Although one court in this District recently found that § 2518(10) did not expressly preempt two claims under the California Penal Code, that case should not control here. *See Valentine v. NebuAd, Inc.*, No. C08-05113-TEH, 2011 WL 1296111 (N.D. Cal. Apr. 4, 2011). In *NebuAd*, the court found that § 2518(10) "does not explicitly provide for the preemption of state law, which is the bar that must be met before express preemption may be found." *Id.* at *6. However, the standard he uses for express preemption misapplies the Supreme Court language on that issue. An express preemption analysis "begin[s] with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 383 (1992) (quoting *FMC Corp. v. Holliday*, 498 U.S. 52, 57 (1990)). In this case, the statutory language is clear: for any nonconstitutional violation of the Wiretap Act, the remedies and sanctions described in the Wiretap Act provide "the ***only*** judicial remedies and sanctions." 18 U.S.C. § 2518(10) (emphasis added); *see also Bunnell*, 567 F. Supp. 2d at 1154 *and Quon*, 445 F. Supp. 2d at 1138 (holding that analogous section of the Stored Communications Act, 18 U.S.C. § 2708, expressly preempts state law claims).

D. Plaintiff Fails To State A Claim Under The UCL.

Plaintiffs' UCL claim fails not only because it is preempted, but also because Plaintiff does not allege adequately the loss of "money or property" to demonstrate UCL standing and fails to plead facts stating a substantive violation of the law.

[5] As argued in Section II.E, below, Plaintiff's claim for unjust enrichment fails because unjust enrichment is not a cause of action in California. Even if such a cause of action existed, Plaintiff's unjust enrichment claim would also be preempted.

1. Plaintiff Lacks UCL Standing Because He Has Not Lost Money or Property.

Plaintiff lacks standing to bring a claim under the UCL because he fails to allege that he "suffered injury in fact and . . . lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Recently, in *Kwikset Corp. v. Superior Court*, the California Supreme Court held that standing requires actual harm in the form of economic injury. *See Kwikset Corp. v. Superior Court*, --- Cal 4th ----, 2011 WL 240278, at *5 (Jan. 27. 2011) (requiring "loss or deprivation of money or property"). As discussed in more detail in Section I, above, Plaintiff has not established that he has suffered an injury in fact.

Unlike the plaintiff who paid money for the challenged product in *Kwikset*, Plaintiff in this case did not pay any money for Toolbar and has failed to allege facts supporting his concocted "value-for-value" theory, based on only his conclusory allegation that Toolbar users "paid" "personal" information in exchange for the use of Toolbar, as discussed in Section I, above. Furthermore, as explained in Section I, "personal" information is not automatically interchangeable with money, for the purpose of alleging an economic injury. The allegations that Plaintiff and the putative Class incurred "opportunity costs of [their] choosing to do business with Google and use Toolbar" (FAC ¶ 76), or "costs in the form of information taken" (*id.* ¶ 73), also do not establish an economic injury under *Kwikset*, because they identify no deprivation of money or property or any diminished interest in property. *See* 2011 WL 240278 at *6-7 (listing cases where plaintiffs adequately alleged loss of money or property, which contain specific allegations of loss, *e.g.*, loss of money due to overcharge or loss of property due to wrongful repossession); *Thompson v. Home Depot, Inc.*, No. 07-cv-1058-IEG, 2007 WL 2746603, at *3 (S.D. Cal. Sep. 18, 2007) ("Plaintiff's . . . argument . . . that his personal information constitutes property under the UCL, is . . . unpersuasive and also rejected."); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (unauthorized release of personal information is not a "loss of property" under the UCL). Moreover, Plaintiff never alleges that ***he*** spent any money or resources investigating or attempting to mitigate the operation of Toolbar on his own computer. (*Compare* FAC ¶ 76 (alleging generically that users suffered such harms) *with Kwikset*, 2011 WL 240278 at

*19 ("[A] private plaintiff filing suit now must establish that he or she has personally suffered much harm.").) Likewise, the FAC relies exclusively on assertions of harm to users generally (FAC ¶¶ 107, 64-81), and even those are mere recitations of legal conclusions rather than factual allegations showing actual harm. These do not satisfy the requirements of *Twombly* and *Iqbal* to plead facts demonstrating economic injury to Plaintiff, even if the Court were to find those types of expenses to be "lost money or property" within the meaning of the UCL. Because Plaintiff has not alleged facts sufficient to show lost money or property as a result of the alleged violation, his UCL claim must be dismissed.

2. Google Did Not Engage In Any Unlawful, Unfair or Fraudulent Practices.

Plaintiff also fails to state a claim under the UCL because he has not pled facts sufficient to establish that Toolbar's alleged practice of collecting users' information is not an "unlawful," "unfair," or "fraudulent" business practice, as those terms have been defined.

a. Plaintiff's Allegations Do Not Establish That Google Has Acted "Unlawfully" In Violation of the UCL.

Under the "unlawful" prong, Plaintiff alleges four predicate violations by Google: the CFAA, the Wiretap Act, Cal. Civ. Code § 17500 (False Advertising Law, or "FAL") and the California Privacy Act, Cal. Const. art. I, § 1. To the extent that Plaintiff bases his "unlawful" claim on violations of the Wiretap Act and CFAA, those claims fail for the reasons provided in Sections II.A and II.B. *See, e.g., Pantoja v. Countrywide Home Loans, Inc.*, 640 F. Supp. 2d 1177, 1191 (N.D. Cal. 2009) (rejecting claim under "unlawful" prong of UCL where court dismissed plaintiff's predicate violations); *Stearns v. Select Comfort Retail Corp.*, No. 08-2746 JF, 2009 WL 1635931, at *16 (N.D. Cal. June 5, 2009) (same).

Additionally, a Wiretap Act violation cannot serve as a predicate for a UCL violation because, as discussed in Section III.C, the Wiretap Act provides "the only judicial remedies and sanctions" for violations of that statute. *See* 18 U.S.C. § 2518(10)(c). Thus, the Wiretap Act preempts any other recovery for alleged violations of that statute, and Plaintiff should not be permitted to make an end-run on the plain language by bootstrapping a Wiretap Act claim into predicate violation for a UCL claim.

To the extent Plaintiff purports to base his "unlawful" claim on violations of the FAL or California Privacy Act, as discussed below, those claims fail to "state with reasonable particularity the facts supporting the statutory elements" of any of the alleged predicate statutory violations. *See Stearns*, 2009 WL 1635931, at *16 (citing *Silicon Knights, Inc. v. Crystal Dynamics, Inc.*, 983 F. Supp. 1303, 1316 (N.D. Cal. 1997)). Claims under each of these laws fail for this and other reasons, as explained below.

The FAL claim cannot serve as a predicate violation because the FAL requires the "intent not to sell" the subject property or services "so advertised at the price stated therein, or as so advertised." Cal. Bus. & Prof. Code § 17500. An intent not to sell something as advertised requires, of course, an intent to sell the thing in the first instance. Toolbar is not, and is not alleged to be, for sale. Moreover, Plaintiff lacks standing under the FAL and has failed to allege that he read or relied on any alleged misrepresentations or omissions.[6] (*See* FAC ¶ 118 (no allegation of reliance).) *Buckland*, 155 Cal. App. 4th at 819 (holding that the UCL and FAL have identical standing requirements); *Laster v. T-Mobile USA, Inc.*, 407 F. Supp. 2d 1181, 1194 (S.D. Cal. 2005) (dismissing plaintiffs' FAL claim because of their "fail[ure] to allege that they actually relied on false or misleading advertisements").

Plaintiff cannot predicate a UCL claim on a right to privacy under the California Constitution, which requires (1) the existence of a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious violation of that privacy interest. *See Sheehan v. S.F. 49ers, Ltd.*, 45 Cal. 4th 992, 999 (2009). Plaintiff fails to identify with particularity any legally protected privacy interest, or whether Plaintiff's expectation of privacy in that unidentified interest was reasonable, or whether Google committed a serious violation of that interest. *See, e.g., Botello v. Morgan Hill Unified Sch. Dist.*, No. C09-02121 HRL, 2009 WL 3918930, at *5 (N.D. Cal. Nov. 18, 2009) (dismissing California Constitution right to privacy claim where plaintiff failed to allege that defendants disseminated or misused plaintiff's private personal information); *Bush v. Klein*, No. C 08-3456 JF, 2008 WL 4614438, at

[6] Plaintiff's failure to establish actual reliance is discussed further in Section II.D.2.c, below.

*3 (N.D. Cal. Oct. 16, 2008) (dismissing California right to privacy claim where plaintiff failed to allege he had a reasonable expectation of privacy and failed to allege facts showing a serious violation of his privacy). Plaintiff's conclusory assertion that Google "obstructed users' rights and actual attempts to pursue and obtain the privacy promised by [Google]" does not allege facts sufficient to state a cognizable claim under the California Constitution. (*See* FAC ¶ 110.)[7]

Accordingly, this Court should dismiss Plaintiff's claim under the UCL's unlawful prong.

b. Plaintiff's Allegations Do Not Establish That Google Has Acted "Unfairly" In Violation of the UCL.

None of the tests for "unfair" practices under the UCL support liability based on the allegation that "Plaintiff and the Class Members have been misled as to the nature and integrity of [Google's] products and services" through Toolbar's "undisclosed functions." (FAC ¶ 114.) To determine whether conduct is "unfair" under the statute, several recent court decisions have applied the three-part test set forth in Section 5 of the Federal Trade Commission Act, which asks whether the alleged consumer injury is substantial, not outweighed by any countervailing benefit to consumers or competition, and one that consumers could not reasonably have avoided; other courts have applied a "tethering" test, which requires that the underlying offense violates a public policy that is "tethered to specific constitutional, statutory, or regulatory provisions," while still others have applied the older, more amorphous "balancing" test, which "weigh[s] the utility of the defendant's conduct against the gravity of the harm to the alleged victim." *See Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 256-57 (2010) (describing tests). Plaintiff revised the FAC to include inadequate conclusory allegations that the elements of these tests are met. (*See* FAC ¶¶ 112-114.) But these allegations fail.

For purposes of this motion, the Court need not determine which of these tests is appropriate because regardless of the applicable test, the California Supreme Court has cautioned that, in construing a claim under the unfair prong of the UCL, "[c]ourts may not simply impose

[7] Nor can Plaintiff overcome the deficiencies of his original Complaint by adding paragraphs 115 and 116. These paragraphs exclusively put forward legal conclusions that are insufficient under *Iqbal*. 129 S. Ct. at 1950.

their own notions of the day as to what is fair or unfair." *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 182 (1999). Likewise, a court in this District cautioned against allowing the "unfairness" prong of the UCL to be used to invite courts to "roam across the landscape of consumer transactions picking and choosing which they like and which they dislike." *Van Slyke v. Capital One Bank*, No. C 07-00671 WHA, 2007 WL 3343943, at *11 (N.D. Cal. Nov. 7, 2007). Yet that is precisely what Plaintiff asks this Court to do. Google disclosed the functions of Toolbar's enhanced features. The more recent version of Toolbar's enhanced features dialog box described in the FAC advises that "[f]or enhanced Toolbar features to work, Toolbar has to tell us what site you're visiting by sending Google the URL." (FAC Fig. 5.) Further, the Toolbar Privacy Notice states that "Toolbar's enhanced features, such as PageRank and Sidewiki, operate by sending Google the address and other information about sites at the time you visit them." (FAC ¶ 38(a); Llyr Decl., Ex. 1 at 2.) Despite these clear statements, Plaintiff alleges that he "and the Class Members have been misled as to the nature and integrity of Defendant's products and services" (FAC ¶ 114), and that Toolbar's "undisclosed functions" prevented Plaintiff from "detect[ing] the means by which Defendant was conducting itself in a manner adverse to its commitments and its users' interests" (*id*. ¶ 117). But Plaintiff does not identify any undisclosed capabilities of Toolbar. Instead, Plaintiff concedes that users consented to Toolbar's collection of data. (*Id*. ¶¶ 55, 63.) Given the disclosure of Toolbar's features, user consent, and the lack of any specificity as to his speculative assertion of harm, Plaintiff's factual allegations do not meet any of the tests because there is no substantial injury that outweighs the benefits associated with Toolbar (and that could not be reasonably avoided), nor is there any violation of a specifically-enunciated public policy "tethered to specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App. 4th at 250. In Plaintiff's opinion, Google should have given users even more detailed disclosures. He is entitled to his opinion, but his desire for even greater disclosures fails, as a matter of law, to render the current disclosures inadequate and Google's alleged practices actionable under the "unfair" prong.

c. Plaintiff's Allegations Do Not Establish That Google Has Acted "Fraudulently" In Violation of the UCL.

Plaintiff also fails to state a claim under the "fraudulent" prong of the UCL. Claims brought under this prong must be pled with particularity under Federal Rule of Civil Procedure 9(b). *See Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103 (9th Cir. 2003); *Fortaleza v. PNC Fin. Servs. Group, Inc.*, 642 F. Supp. 2d 1012, 1020 (N.D. Cal. 2009). Plaintiff's allegations do not satisfy the heightened particularity standard. Plaintiff never alleges with any particularity if and when he read the relevant disclosures regarding Toolbar, nor does he allege that he relied on any alleged representations by Google. These failures are fatal to his claim. *Pfizer, Inc. v. Superior Court*, 182 Cal. App. 4th 622, 630 (2010) (Putative class representatives "must demonstrate actual reliance on the allegedly deceptive or misleading statements, in accordance with well-settled principles regarding the element of reliance in ordinary fraud actions." (emphasis in original)). Therefore, this Court should dismiss Plaintiff's claim under the "fraudulent" prong of the UCL.

E. Plaintiff's Unjust Enrichment Claim Fails As A Matter Of Law.

Plaintiff's unjust enrichment claim fails because there is no distinct cause of action for unjust enrichment under California law. *See Melchior v. New Line Prods., Inc.*, 106 Cal. App. 4th 779, 793 (2003) ("[T]here is no cause of action in California for unjust enrichment."); *Jogani v. Superior Court*, 165 Cal. App. 4th 901, 911 (2008) ("[U]njust enrichment is not a cause of action."); *McKell v. Wash. Mut., Inc.*, 142 Cal. App. 4th 1457, 1490 (2006) (same). "Unjust enrichment is not a cause of action . . . or even a remedy, but rather a general principle, underlying various legal doctrines and remedies." *McBride v. Boughton*, 123 Cal. App. 4th 379, 387 (2004) (quoting *Melchior*, 106 Cal. App. 4th at 793). Accordingly, the Court should dismiss Plaintiff's claim for unjust enrichment because such a claim is not viable under California law

CONCLUSION

For the foregoing reasons, Google respectfully requests that the Court dismiss Plaintiff's FAC in its entirety with prejudice.

Dated: April 15, 2011

O'MELVENY & MYERS LLP

By: /s/ *Randall W. Edwards*
Randall W. Edwards
Attorneys for Defendant
Google Inc.