Michael R. Reese (State Bar No. 206773)
REESE RICHMAN LLP
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272
Email: mreese@reeserichman.com

Sanford P. Dumain
Peter E. Seidman (admitted *pro hac vice*)
Charles Slidders
Melissa Ryan Clark
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119-0165
Telephone: (212) 594-5300
Facsimile: (212) 868-1229
Email: pseidman@milberg.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

KEVIN LOW, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

LINKEDIN CORPORATION, a California Corporation, and Does 1 to 50 inclusive,

Defendants.

Case No. 5:11-cv-01468 LHK

PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION TO DISMISS THE COMPLAINT

ACTION FILED: March 28, 2011

Date: September 15, 2011
Time: 1:30 P.M.
Judge: The Hon. Lucy Koh

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Plaintiff Kevin Low ("Plaintiff") respectfully submits the following in opposition to the motion to dismiss filed by defendant LinkedIn Corp. ("Defendant"). Defendant's motion is without merit and should be denied.

INTRODUCTION AND STATEMENT OF FACTS

Consumers who use the Internet have a right to privacy and expect that businesses (and the government) are not watching their every move. This right to privacy is so important that it is protected by California's Constitution, federal law, common law, and the state consumer protection statutes at issue here. Consumers use the Internet, often from the sanctity of their own homes, to seek advice on personal and sensitive matters such as abortion, hemorrhoids, sexually transmitted disease, drug rehabilitation, or care for the elderly, to search for jobs, seek out new romantic partners, engage in political activity; in fact, to do more or less anything. Consumers do not expect this information to be broadcast to complete strangers.

LinkedIn is a web-based social networking site that allows consumers to share career information about themselves and to "link" to one another via e-mail and instant messaging services. Unfortunately for LinkedIn users, Defendant secretly shares personal information that Plaintiff and other LinkedIn users have ***not*** chosen to share with complete strangers, thereby violating the users' right to privacy. Defendant does this to increase its profits at the expense of its consumers.

Specifically, upon sign-up, LinkedIn assigns each consumer a unique User Identification number ("User Identification") that is associated with the consumer's name. ¶¶ 14-19.[1] LinkedIn is configured such that every time a link or advertisement appears on the consumer's LinkedIn webpage, the User Identification is disclosed to third-parties (advertisers, data aggregators, and the like) along with the consumer's Internet search history as recorded by secret tracking devices that third parties place on the consumers' computer.

When a user clicks a link on a LinkedIn webpage, LinkedIn sends an "HTTP Referrer" header which sends information about where the click is coming from, including what precise

[1] "¶_" are references to the paragraphs of the complaint filed on March 28, 2011 (Dkt. 1).

URL[2] (web page) the consumer was viewing at the time of the click. ¶ 16. Unbeknownst to users, LinkedIn explicitly includes users' User Identification as a "URL parameter," allowing the third party to identify the user. *Id.* In addition, because LinkedIn's URLs contain the User Identification of the member whose profile is being viewed, the third party is also able to ascertain which LinkedIn member's profile the user was viewing when the click was made. *Id.* This process allows online marketers and other data aggregators frightening access to the most intimate details of the users' lives—allowing third parties to connect personal, specific identities with the users' browsing histories.

LinkedIn engages in this conduct because the personal information at issue here is a valuable commodity, sold in the marketplace. ¶¶ 20-23. Multiple marketers have touted the high market value of this information in targeting consumers based on the data mined from their computers and mobile devices, giving credence to the statement that "the more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him." Federal Trade Commission Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change* (Dec. 2010), at 24 ("FTC Report"). ¶ 21.

One data aggregator, Audience Science, states that its work involves "recording billions of behavioral events daily and reaching over 385 million unique Internet users" and then making such data available to its clients: "web publishers, marketers, networks, exchanges, and agencies[,] to create intelligent audience segments to connect people with relevant advertising driving the transition to data-driven audience marketing online." ¶ 21.

On March 7, 2011, the *Wall Street Journal* published an article under the headline, "Web's Hot New Commodity: Privacy," in which it highlighted a company called Allow Ltd., one of nearly a dozen companies that offer to sell people's personal information on their behalf, and pay 70% of the sale proceeds to the individual. One Allow Ltd. customer received payment of $8.95 for letting Allow tell a credit-card company he was shopping a new credit card. *Id.*

[2] A URL is a Uniform Resource Identifier that specifies where a known resource is available and the mechanism for retrieving it.

Defendant's motion to dismiss is based on two arguments, both of which are wrong. First, Defendant argues that it is only disclosing "a non-sensitive number randomly assigned to plaintiff by LinkedIn." As alleged in the Complaint, however, expert studies have shown first and last names and other personal information (including address, sexual orientation, and income level) can be easily and quickly determined from User Identification numbers. Accordingly, because of Defendant's conduct, third-parties who are complete strangers to the consumer can link the consumer name with that person's search history, revealing sensitive and potentially embarrassing information.

Second, Defendant argues that even if additional personal information is being disclosed, such personal information is not "property," money, or otherwise of value. In fact, the personal information at issue in this case is part of a robust, monetized commerce that is worth hundreds of millions of dollars. By collecting personal information from the computers and mobile devices, "Websites and stores can, therefore, easily buy and sell information on visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them." ¶ 20 (quoting Joseph Turow, *et al.*, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), *available at* http://ssrn.com/abstract=1478214). Similarly, "Internet merchants may obtain a great deal of valuable marketing information from visitors who merely window-shop at their electronic storefronts. . . . This data may also be licensed or sold to third parties." Ian C. Ballon, 1 *E-Commerce & Internet Law* § 26.01, at 26-7 (2010).

Thus, LinkedIn strips individuals of the common law and constitutional right to control the personal information they reveal about themselves and to whom they reveal it. It also improperly obtains and divulges personal and embarrassing information to data aggregators who treat such information as a commodity that is valued by reference to a robust market. Accordingly, Defendant's motion to dismiss must be denied.

ARGUMENT

I. PLAINTIFF HAS ESTABLISHED ARTICLE III STANDING

Article III standing derives from separation of powers doctrine and is intended to prevent the judiciary from encroaching on the other branches by deciding political issues of general applicability. To this end, Article III standing limits the court's subject matter jurisdiction to cases or controversies that are "*justiciable*," that is, arising from a constitutional, statutory or common law violation of an individual right and, as such, capable of being appropriately decided by resolution of the particular case or controversy before the court, as opposed to issues that are political, the resolution of which are generally applicable, and properly decided by the other branches. *See* 13A Charles Alan Wright, Arthur R. Miller, *et al*., *Federal Practice and Procedure* § 3531.4 (3d ed. 2011) ("The choice is made between the importance of having the issues decided by the courts and the importance of leaving the issues for resolution by other means.").

Hence, the "standing question . . . is whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *In re Facebook Privacy Litig.*, No. 10-02389, WL 2039995, at *4 (N.D. Cal. May 12, 2011) (Ware, J.) (internal quotations and citations omitted) (holding that plaintiffs had standing); *see also Jenkins v. McKeithen*, 395 U.S. 411, 423 (1969) ("In this sense, the concept of standing focuses on the party seeking relief, rather than on the precise nature of the relief sought.").

As the United States Supreme Court has held: "[i]njury-in-fact is not Mount Everest." *Danvers Motor Co. v. Ford Motor Co.*, 432 F.3d 286, 294 (3d Cir. 2005). To the contrary, it suffices for federal standing purposes to allege some specific, "identifiable trifle" of injury. *Id*.; *See Council of Ins. Agents & Brokers v. Molasky-Arman*, 522 F.3d 925, 932 (9th Cir. 2008) (in affirming the plaintiff's standing, the Ninth Circuit court noted that the U.S. Supreme Court "has allowed important interests to be vindicated by plaintiffs with no more at stake in the outcome of an action than a fraction of a vote, a $5 fine and costs, and a $1.50 poll tax . . . . 'The basic idea that comes out in numerous cases is that ***an identifiable trifle is enough to fight out a question of principle; the trifle is the basis for standing and the principle provides the motivation.'"***)

(emphasis added). Here, where constitutional protected rights to privacy have been violated, Plaintiff's alleged injuries are certainly more than such a "trifle." ¶¶ 1-2; 20-23.

The determination of whether a plaintiff has standing is separate and preliminary to the issue of whether the plaintiff pleaded a cause of action. *Meaunrit v. ConAgra Foods Inc.*, No. 09-2220, 2010 WL 2867393, at *4 (N.D. Cal. July 20, 2010) ("While [defendant] may indeed be correct that there is no cognizeable cause of action in this case - i.e., there was no actionable misrepresentation - this is not the same thing as finding the plaintiff lacks standing. Plaintiff alleges an injury, and alleges that it was caused by defendant's actions. ***Asking whether or not she has a legally cognizable claim is not the same thing as asking whether she has suffered an injury in fact***.") (emphasis added). *See also Davis v. Passman,* 442 U.S. 228, 239 n.18 (1979) (court of appeals improperly confused the question of standing with the question of whether plaintiff had a cause of action). Sufficiently alleging injury in fact creates a justiciable issue that allows the court to advance to the merits inquiry.

Plaintiff's allegations of personal injury arising from LinkedIn's misconduct raise a justiciable issue that the court has subject matter jurisdiction to decide. There is no constitutional or factual basis for depriving Plaintiff access to this Court, the only venue for resolution available to them. The best Defendant can do in the face of these well-established principles is to ignore allegations that run counter to its argument. Def. Br. at 6-8. In fact, the Complaint alleges, with specificity, legal harm sufficient to confer standing. ¶¶ 1-2, 20-23.

The recent Ninth Circuit case of *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), is on point here. In *Krottner*, plaintiffs alleged that Starbucks had violated their privacy in that it failed to encrypt personal information regarding plaintiffs on a company laptop that was stolen from a Starbucks store. Defendant moved to dismiss, arguing that the plaintiffs did not have Article III standing. The Ninth Circuit rejected this argument, stating: "we hold that Plaintiffs-Appellants, whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III, Section 2 of the U.S. Constitution." *Id.* at 1140; *see also Pisciotta v. Old Nat'l Bancorp,* 499 F.3d 629, 634 (7th Cir. 2007) (reasoning that person who

had his private information taken without plaintiff's permission, but not misused, had standing under Article III).

Hence, under the governing authority of *Krottner*, Plaintiff clearly has Article III standing. Accordingly, Defendant's argument to the contrary should be denied.[3]

II. LINKEDIN VIOLATED THE RIGHT TO PRIVACY ARISING FROM CALIFORNIA'S STATE CONSTITUTION AND COMMON LAW

Defendant tries to trivialize the effects of LinkedIn's invasion of privacy by suggesting that it is nothing more than disclosure of Plaintiff's LinkedIn User Identification, which Defendant describes as a "a non-sensitive number randomly assigned to plaintiff by LinkedIn." Def. Br. at 20. The Complaint, however, clearly alleges not just that LinkedIn's invasion of privacy is far more serious than disclosure of a User Identification, but also that it amounts the very type of "serious" invasion of privacy that Article 1, Section 1 of California's Constitution, as amended, was intended to prevent.

It was voters who were alarmed that "[c]omputerization of records makes it possible to create 'cradle-to-grave' profiles on every American" and believing that such "data collecting is threatening to destroy our traditional freedom" who amended California Constitution's Article 1, Section 1 ("the Privacy Initiative") to recognize a right to privacy. Official Ballot Pamphlet at 26.

---

[3] Defendant's reliance on *La Court v. Specific Media, Inc.,* No. 10-1256, 2011 WL 2473399 (C.D. Cal. Apr. 28, 2011), is misplaced. (Def. Br. at 7). Unlike Plaintiff here, the *Specific Media* plaintiffs referred to a host of facts, including facts pertaining to the value of their personal information, "not contained in their [c]omplaint *at all*." *Id.* at *4 (emphasis added). An amended complaint was filed shortly after the dismissal without prejudice and took into account the admonitions of the Court, which in no way foreclosed the possibility of such theories of harm giving rise to Article III standing. The *Specific Media* Court recognized the viability in the abstract of such concepts as "opportunity costs," "value-for-value exchanges," "consumer choice," and other concepts referred to in plaintiffs' opposition brief, and therefore allowed the plaintiffs to amend their complaint. *Id.; see also id.* at *6 ("It is not obvious that [p]laintiffs cannot articulate some actual or imminent injury in fact").

Defendant's citation to *Robins v. Spokeo, Inc.,* No 10-5306, 2011 WL 597867, at *1 (C.D. Cal. Jan. 27, 2011) (Def. Br. at 7), is also inapposite because, as Defendant acknowledges, *id.*, that case dealt with concern that defendant's website would adversely affect him in future, whereas Plaintiff in this case alleges past, current and ongoing injury. LinkedIn's reliance on the non-binding case of *In re DoubleClick Inc. Privacy Litigation,* 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (Def. Br. at 7), is also misplaced because the *DoubleClick* court did not analyze the issue of standing.

This Court should interpret the Privacy Initiative to give effect to the intent of California voters, which was expressed in the Privacy Initiative as follows:[4]

> The principal focus of the Privacy Initiative is readily discernable. The Ballot Argument warns of unnecessary information gathering, use and dissemination by public and private entities -- images of "government snooping," computer stored and generated "dossiers" and "'cradle-to-grave' profiles on every American" dominate the framers' appeal to the voters.… The evil addressed is … business … "collecting and stockpiling unnecessary information … and misusing information gathered for one purpose in order to serve other purposes or to embarrass …"

Hill v. NCAA, 865 P.2d 633, 645 (Cal. 1994) (quoting Official Ballot Pamphlet at 26-27). Plaintiff alleges that LinkedIn knowingly linked its users' identifications to secret tracking devicess, thereby enabling the "collecting and stockpiling" of personal information, not submitted for that purpose, to create "dossiers" about the Plaintiff and Class Members for sale to marketers. This is the precisely the type of conduct California voters intended to prevent.[5]

Defendant's reliance on *Ruiz v. Gap, Inc.,* 540 F. Supp. 2d 1121 (N.D. Cal. 2008) and *Folgelstrom v. Lamps Plus Inc.,* 195 Cal. App. 4th 986 (2011), and *Hill*, *supra*, is misplaced. Def. Br. at 20. Those cases involved disclosure of a single piece of unlinked information (social security numbers or ZIP codes). In contrast, LinkedIn has disclosed its users' identifications in conjunction with their browsing history, thereby enabling third parties to "stockpile" information about the user's most personal habits and preferences (derived from their browsing history) and create the type of personal "dossier" the Privacy Initiative was intended to prevent.[6]

---

[4] *See Lungren v. Deukmejian*, 45 Cal. 3d 727, 740 n.14 (1988) ("The rule that the ballot pamphlet is an important aid in determining the intent of the voters in adopting a constitutional amendment or statute is too well settled to require extensive citation of authority.").

[5] If the Court questions the "seriousness" of LinkedIn's conduct, it should consider its ramifications. For instance, the voters of California intended that the right to privacy also protect "our freedom to associate with the people we choose." Official Ballot Pamphlet at 28. The Supreme Court has also "recognized the vital relationship between freedom to associate and privacy in one's associations." *NAACP v. State of Alabama,* 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."). Here, LinkedIn is disclosing a User Identification connected to a web browsing history that may disclose information about the users' associations, including membership in, or an interest in, dissident groups.

[6] Defendant's contention with respect to the common law invasion of privacy claim, that its conduct is not "highly offensive to a reasonable person," also is unavailing. It goes without saying that a reasonable person would be highly offended by somebody eavesdropping on their

III. PLAINTIFF HAS ALLEGED A CLAIM FOR UNJUST ENRICHMENT

LinkedIn asserts that Plaintiff's unjust enrichment claim should be dismissed because "there is no independent cause of action for unjust enrichment in California." Def. Br. at 24. This Court, however, has recently noted that although it is "technically true" that there is no cause of action for unjust enrichment in California, "courts have held that unjust enrichment is equivalent to restitution and have allowed litigants to seek restitution using an unjust enrichment claim." *SOAProjects, Inc. v. SCM Microsystems, Inc.*, No. 10-1773, 2010 U.S. Dist. LEXIS 133596, at *24-25 (N.D. Cal. Dec. 7, 2010) (Koh, J.) (internal citations omitted).

Defendant's assertion that the unjust enrichment claim should be dismissed because the Plaintiff also alleges a breach of an express contract, Def. Br. at 24, is meritless. As this Court noted, "restitution may be awarded in lieu of breach of contract damages when the parties had an express contract, but it was procured by fraud or is unenforceable or ineffective for some reason." *SOAProjects,* 2010 U.S. Dist. LEXIS 133596, at *25 (internal quotations omitted). Accordingly, the motion to dismiss the unjust enrichment claim should be denied.

IV. PLAINTIFF STATES A CLAIM UNDER THE STORED COMMUNICATIONS ACT

Defendant attempts to escape liability for its misconduct by taking advantage of the technical complexities of the Electronic Communications Privacy Act ("ECPA") and the Stored Communications Act ("SCA" or the "Act"). *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) ("[T]he intersection of [the Wiretap and Stored Communications Acts] 'is a complex, often convoluted area of law.' . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework . . .") (citations omitted). In

---

Internet browsing, an activity that is often conducted in the privacy of one's home and behind closed doors, on a computer that is password protected, or on mobile devices—perhaps also password protected and, in all cases, inaccessible to public view.

In any event, whether LinkedIn's conduct is "highly offensive" or a serious invasion of privacy involves factual issues not ordinarily decided on a motion to dismiss. *See Gilmore v. Union Pac. R.R. Co.*, No. 09-2180, 2009 U.S. Dist. LEXIS 111740, at *22-23 (E.D. Cal. Dec. 1, 2009) ("Whether plaintiff had a reasonable expectation of privacy in the circumstances and whether defendant's conduct constituted a serious invasion of privacy are mixed questions of law and fact."); *Taus v. Loftus*, 40 Cal. 4th 683, 737 (2007) ("The question remains whether a trier of fact properly could determine that the alleged conduct here at issue constituted 'highly offensive conduct' that can be the basis for tort liability").

enacting the SCA, however, the Senate made clear its intention to protect users' communications as technology evolved, stating: "the law must advance with technology" to avoid "promot[ing] the gradual erosion of this precious right [to privacy]." S. Rep. No. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559. Despite this express intention, Defendant argues for dismissal of Plaintiff's SCA claim. However, as seen below, Defendant's arguments are in error and should be denied.

First, LinkedIn presents a tortured interpretation of the SCA that would effectively nullify the statute—a result Congress obviously never intended. It argues that any communication that is wrongfully divulged via a transmission is outside of the scope of the SCA, because the SCA only applies to stored communications, not transmissions. Def. Br. at 9-10. That argument would render the SCA meaningless, as all communications under the SCA must somehow be "divulged," i.e., shared with a third party via a transmission. Furthermore, Defendant's arguments regarding electronic storage ignore Plaintiff's allegations that LinkedIn functions not only as an "electronic communications service" (ECS), which can be held liable for divulging communications that are "stored" by the provider, but also as a "remote computing service" (RCS), for which liability attaches when the provider divulges communications that it "carried or maintained."

Second, LinkedIn denies that any of the divulged information qualifies as "contents" of the communication. "Contents," however, are defined broadly by the ECPA, and include any data or information that goes to the "substance, meaning, or purport" of a communication. In light of the context alleged here, wherein third party advertisers and data aggregators are using users' information to create demographic profiles and monitor web use patterns, the identity of the user is the exact "substance" or "meaning" that the third parties hope to attain. Moreover, Defendant does not even address the alleged disclosure of Plaintiff's last-viewed page, which is undoubtedly the "content" of a communication.

Third, LinkedIn argues that, as the service provider for the communications, it was permitted to access the stored communications. Def. Br. at 10-11. LinkedIn, however, did not merely *access* communications, it wrongfully *divulged* them to third parties.

Finally, Defendant claims, speciously, that the third parties were "addressees or intended recipients" of Plaintiff's personal information. Plaintiff, however, did not know this information was being divulged, let alone did he "address" or "intend" to disclose the information to third parties. LinkedIn's implication that the third parties are "addressees or intended recipients" because *LinkedIn,* not Plaintiff, intended to send them the divulged information assumes that Plaintiff is to have no effective control over what information he sends to whom. Such a reading is clearly contradictory to the entire purpose and intent (as well as the plain language) of the SCA, which plainly prohibits service providers from divulging users' information.

For these reasons, as discussed in detail herein, Plaintiff's SCA claim must be upheld.

A. Provisions of the ECPA

The ECPA protects electronic communications from interception during transfer (via Title I, the Wiretap Act) and from unauthorized access or disclosure (via Title II, the SCA). The SCA, the portion of the ECPA applicable here, prohibits ECSs, which provide "the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15), from divulging "the contents of a communication *while in electronic storage*," 18 U.S.C. § 2702(a)(1) (emphasis added). An RCS, which provides "computer storage or processing services by means of an electronic communications system," 18 U.S.C. § 2711(2), is prohibited from divulging "the contents of any communication which is *carried or maintained on that service* . . . ," 18 U.S.C. § 2702(a)(2) (emphasis added). "[E]lectronic communication[s]" are defined broadly under the ECPA to extend beyond e-mails and other messages and include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature . . . ." 18 U.S.C. § 2510(12).

B. The Divulged Information is a "Stored Communication" Under the SCA

Defendant attempts to evade liability under the SCA by contending that "the [SCA] protects only electronic communications held *in storage*" and not the alleged "*transmissions* of data," for which Defendant claims the Wiretap Act would apply. Def. Br. at 9 (emphasis in original). But "electronic storage" includes even the "temporary [or] intermediate storage" of a communication that is "incidental to the electronic transmission thereof," as well as storage for "backup protection." 18 U.S.C. § 2510(17). Congress specifically disavowed any "inten[tion] to

limit the term[] 'electronic storage'. . . to any particular medium of storage." H.R. Rep. No. 99-647, at 39 (1986).

The divulged communications did not, as Defendant seems to suggest, exist in some ethereal location in "cyber space." The User Identification and last-viewed page were stored on LinkedIn's servers and/or carried on its network[7]--a fact which Defendant does not deny. LinkedIn acknowledges in its prospectus that it stores information, stating: "Our solutions involve the ***storage*** and transmission of members' and customers' information, some of which may be private, and security breaches could expose us to a risk of loss of this information, which could result in potential liability and litigation." LinkedIn Corp., Prospectus (Form 424B4) (May 18, 2011) at 14 (emphasis added). Moreover, Defendant's own authority (Def. Br. at 9) makes clear that that the communications were divulged while "in storage." *See Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 450 (C.D. Cal. 2007) ("The Ninth Circuit has held that the Wiretap Act applies only to 'acquisition *contemporaneous with transmission*[.]'. . . Communications are in 'electronic storage' under the SCA, and outside the scope of the Wiretap Act, even where the storage is transitory and lasts for only a few seconds.") (citations omitted).

In the face of this authority, the SCA's plain language, and its own admission in its prospectus, Defendant fixates on Plaintiff's allegation that LinkedIn wrongfully "transmitted" user information to third parties. Def. Br. at 9. But the Complaint alleges the "transmission" of information only insofar as LinkedIn improperly sent or divulged user information to third parties. *See* ¶¶ 2, 15-18. The Complaint makes no allegations that this information was "intercepted," but instead alleges that LinkedIn divulged the contents of communications already in its possession.[8]

---

[7] *See Konop*, 302 F.3d at 874, 876, 879 n.6 ("A website consists of electronic information stored by a hosting service computer or 'server'"; "website owners . . . transmit electronic documents to servers, where the documents are stored. If a user wishes to view the website, the user requests that the server transmit a copy of the document to the user's computer"; "electronic communications are stored at various junctures in various computers between the time the sender types the message and the recipient reads it.").

[8] *See, e.g., Crowley v. CyberSource Corp.,* 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (finding that the electronic communication did not fall within the Wiretap Act because "[the user] sent certain information to [the service provider], which then conveyed it to [a third party]. . . . [The service provider] did not, however, 'intercept' the communication within the meaning of the Wiretap Act, because [the Service Provider] did not acquire it using a device other than the drive

Courts have expressly rejected Defendant's suggestion that documents are not "in storage" pre- or post-transmission.[9] The SCA would have no effect if every communication that was divulged via transmission fell outside of its scope.[10]

C. LinkedIn Also Operated as a RCS and was Precluded from Divulging Communications Regardless of Whether they were "Stored"

Even if LinkedIn prevailed on its argument that the communications it divulged were not in "electronic storage," it would not be relieved of SCA liability because Plaintiff also alleges that LinkedIn is an RCS (¶ 43),[11] as to which the "electronic storage" requirement is inapplicable. Rather, an RCS can be held liable for divulging communications which it "*carried or maintained*," if "received by means of electronic transmission . . . solely for the purpose of providing *storage or computer processing services* . . . ." 18 U.S.C. § 2702(a)(2) (emphasis added). The communications here were transmitted to, and carried by, LinkedIn for the purpose of providing

---

or server on which the e-mail was received." Also, reiterating the Ninth Circuit's position that "some storage is essential to communication via e-mail.").

[9] *See, e.g., United States v. Councilman*, 418 F.3d 67, 77-78, 79 (1st Cir. 2005) (finding, in context of the Wiretap Act: "Congress sought to ensure that the messages and by-product files that are left behind after transmission, as well as messages stored in a user's mailbox, are protected from unauthorized access. . . . [I]t appears that Congress had in mind these types of pre- and post-transmission 'temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,' *see* 18 U.S.C. § 2510(17), when it established the definition of 'electronic storage.' Its aim was simply to protect such data.") (citing, *e.g., In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 21 (1st Cir. 2003) (a rigid 'storage-transit dichotomy ... may be less than apt to address current problems.'") (other citations omitted)).

[10] Under Defendant's reading, the only way that the SCA could ever apply would be if the service provider divulged the communication by allowing an in-person view of its computer screen, or perhaps by printing a hard copy of the communication.

[11] LinkedIn operates as both an ECS and an RCS because it offers private messaging services, like an ECS, as well as public posting abilities and biographical data storage, like an RCS. ¶¶ 42, 43. *See, e.g., Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 990 (C.D. Cal. 2010) (noting that private mail and messaging falls with the scope of an ECS, and holding in the alternative that social networking sites are also RCS providers, at least with regard to postings or information that are accessible to a limited number of users, and stored by the social networking site, like videos, wall postings, and comments.); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1215-16 n. 48 (Aug. 2004) (". . . the SCA allows both protected categories [RCS and ECS] to apply to the same provider . . . . Focusing on the provider's status in the abstract would create major gaps in the statute. . . .").

computing services (i.e., to identify the user, and to display webpages to the user). Indeed, Defendant's prospectus acknowledges that, in addition to storing information, LinkedIn processes information, stating, in part: "We ***process, store*** and use personal information and other data. . . ." LinkedIn Corp., Prospectus (Form 424B4) (May 18, 2011), at 15 (emphasis added). Thus, while these communications were stored, at least temporarily, Defendant also acted as an RCS and is liable regardless of whether the information was stored.

D. LinkedIn Impermissibly Divulged "Contents"

Defendant alternatively argues that "no communications content is at issue" because the divulged information amounts to merely "non-content records." Def. Br. at 11. The SCA's far-reaching definition of "contents," however, includes "information concerning the substance, purport, or meaning of that communication," 18 U.S.C. § 2510(8), as distinguished from the mere "existence of the communication or transactional records about it,"[12] 1986 U.S.C.C.A.N. 3555, 3567. "[T]he line between the two occasionally blurs." Kerr, *User's Guide, supra*, 72 Geo. Wash. L. Rev. at 1228.[13] It is not the communication's type (e.g., data, signals, intelligence) that defines whether it includes "contents," but is instead the communication's "functional role" that "explains the different treatment that the two categories receive in the SCA." *Id.*

[12] In other words, the "information about the communication that the network uses to deliver and process the content information." Kerr, *User's Guide, supra,* 72 Geo. Wash. L. Rev. at 1228.

[13] Citing Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 645-46 (2003) ("The conceptual difficulty is that the legal categories of 'contents' and 'addressing information' . . . can be quite murky when considering human-to-computer communications. . . . When an Internet user surfs the web, he sends commands to his computer directing it to send commands to the host computer . . . . We can look at the user's command in two ways: either the command is the 'content' of the communication between the user and his computer or it is merely 'addressing information' that the user entered into his computer to tell the computer where it should go and what it should do. . . ." Here, the personal information divulged by LinkedIn does not merely serve the purpose of "tell[ing] the computer where [the communication] should go and what it should do," but conveys "substance" and "meaning" to advertisers regarding the user's browsing patterns, interests, and identity).

1. The User Identification Fits Squarely Within the Definition of Content

Here, LinkedIn improperly divulged Plaintiff's User Identification to its third party advertisers and advertising data aggregators. The very business goal of these companies (and indeed, the purpose of the secret tracking devices and beacons that these third parties place on users' computers) is to create a profile of the type of person, so as to target advertising based on demographic information. ¶¶ 9-13. The business is lucrative; these third parties pay LinkedIn for the privilege of advertising on its site, and in turn, sell user information and demographic profiles. Certainly, in the context of such profiling, the identity of the user and his/her demographic information is the "substance, purport, or meaning" of the communication. While names are frequently considered "non-content records," the context of the communication dictates otherwise here. The H.R. Report made clear:

> Under [the definition of contents], a service provider is ***allowed to divulge mailing lists*** that identify persons fitting broad demographic criteria. Unless otherwise authorized, ***service providers may not divulge to third parties information that profiles the activities of individual subscribers*** through the divulgence of the contents of a communication.

H.R. Rep. No. 99-647, at 64 (emphasis added). Given the "functional role" of the communication, the User Identification plainly qualifies as "contents."

2. Plaintiff's Browsing History Is Also "Content" of a Communication

Contrary to Defendant's statement that "plaintiff simply alleges that LinkedIn has disclosed his 'personal identity' in the form of a User ID within a URL," (Def. Br. at 12), the Complaint alleges that LinkedIn also disclosed the most recent webpage that the user viewed. *See* ¶¶ 15, 16 ("LinkedIn . . . add[s] 'social' information such as the name of each user and the other LinkedIn profiles they view and interact with," "the 'HTTP Referrer' header [] tells the third party what precise URL the user is looking at" and "allow[s] third parties to see . . . which other LinkedIn profile pages each of those users is looking at and interacting with."). Defendant does not—and cannot—attempt to categorize Plaintiff's browsing history as "record" information that can permissibly be disclosed. When the Ninth Circuit allowed the disclosure of record information in

United States v. Forrester, 512 F.3d 500 (9th Cir. 2008), it reasoned, in part, that the information did not disclose "the contents of [] messages ***or [] the particular pages on the websites*** the person viewed." (emphasis added). Here, LinkedIn divulged such content.

3. Records Cannot Be Disclosed When Accompanied by Content

Even if the User Identification was interpreted as a "record," Defendant was still prohibited from disclosing that record in connection with a substantive communication. The SCA allows a provider to "divulge a record . . . (***not including the contents of communications***. . .)." 18 U.S.C. § 2702(a)(3) (emphasis added). This plain language prohibits disclosing those records "including," i.e., together with, contents. *See, e.g., United States v. Davis,* Crim. No. 10-339, 2011 WL 2036463, at *4 (D. Or. May 24, 2011) ("Basic subscriber data which identifies a call's origination, destination, duration, and time of call enjoy no privacy protection because the data is *incidental* to the [communication], and *contains no content information.*") (citing *United States v. Reed*, 575 F.3d 900, 914–16 (9th Cir. 2009)) (emphasis added). Defendant concedes that the records exception applies to "information that ***only reveals that a communication occurred*** (and between or among whom), without revealing what was said or communicated." Def. Br. at 12 (emphasis added). Here, however, LinkedIn disclosed records, not in an isolated context such as a mailing list "fitting broad demographic criteria," but in connection with a communication, "divulg[ing] to third parties information that profiles the activities of individual subscribers. . . ." *See* H.R. Rep. No. 99-647, at 64.

Defendant's cited authority on this issue is unavailing. In *Forrester*, 512 F.3d at 510 (Def. Br. at 12), the Court found that there was no Fourth Amendment expectation of privacy for IP addresses or email addresses because users "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. . . . [They] are ***voluntarily turned over*** in order to direct the third party's servers." (emphasis added). Here, however, Plaintiff never voluntarily turned over information; he merely clicked on a LinkedIn webpage. While Plaintiff may have expected that his IP address would be used in connection with that page visit, no reasonable person would have expected that his User

Identification or browsing history would also be transmitted, nor was such information required for LinkedIn to direct the communication.[14]

The Ninth Circuit compared "records" to the address on physical mail, stating: "At best, the [third party] may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed." *Forrester*, 512 F.3d at 510. LinkedIn takes this several steps further, however: 1) Defendant sends the User Identification *with* an otherwise anonymous communication (the click), eliminating the need for any "speculation" regarding the content of the identified-person's communications; 2) Defendant contemporaneously sends the user's last-viewed page along with its User Identification, plainly divulging additional, protected content; and 3) Defendant transmits this information to its paid advertisers, who employ beacons and secret tracking devices to monitor browsing history.

Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105 (E.D. Mich. 1998) (Def. Br. at 12), is also inapplicable. That case involved a particularly egregious set of facts wherein a user publicly, but anonymously, posted a malicious and defaming post while posing as (and providing contact information for) another person. The court declined to hold the defendant liable for revealing the identity of the user, in compliance with a subpoena. *Id.* at 1108.

The facts here are distinguishable from those in *Jessup* in a number of regards.[15] First, there is no public interest served by disclosing the identities of LinkedIn users, as there might have been in disclosing the identity of a malicious, anonymous poster. Second, in *Jessup*, the third party (and the public) already had possession of the contents of the communication, and sought only to place

---

[14] Similarly, in *Hill v. MCI WorldCom Communications, Inc.,* 120 F. Supp. 2d 1194 (S.D. Iowa 2000), the defendant divulged telephone transaction records (phone numbers and billing information) which were neither content in that context nor divulged in connection with content. Here, however, LinkedIn transmitted the User Identification *with* a communication (the click to visit/interest in a webpage), and simultaneously included contents of an unrelated communication (the last-viewed page).

[15] Plaintiff also respectfully asserts that the non-controlling decision in *Jessup* was misplaced and does not comport with the plain language of the statute.

a name with an anonymous posting. *Id.* Here, by contrast, LinkedIn wrongfully divulged information that Defendant has not disputed is "contents" (the last-viewed page), *with* the user's identifiable information. Third, and perhaps most alarmingly, the defendant in *Jessup* paired record information with communications conveyed through the defendant's communications service; while here, LinkedIn paired the user's identity with the user's ongoing browsing history, i.e., communications between the user and various websites and companies, made without any participation by, use of, or communications with LinkedIn.

E. The Third Parties Were Not an "Addressee or Intended Recipient" of the Divulged Information

Finally, Defendant asserts that its misconduct is "permissible under SCA because . . . any disclosure was made to the 'addressee or intended recipient' of the communication." Def. Br. at 13 (citing 18 U.S.C. § 2702(b)(1)). Defendant illogically concludes that the allegation that "LinkedIn violated the SCA by transmitting plaintiff's User ID to third parties" is an "admission [that] these third parties are the 'addressee or intended recipient' of the purported communication."[16] Id. Defendant's reasoning is fundamentally flawed: ***LinkedIn*** may have intended to send the browsing history and User Identification to a third party, but the ***Plaintiff*** did not. LinkedIn cannot reasonably argue that the SCA permits a communications service provider to divulge users' communications as long as it does so intentionally. Such misconduct is plainly prohibited. 18 U.S.C. § 2702.

[16] In support of its argument, Defendant cites *Facebook,* 2011 WL 2039995 (a decision that Defendant, earlier in its brief, contends is poorly reasoned, Def. Br. at n.3). In *Facebook,* plaintiffs failed to articulate that the name, user ID, and browsing history of the person sending the message were not a part of the "communication" that the user intended to send to the third party. *See id.* at *6, 9, 10, 17 (Court granting plaintiffs "leave to amend to allege specific facts showing that the information allegedly disclosed by Defendant was not part of a communication from Plaintiffs to an addressee or intended recipient of that communication"). Here, Plaintiff alleges that the User Identification and prior browsing history were impermissibly divulged, and there is no suggestion that they were part of any intended communication from the user to the third parties.

F. Defendant's Misconduct is not Excused by the Service Provider Exception

Defendant contends that "the User ID is assigned by and belongs to LinkedIn[17] . . . and the SCA does not limit LinkedIn's access to its own systems." Def. Br. at 10 (citing 18 U.S.C. § 2701(c)(1)). While the SCA exempts *searches* of stored data by ECSs—the Complaint alleges that LinkedIn did far more: it *divulged* stored data to third parties. *See, e.g.*, ¶¶ 15-19. Defendant's cited authority makes clear that the "service provider exception" is limited to *access*--not *disclosure*--of information in the service provider's possession.[18] *E.g.*, *Crowley,* 166 F. Supp. 2d at 1272 (allowing "*access* to [service provider's] own systems, and declining to hold service provider liable for SCA violation because it was neither an ECS nor RCS covered by the Act) (emphasis added); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003) (allowing an insurance company to *search* emails on its own server); *see also*, 18 U.S.C. § 2702(a)(2).

LinkedIn violated the SCA by divulging Plaintiff's communications, is not covered by any exceptions to the SCA, and its motion to dismiss must be denied.

V. LINKEDIN VIOLATED CALIFORNIA CONSUMER PROTECTION LAWS

A. Plaintiff Has Adequately Pleaded Lost Money or Property for the Purpose of the UCL and FAL

Plaintiff already has demonstrated that he suffered an injury-in-fact for the purposes of the Article III standing requirement. *Supra, sec.* I. Defendant's arguments notwithstanding (Def. Br. at 14), Plaintiff also has adequately pleaded injury in the form of the loss of money or property, the value of which is determinable by reference to prices set in an active market for personal profiles.

---

[17] The representation that the User Identification is "assigned by and belongs to LinkedIn" trivializes the importance of the personal, private information that the user has entrusted to LinkedIn, and with which LinkedIn has tied to that User Identification. Revealing the User Identification carries with it a tremendous amount of information, especially in light of LinkedIn's transmission of the last-viewed page, and its use of advertisements that utilize secret tracking devices on its website.

[18] Moreover, the "service provider exception" applies only to ECSs, 18 U.S.C. § 2702(c)(1). As discussed above, LinkedIn also functioned as an RCS.

"Data is currency," according to then-FTC Commissioner Pamela Jones Harbour. *FTC Roundtable Series I on Exploring Privacy* (Matter No. P095416), Dec. 7, 2009, at 2. In *Property, Privacy, and Personal Data*, Berkeley School of Law Professor Paul M. Schwartz wrote:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

117 Harv. L. Rev. 2055, 2056-57 (May 2004).

Active markets define values for a wide range of personal information. For example, full social networking credentials can be worth between $1 and $35. Thorsten Holz, *et al., Learning More About the Underground Economy: A Case Study of Keyloggers and Dropzones*, University of Mannheim, Laboratory for Dependable Systems (2008) ("[E]ach credential is a marketable good that can be sold in dedicated forums.").

"Personal information is now a valuable commodity, with readily available market prices." Luiz Salazar, *Privacy And Bankruptcy Law, Part I: Technology Explosion Creates Personal Privacy Tension*, Am. Bankr. Inst. J. (Nov. 2006), at 18; *see also* John T. Soma, *et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1, 14 (2009), *available at* http://law.richmond.edu/jolt/v15i4/article11.pdf ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets . . . . Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L.J. 2381, 2402 (July 1996) ("[P]articularized information is a commodity that can be sold in a well developed market. . . . Therefore, the typical transaction between a merchant or seller and a consumer increasingly can be characterized as an exchange of goods or services for money *and information*.").

Accordingly, in *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1113-14 (N.D. Cal. 2010), the Court denied a motion for summary judgment on the pleadings with respect to CLRA and UCL

claims for the disclosure of users' personal information. The court found that the plaintiffs suffered injury resulting from AOL's disclosure of confidential member information. *Id.* at 1111.

B. Plaintiff Alleged Reliance for the purpose of UCL and CLRA

Contrary to Defendant's contention, (Def. Br. at 16) Plaintiff adequately pleaded reliance to his detriment by alleging that "[h]ad Plaintiff known that Defendants would share his personally identifiable information with third parties, he would not have purchased or used [ ] Defendants' services…" ¶ 64. This establishes that Plaintiff relied upon, and believed, that Defendant would not share his personally identifiable information for the purposes of the UCL and CLRA claims. *Shin v. BMW of N. Am.*, No. 09-0398, 2009 U.S. Dist. LEXIS 67994, at *7 (C.D. Cal. July 16, 2009) ("For purposes of pleading a fraudulent omissions claim under the UCL and CLRA, a plaintiff satisfies the "as a result of" requirement by pleading that he would have behaved differently if he had been aware of the information and the undisclosed information would have been important to reasonable consumers").

C. Plaintiff Properly Alleged UCL Unlawful, Fraudulent, or Unfair Conduct

Defendant's argument notwithstanding (Def. Br. at 17), Plaintiff adequately alleged the underlying unlawful, fraudulent, or unfair conduct required by the statute through violations of the SCA, California Civil Code Section 1750, and the California Constitution.

1. Plaintiff Properly Pleaded UCL Unlawful Conduct

As shown above, Defendant violated the SCA and California Constitution. Accordingly, the "unlawful" prong is met. *Quintero Family Trust v. OneWest Bank, F.S.B.*, No. 09-1561, 2010 WL 392312, at *12 (S.D. Cal. Jan. 27, 2010) ("An act is 'unlawful' under section 17200 if it violates an underlying state or federal statute or common law").

2. Plaintiff Properly Pleaded UCL Fraudulent Conduct

Plaintiff properly alleged fraudulent behavior as it is defined by the UCL. Under the "fraudulent" prong it is only necessary to show that "members of the public are likely to be deceived." *Sanchez v. Bear Stearns Residential Mortg. Corp.*, No. 09-2056, 2010 WL 1911154, at *7 (S.D. Cal. May 11, 2010). The California Supreme Court noted that "the 'fraud' contemplated by section 17200 … bears little resemblance to common law fraud or deception … [and] can be

shown even if no one was actually deceived, relied upon the fraudulent practice, or sustained any damage." *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal. App. 4th 861, 888 (1999) (internal quotations and citations omitted). Because this is not an action under common law fraud, Plaintiff's claims do not sound in fraud and are not required to be pled with the specificity required under Rule 9(b). Plaintiff is only required to show that members of the public are likely to be deceived.[19]

Plaintiff properly pleaded fraudulent conduct by alleging that members of the public were likely to be deceived by Defendant's practices, including publication of its privacy policy, which Defendant violated. ¶¶ 25, 29. Furthermore, Plaintiff also alleges that even if Defendant's privacy policy accurately described the disclosure of its users private information (which it did not), such a privacy policy is ineffective in providing consumers with useful and accurate information about how personal information will be collected and used. Instead, consumers are likely to believe, when seeing that a Website has a privacy policy, that the information collected is ***not*** shared with third parties. Plaintiff thus properly alleged that members of the public are likely to be deceived by Defendant's privacy policy with respect to private, personal information.

3. Plaintiff Properly Pleaded UCL Unfair Conduct

There are three tests that a court may apply to a consumer action relating to the "unfair" prong of the UCL. *See Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 256-57 (2010). The first test requires: (a) substantial consumer injury; (b) that the injury is not outweighed by countervailing benefits to consumers; and (c) that the injury is one that consumers could not reasonably have avoided. *Id.*; *see Camacho v. Auto. Club of S. Cal.*, 142 Cal. App. 4th 1394, 1403 (2006). The second test requires that the unfair conduct be "tethered to specific constitutional,

[19] Even if the Court were to apply the standards of Rule 9(b) to the Complaint, Plaintiff has pleaded the allegations with sufficient particularity to put the Defendant on notice of their claims. "Averments of fraud must be accompanied by 'the who, what, when, where, and how' of the misconduct charged." *Vess v. Ciba-Geigy Corp. U.S.A.*, 317 F.3d 1097, 1106 (9th Cir. 2003) (citation omitted). Plaintiff has clearly met this standard, including the when (March 24, 2011); the what (providing Plaintiff's personal information to third parties); the who (Quantcast and Scorecard Research); the where (Plaintiff's computer located at his home in San Francisco); and the how (including the User Identification in a HTTP Referrer header).

statutory, or regulatory provisions," and the third test asks whether the conduct was "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers," weighing the utility of the defendant's conduct against the harm to the victim. *Drum*, 182 Cal. App. 4th at 256-57. Contrary to Defendant's assertion, Plaintiff has alleged facts that satisfy any one of these tests that the Court may apply.

Plaintiff has satisfied the first test; Plaintiff sustained a substantial consumer injury, there was no countervailing benefit to consumers at all, and Plaintiff could not have avoided the injury. Indeed, California places a strong emphasis on the right to privacy at issue here. California Const. Article 1 Section 1. Courts have repeatedly recognized that invasion of privacy constitutes injury, and is actionable under the law. *See, e.g., Forsher v. Bugliosi*, 26 Cal. 3d 792 (1980). Defendant caused this injury when it gave Plaintiff's personally identifiable information to third parties, and there was no countervailing benefit to consumers. Plaintiff could not have avoided the injury because Defendant acted contrary to the position taken in its privacy policy, and there was no other way for Plaintiff to learn of Defendant's practices.

The second test is satisfied because Plaintiff alleged unfair conduct that is specifically tethered to a constitutional provision as well as multiple statutory provisions. Finally, Plaintiff pleaded facts sufficient to satisfy the third test, alleging the unscrupulous behavior of Defendant in acting contrary to its privacy policy, with no corresponding utility for the consumer and serious harm based on the violation of privacy. ¶¶ 11, 13-19, 24-33.

D. Plaintiff is a Consumer Who Purchased a Service From LinkedIn

1. Plaintiff is a "Consumer" under the CLRA

A violation of the CLRA may only be alleged by a "[c]onsumer," defined in the statute as an "individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes." Cal. Civ. Code § 1761(d). The statute does not require that the consumer actually purchased, leased, or otherwise paid for the good or service. Cal. Civ. Code 1770(a) ("The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction ***intended to result or which results*** in the sale or lease of goods or services to any consumer are unlawful") (emphasis added).

Here, Plaintiff is a "consumer" because he exchanged valuable consideration, in the form of personal information, for Defendant's service. Moreover, Defendant offered its service to Plaintiff, and other consumers, for a price of $24.95 per month. ¶ 3. Accordingly, the conduct at issue falls within the definition of the CLRA.

2. LinkedIn is a "Service" under the CLRA

The CLRA defines "[s]ervice" as "work, labor, and services for other than a commercial or business use, including services furnished in connection with the sale or repair of goods." Cal. Civ. Code 1761(b). Defendant provides a service under this definition, allowing access to a social network of professionals to users of the website in exchange for personal information, revenue from data aggregators, as well as selling premium services. Indeed, LinkedIn acknowledges that it provides a "service" in its own User Agreement, stating, in part: "For as long as LinkedIn continues to offer the Services, LinkedIn shall provide and seek to update, improve and expand the Services." *User Agreement*, LINKEDIN, http://www.linkedin.com/static?key=user_agreement (last visited Aug. 1, 2011). These services are not provided for commercial or business use, but for personal use by consumers looking to connect with other professionals and develop their professional career.

Furthermore, the cases that Defendant relies on to argue that LinkedIn is not a service are inapplicable. Def. Br. at 19. Unlike *Ferrington v. McAfee, Inc.*, No. 10-1455, 2010 WL 3910169 (N.D. Cal. Oct. 5, 2010), the instant case does not involve software. *Fairbanks v. Superior Court*, 46 Cal. 4th 56, 61 (Oct. 5, 2009), involved an insurance policy and the court held that the obligation to pay money under such a policy is neither work nor labor, factors not at issue in this case. *Id. Berry v. American Express Publishing, Inc.*, 147 Cal. App. 4th 224, 227 (2007), held that credit card transactions were not covered by the CLRA, primarily because of the legislative history of the CLRA, where the drafters considered adding the term "credit" into the definitions but ultimately rejected it. *Id.* at 230-32. This reasoning has no application here.

Moreover, Defendant's contention that LinkedIn is not a "service" under the CLRA is inconsistent with the CLRA's purpose. The CLRA is to be "liberally construed and applied to promote its underlying purposes, which are to protect consumers against unfair and deceptive

business practices and to provide efficient and economical procedures to secure such protection." Cal. Civ. Code §1760 (West 2009). With the development of personal information as a form of currency on the Internet for data aggregators and advertisers, as well as the rise of social networking Websites like the Defendant's, it is important to protect consumers from unfair and deceptive business practices in these new areas, and the CLRA was designed to do just that.

E. Plaintiff Alleged Breach of Contract Damages

Plaintiff alleged facts that show appreciable and actual damage as a result of the breach of contract. *See supra, sec.* V.A.

F. LinkedIn Converted Plaintiff's Property

Defendant tries to avoid liability by arguing that the personal browsing history and other personally identifiable information of the Plaintiff is not an intangible interest that is merged with or reflected in something tangible and that it cannot be exclusively possessed. Def. Br. at 23-24. Defendant's argument is in error.

Plaintiff had a precisely defined, legally protected privacy interest. "In order to determine whether an intangible property right existed … (1) there must be an interest capable of precise definition; (2) it must be capable of exclusive possession or control; and (3) the putative owner must have established a legitimate claim to exclusivity." *Ali v. Fasteners for Retail, Inc.*, 544 F. Supp. 2d 1064, 1072 (E.D. Cal. 2008). A legally recognized informational privacy interest is one which protects the dissemination or misuse of confidential information. *Hill,* 865 P.2d at 642. A LinkedIn member, like the Plaintiff, has an informational privacy interest in preventing third parties from collecting and disseminating private browser histories and other personally identifiable information. The privacy amendment to the California Constitution was enacted to guard against exactly such an intrusion. *Id.* This privacy interest is exclusively controlled by the person whose private, sensitive information is at issue.[20]

[20] Defendant notes that *Boon Rawd Trading International Co. v. Paleewong Trading Co.*, 688 F. Supp. 2d 940, 954 (N.D. Cal. 2010), puts forth the proposition that an intangible interest can be the subject of a conversion claim only where that interest is merged with, or reflected in, something tangible. Def. Br. at 23-24. However, that Court notes that "to the extent 'California retains some vestigial merger requirement, it is clearly minimal, and at most requires only some connection to a document or tangible object.'" *Boon,* 688 F. Supp. 2d at 954 (quoting *Kremen v.*

CONCLUSION

For the reasons stated above, Defendant's motion to dismiss must be denied.[21]

Dated August 1, 2011

Respectfully submitted,

/s/ Michael R. Reese
Michael R. Reese (State Bar No. 206773)
REESE RICHMAN LLP
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272
Email: mreese@reeserichman.com

Sanford P. Dumain
Peter E. Seidman (admitted *pro hac vice*)
Charles Slidders
Melissa Ryan Clark
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119-0165
Telephone: (212) 594-5300
Facsimile: (212) 868-1229
Email: pseidman@milberg.com

Cohen, 337 F.3d 1024, 1033 (9th Cir. 2003)). It further notes that there is a clear trend that intangible property can be a subject of conversion. *Id.* Defendant's reliance on this case is thus misplaced.

[21] If the court grants any part of Defendant's motion to dismiss, Plaintiff respectfully request leave to amend under Federal Rule of Civil Procedure 15.