SIMON J. FRANKEL (State Bar No. 171552)
E-Mail: sfrankel@cov.com
MALI B. FRIEDMAN (State Bar No. 247514)
E-Mail: mfriedman@cov.com
COVINGTON & BURLING LLP
One Front Street, 35th Floor
San Francisco, California 94111
Telephone: (415) 591-6000
Facsimile: (415) 591-6091

Attorneys for Defendant
LINKEDIN CORPORATION

UNITED STATES DISTRICT COURT

FOR THE 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.

Civil Case No.: 5:11-cv-01468 LHK

DEFENDANT LINKEDIN CORPORATION'S REPLY IN SUPPORT OF MOTION TO DISMISS

Date: September 15, 2011
Time: 1:30 pm
Courtroom: 4, 5th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

Plaintiff's Opposition is long on rhetoric but short on citations to the Complaint. By conflating concepts and confusing issues, plaintiff seeks to obscure the fact that the actual allegations regarding LinkedIn's actions are narrow and do not amount to a violation of any law.

The Complaint's basic allegation is that LinkedIn discloses LinkedIn user identification numbers ("User IDs") within URL referrers and as a URL parameter (a component of the URL). *See* Complaint ("Compl.") ¶¶ 14-18. LinkedIn User IDs are not users' names, but unique numbers assigned to each LinkedIn member by LinkedIn, and their transmission does not convey any personally identifiable information about plaintiff or any other user. *See id.* ¶¶ 14, 18. Referrer URLs or the "HTTP Referer' header" (the Complaint's term) (*id.* ¶ 16) are, as plaintiff acknowledges, a "standard piece of information." *See id.*[1]

Contrary to the Opposition's contention, the Complaint does *not* allege that LinkedIn transmits users' Internet browsing history to third parties. As the Complaint acknowledges, any browsing history compiled, retained, or utilized by third parties occurs entirely independent of LinkedIn. *See id.* ¶¶ 14-18. The only allegation as to LinkedIn is that because LinkedIn includes a LinkedIn User ID within a URL referrer header or as a URL parameter, *third parties* can associate this information with the anonymous browsing profiles they have collected. *See id.* ¶¶ 11, 14-18. The Complaint never explains how this could occur, let alone how any third party could link users' *names* (as distinct from their User IDs) with their browsing histories. Nor does the Complaint contain a single fact suggesting that any third party actually *did* link identity and browsing history for plaintiff or for any other LinkedIn user. Moreover, even if such a correlation were theoretically possible, the Complaint's basic factual premise is fatally flawed because, in fact, the User ID that is transmitted to third parties in the "'HTTP Referer' header" or as a "URL parameter" (*see id.* ¶ 16) is the User ID of the *viewed* user, not that of the

[1] Although the Complaint asserts that it is LinkedIn that transmits the referrer URLs, they are actually transmitted by users' web browsers as a standard feature of current Internet architecture.

user viewing the page—a fact the Opposition never addresses. *See* LinkedIn Motion to Dismiss ("Mot.") at 4 n.2.[2]

Once the focus is returned to the specific allegations actually in the Complaint, it is clear that plaintiff has not properly alleged any claim. Plaintiff does not allege any "injury-in fact" resulting from LinkedIn's conduct and thus lacks the requisite Article III standing to bring suit. The Stored Communications Act does not fit the allegations, because plaintiff has not alleged that LinkedIn divulged any communications contents of plaintiff stored by LinkedIn and because any such communications were divulged either to or by an "intended recipient" of those transmissions. And although the Opposition contends that plaintiff was deprived of "his" LinkedIn User ID or "his" browsing history, courts consistently have rejected the argument that an individual's personal information has an economic value recoverable to that person—so plaintiff has not alleged cognizable damages. All of plaintiff's claims must be dismissed.

II. ARGUMENT

A. The Complaint Must Be Dismissed For Lack Of Article III Standing.

Article III standing requires that a plaintiff allege adequate "injury in fact"—meaning both that the plaintiff has suffered an "invasion of a legally protected interest" which is (a) "concrete and particularized" (meaning, that it "must affect the plaintiff in a personal and individual way") and (b) not "conjectural or hypothetical," *and* that the injury complained of has to be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 & n.1 (1992) (quotations and citations omitted); *see* Mot. at 6.[3]

---

[2] This fact is not difficult to discern. When the same user views different profile pages on the LinkedIn site, the User ID within the URL changes. If the User ID were that of the *viewing* user, it necessarily would be the same.

[3] Plaintiff looks to out-of-Circuit authority—misleadingly described as from "the United States Supreme Court"—to try to minimize this threshold requirement, arguing that "[i]njury-in-fact is not Mount Everest" and requires only an "identifiable trifle." *See* Opp. at 4-5 (quoting *Danvers Motor Co. v. Ford Motor Co.*, 432 F.3d 286, 294 (3d Cir. 2005)). But the case he quotes involved a complaint the Third Circuit found was "replete with assertions of cognizable harm," including itemized "out-of-pocket expenses Plaintiffs made," as well as specific allegations of loss of control of a business due to the alleged conduct. *Danvers*, 432 F.3d at 292-93.

Although the Complaint contains speculative allegations of hypothetical harm that the disclosure of User IDs in referrer headers and as a URL parameter *might* pose, it does not allege a single fact even suggesting that the named plaintiff has suffered *any* actual injury or faces *any* risk of imminent, cognizable injury by virtue of LinkedIn's alleged conduct. *See* Mot. at 6. Plaintiff speculates that LinkedIn's alleged disclosures allow third parties that collect anonymous browsing histories to match such histories with LinkedIn users (*see* Opposition ("Opp.") at 3; Compl. ¶¶ 11, 13), but there are no facts to support these conjectures. Moreover, there is no specific allegation that *plaintiff's* browsing history *was* (or even will be) linked to his identity, or, if it was, that a third party made use of such information in any context. *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 960 (9th Cir. 2009) (dismissing class action where "[t]he risk of injury the plaintiffs allege is not concrete and particularized *as to themselves*") (emphasis in original); *see generally Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949-50 (2009).[4]

The Opposition relies on academic articles discussing speculative possibilities for usage of aggregated information (Opp. at 2), but courts have rejected this precise argument. For example, *La Court, et al. v. Specific Media, Inc.* found no Article III standing where plaintiffs did not allege a "particularized example" of how the purported collection and retention of plaintiff's browsing history caused injury or harm or how they were "deprived" of the economic value of their personal information simply because unspecified personal information was allegedly collected by a third party. No. SACV 10-1256-GW (JCGx), 2011 WL 1661532, at *3-6 (C.D. Cal. Apr. 28, 2011) *See also* Mot. at 7 (citing cases).[5]

---

[4] The Opposition asserts (without citation) that "expert studies have shown first and last names and other personal information . . . can be easily and quickly determined from User Identification numbers." Opp. at 3. But even if theoretically true (which LinkedIn disputes), the Complaint does not include this allegation, let alone allege that this correlation actually occurred with respect to plaintiff or any other LinkedIn user, or that such correlation caused plaintiff or anyone else any actual and particularized harm.

[5] Plaintiff seeks to distinguish *Specific Media*, claiming the plaintiffs there referred to facts not contained in their complaint "at all." *See* Opp. at 6 n.3 (quoting *Specific Media*, 2011 WL 1661532, at *4). Plaintiff, however, cannot cite any statements in *his* complaint containing the types of non-speculative facts that were missing in *Specific Media*. Moreover, although the *Specific Media* plaintiffs were permitted leave to amend, amendment would be futile here because plaintiff's fundamental factual inaccuracy—the fact that it is the *viewed* user whose User ID appears as a URL parameter and within URL referrers (*see* Mot. at 4 n.2)—means that (continued…)

The fact that plaintiff here does not allege more than speculation of harm due to the possible conduct of third parties distinguishes this case from the two on which plaintiff relies. *See* Opp. at 5-6. In *Krottner v. Starbucks Corp.*, a company laptop containing sensitive, unencrypted personal information about employees was *actually* stolen, putting names, addresses, and social security numbers of the plaintiffs in the hands of a third party. 628 F.3d 1139, 1140 (9th Cir. 2010). This created an actual and imminent threat of identity theft, as evidenced by the fact that a fraudulent bank account apparently was opened using the social security number for one of the plaintiffs. *Id.* at 1141. Similarly, *Pisciotta v. Old National Bancorp* involved the unauthorized hack of a bank application website, giving the hacker actual access to plaintiffs' names, addresses, social security numbers, driver's license numbers, dates of birth, mother's maiden names, and credit card or other financial account numbers. 499 F.3d 629, 631-32 (7th Cir. 2007) ("intrusion was sophisticated, intentional and malicious").

In short, both *Krottner* and *Pisciotta* involved allegations of *actual* dissemination of sensitive financial information, not merely the possibility that, due to the defendant's alleged conduct, a third party might be able to de-anonymize a browsing history it had already collected. As the Ninth Circuit noted in *Krottner*, "[w]ere Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible." *Krottner*, 628 F.3d at 1143. That is the circumstance here.

B. The Stored Communication Act Claim Fails On Multiple Grounds.

The SCA was enacted because "the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment [did] not address." *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir.2008), *reversed on other grounds by City of Ontario v. Quon*, 130 S. Ct. 2619 (2010). The SCA generally sought to address this gap "by offering network account holders a range of statutory privacy rights against access to stored

---

it would be impossible for plaintiff to allege in good faith any particularized example of harm that can be fairly traceable to LinkedIn.

account information held by network service providers," creating "a set of Fourth Amendment-like privacy protections by statute, regulating . . . service providers in possession of users' private information." 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, 1212 (2004).

The resulting statute is complex, creating an intricate matrix of protections and non-protections for stored information, depending on distinctions such as the type of communication (content or non-content), to whom disclosure is made (governmental or non-governmental entity), and whether disclosure is to or by an intended recipient. *See id.* at 1223, 1231-1233. And while the SCA protects the privacy of some categories of stored communications, the Wiretap Act and Pen Register Statute protect the privacy of Internet communications in transit. *Id.* The Opposition seeks to trivialize these technical distinctions, but they are critical to assessing plaintiff's failure to plead a proper SCA claim. *See id.* at 1214, 1224.

1. The SCA Claim Fails Because The Complaint Does Not Allege That LinkedIn Disclosed Communications Of Plaintiff That Were Held In Storage By LinkedIn.

As set out in Linkedin's Motion, the SCA only applies where *plaintiff's communications* are held *in storage* by two types of network providers—an Electronic Communication Service ("ECS") or a Remote Computing Service ("RCS"). 18 U.S.C. §§ 2701(a); 2702(a); *see* Mot. at 8-9.[6] Here, the Complaint does not contend that any allegedly disclosed communications of plaintiff were stored by LinkedIn, and so the SCA claim must fail.[7]

---

[6] The Opposition (at 11) backs away from the Complaints' extensive allegations that it was LinkedIn's *transmission* of information that was improper—which would be the realm of the Wiretap Act, not the SCA. *See* Mot. at 9-10. Plaintiff's new focus on divulgence, rather than transmission, in no way changes the threshold requirement that data *belonging to plaintiff* be *stored* by LinkedIn to fall within the purview of the SCA, as discussed in the text.

[7] Although the Complaint alleges both that LinkedIn improperly accessed and improperly disclosed plaintiff's stored data (*see* Compl. ¶¶ 46-52), the Opposition concedes that any *access* of plaintiff's stored data was exempted under the SCA's service provider exception. *See* Opp. at 18; 18 U.S.C. § 2701(c); Mot. at 10-11. Plaintiff seeks to withdraw this concession in part in a footnote, contending that the service provider exception applies only to an ECS, not an RCS. *See* Opp. at 18 n.8. Plaintiff apparently misunderstands why the service provider exception is limited to an ECS. The SCA's *restriction* on access only applies to an ECS in the first place. *See* 18 U.S.C. § 2701. Hence, there is no need for a service provider *exception* for an RCS.

As the Complaint alleges, LinkedIn User IDs are assigned and controlled by LinkedIn (*see* Compl. ¶ 14), and so are not communications of plaintiff. Accordingly, there cannot be any improper access to or improper disclosure of a LinkedIn User ID under the SCA. *See Kerr*, 72 GEO WASH L. REV. at 1214 & n.47 (the SCA pertains only where a "*user's communications* [are] in the possession of the provider") (emphasis added); Mot. at 10. The other type of information plaintiff alleges that LinkedIn disclosed is referrer URLs, reflecting the page on LinkedIn viewed by plaintiff. *See* Compl. ¶¶ 14-18. Although plaintiff asserts in his Opposition (in the alternative) that "[t]he User Identification and last-viewed page were stored on LinkedIn's servers and/or carried on its network" (Opp. at 11), in fact the Complaint never alleges that the "last-viewed page" (presumably the referrer URL) is held in electronic storage by LinkedIn.

The only other category of data even referenced in the Complaint is plaintiff's "browsing history," which the Complaint specifically alleges is held in third party tracking cookies or otherwise compiled and retained by third parties. *See* Compl. ¶¶ 18, 24. The Complaint naturally does not allege that LinkedIn stores on its servers or networks these third party tracking cookies or the browsing history of plaintiff compiled by third parties.

Accordingly, because plaintiff does not allege that any purportedly disclosed communications *of plaintiff* were held in storage by LinkedIn, the SCA does not apply.[8]

---

[8] Plaintiff also contends that because LinkedIn can be considered an RCS, it is irrelevant whether plaintiff's communications were stored—because the restriction for an RCS applies to communications "carried or maintained" by the RCS. *See* Opp. at 12-13 (citing 18 U.S.C. § 2702(a)(2)). As an initial matter, the Complaint's characterization of LinkedIn makes it clear that LinkedIn acts as an ECS with respect to the activities at issue in the Complaint, as an ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Plaintiff does not explain why the definition for an RCS would be more applicable here. But even if plaintiff is correct that LinkedIn acts as an RCS for some relevant purposes, the SCA's restrictions on divulgence of information by an RCS demonstrate as a practical matter that a user's data must be held in storage for the SCA to be triggered in the first instance. It is not clear how a communication can be "carried or maintained" by an RCS without being stored. In addition, the statute defines an RCS as "the provision to the public of computer storage or processing services *by means of an electronic communications system*" and then defines "electronic communications system," in relevant part, as "any computer facilities or related electronic equipment for the electronic *storage* of such communications." *Id.* §§ 2711(2); 2510(14) (emphasis added). Finally, the SCA's disclosure restrictions for an RCS only apply where communications stored by the RCS are carried or maintained "on behalf of, and received . . . from . . . a subscriber or customer." *Id.* § 2702(a)(2)(A). As explained in the text, because the communications alleged to have been (continued…)

2. LinkedIn's Conduct Was Authorized Under The SCA Because The Disclosures Alleged Were Made To Or By The Intended Recipient Of The Communications.

Even if the User IDs and referrer URLs were communications of plaintiff held in storage by LinkedIn, the alleged disclosures still would be permitted by the SCA. A provider can divulge the contents of a communication to "an addressee or intended recipient of such communication." 18 U.S.C. § 2702(b)(1); *see* Mot. at 13; *Quon*, 529 F.3d at 900 ("both an ECS and RCS can release private information to, or with the lawful consent of, 'an addressee or intended recipient of such communication'"). The Opposition contends that because *plaintiff* did not intend to send his User ID or the referrer URLs to third parties, the "addressee or intended recipient" exception should not apply. *See* Opp. at 17. This argument both misses the point and underscores why application of the SCA here does not make sense.

Plaintiff's allegations do not concern, for example, a message that plaintiff sent to another LinkedIn *user*, which LinkedIn allegedly then disclosed to a third party. Rather, the Complaint alleges that the "communications" at issue are ones sent *by LinkedIn* to third parties. Specifically, the Complaint alleges that "logging in and looking at a profile page caused *LinkedIn to transmit* the user ID" to a third party. Compl. ¶ 18 (emphasis added). *See also id.* ¶ 16 ("*LinkedIn discloses* this package of information [referrer URL, including User ID]") (emphasis added). Plaintiff therefore alleges that *LinkedIn*, not plaintiff, is the original transmitter of the communications at issue—the User ID and the referrer URL—and that such communications were sent directly from LinkedIn to third parties.[9] Accordingly, the third parties were the intended recipients of the communications at issue, and the SCA permits the disclosure of "the contents of a communication . . . to an addressee or intended recipient of such communication" (18 U.S.C. § 2702(b)(1))—just as another judge of this Court held in a case with parallel allegations of transmission of User IDs and referrer URLs. *See In re Facebook*

---

disclosed are not received from plaintiff, the SCA's prohibitions are not triggered—regardless of whether LinkedIn is an ECS or an RCS.

[9] In fact, as explained above, the referrer URL actually originates with plaintiff's web browser and is communicated directly to the third parties at issue such that *LinkedIn* does not even make a disclosure in the first instance.

Privacy Litig., No. C 10-02389 JW, 2011 WL 2039995, at *6 (N.D. Cal. May 12, 2011); *see also* 18 U.S.C. § 2702(b)(3) (disclosure permissible with consent of "originator").

To the extent plaintiff asserts that the referrer URL reflects a communication *by plaintiff*, it must be a communication *with someone*—here presumably a communication to LinkedIn as to what page plaintiff had viewed (or wished to view). But if the communication allegedly disclosed was one *to LinkedIn*, then LinkedIn, as the "intended recipient" of the communication, could disclose it to third parties under the SCA. *See* 18 U.S.C. § 2702(b)(3); *In re Facebook Privacy Litig.*, 2011 WL 2039995 at *6 n.8. This is true even if plaintiff were to claim that LinkedIn contractually agreed not to disclose such communications to third parties. *See In re Am. Airlines, Inc. Privacy Litig.*, 370 F. Supp. 2d 552, 560-61 (N.D. Tex. 2005).

3. The SCA Claim Fails Because The Complaint Only Alleges Disclosure Of Non-Content Information.

The SCA claim also fails because the statute permits the disclosure of *non-content* information to non-government entities. 18 U.S.C. § 2702(c)(6); *see* Mot. at 11-13. Here, the recipients of the alleged disclosures—"third parties, including advertisers, Internet marketing companies, data brokers, and web tracking companies" (Compl. at 1)—are non-governmental entities. The only issue, then, is whether the data allegedly disclosed by LinkedIn constitutes the "contents" of a communication of plaintiff. As set out in LinkedIn's Motion, "contents" includes "information concerning the substance, purport, or meaning of that communication" (18 US.C. § 2510(8)), but not the fact of a communication, the identity of the parties to it or "transactional records about it." S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555, 3576; Mot. at 11.[10]

[10] The essential distinction between content and non-content transactional records (often referred to as "envelope" information) remains constant across different technologies. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 (2003). With respect to postal mail, the non-content, envelope information is the information derived from the outside of the envelope—mailing and return addresses, stamp and postmark, size and weight, etc. *See id.* (citing 39 C.F.R. § 233.3(c)(1)). For telephone calls, the non-content, envelope information includes the number the caller dials, the number from which the caller dials, and the time and duration of the call. *See id.* For emails, the non-content information includes the "to" and "from" email addresses, the date and time sent, how the email was processed by the network from its origin to its destination. *Id.*

The only two types of information that the Complaint alleges to have been disclosed *by LinkedIn* are plaintiff's LinkedIn User ID (as part of a URL parameter) and URL referrer headers. *See* Compl. ¶¶ 14, 18; *see also* Opp. at 1-2. Neither can properly be considered communications "contents" for purposes of the SCA. *See* Mot. at 11-13.

Plaintiff argues that a LinkedIn User ID "plainly qualifies as 'contents,'" on the theory that third parties can later use the User ID to correlate a user's identity with his or her browser history (an assertion that ignores plaintiff's critical mistake as to whose User ID is contained in the URL, noted above). Opp. at 14 (discussing House Report). But a LinkedIn User ID is a generic number assigned by LinkedIn and unrelated to any communications by plaintiff. As such, it cannot be considered the contents of plaintiff's communications, as it is precisely the type of transactional and routing "envelope" information that the SCA excludes from the definition of contents. *See* 18 U.S.C. § 2510(8); Mot. at 11. Courts have consistently held that a person's *name*, as party to a communication, cannot constitute the contents of that communication for purposes of the SCA.[11] If a person's name, which reveals his identity, is not content, then certainly a User ID assigned by LinkedIn cannot be either.

The alleged disclosure of a LinkedIn URL address within a referrer header also does not constitute communications contents, as this is precisely the type of transactional, routing information that has been deemed non-content information across all technological mediums. As the Complaint acknowledges, referrer URLs are "a standard piece of information" routinely

---

[11] *See Sams v. Yahoo!, Inc.*, No. CV-10-5897-JF (HRL), 2011 WL 1884633, at *6-7 (N.D. Cal. May 18, 2011) (all records regarding "the Yahoo! ID 'lynnsams' or 'lynnsams@yahoo.com' . . . includ[ing] name and address, date account created, account status, Yahoo! E-mail [sic] address, alternative e-mail address, registration from IP, date IP registered and login IP addresses associated with session time and dates" were "user identification information" not "content-based" data); *Jessup-Morgan v. Am. Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (disclosure of basic identity information revealing account holder's name was not the "'content' of an electronic communication" under 18 U.S.C. § 2702); *U.S. v. Kennedy*, 81 F. Supp. 2d 1103, 1107-09 (D. Kan. 2000); *Freedman v. Am. Online, Inc.*, 412 F. Supp. 2d 174, 181 (D. Conn. 2005); *see generally U.S. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

transmitted in connection with web page requests and simply identify the URL being viewed—much like a postal address or telephone number. Complaint ¶ 16.[12] Plaintiff alleges that referrer URLs "allow third parties to see . . . which other LinkedIn profile pages each of those users is looking at and interacting with" (Compl. ¶ 16), but a URL is simply an address where a particular webpage can be found. This does not reveal anything more than the email to/from addresses, IP addresses, or telephone numbers the Ninth Circuit deemed to be non-content information in *Forrester*. *See* 512 F.3d at 503 (telephone numbers are non-content information, even though "when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information").[13]

The Opposition also carelessly asserts without citation that "LinkedIn paired the user's identity with the user's ongoing browsing history." Opp. at 17. As explained above, however, the Complaint actually alleges only that LinkedIn divulged two specific pieces of data, neither of which constitutes "contents." While plaintiff seeks to hold LinkedIn responsible for third parties' aggregation of anonymous browsing histories, no case has suggested, let alone held, that

---

[12] The referrer URLs are actually transmitted by a user's web browser (not the site visited) and are a basic feature of the Internet architecture. Indeed, plaintiff's reference to referrer URLs as a "standard piece of information" hints at the problematic implications of the Complaint: Plaintiffs' contention that such referrer URLs—transmitted by web browsers whenever a browser user views a particular webpage—constitute communications content of users under the SCA would mean that web browsers would be violating the SCA billions of times a day, calling into question the basic functionality of the Internet.

[13] Plaintiff rely on dicta in *Forrester*, a Fourth Amendment decision suggesting that while IP addresses of website would not be content information, the URLs "of the pages visited *might be more constitutionally problematic*." 512 F.3d at 510 & n.6 (emphasis added). But the Ninth Circuit's suggestion that some URLs can constitute content does not mean that *all* URLs do so, let alone that all referrer URL transmissions would be content. As alleged by plaintiff here, the referrer URL contained the URL address of the page *on LinkedIn* that plaintiff viewed. *See* Compl. ¶¶ 15-16; Opp. at 14. The fact that plaintiff viewed a person's LinkedIn page is no different from the fact that one person communicated with another specific person—precisely the "envelope" information that does not constitute contents under the SCA.

Sometimes a referrer URL can contain more, such as the specific search terms that a user used to navigate to the page being viewed. *See, e.g.*, *In re Application of the U.S. for an Order*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005) (suggesting that a search phrase from the Google search engine appearing in a URL could reveal content) (cited in *Forrester*, 512 U.S. at 510 n.6). But here, plaintiff alleges only that, in addition to the URL, the referrer URL contains his User ID—which, as explained in the text, cannot constitute content. *See* Compl. ¶ 16.

a service provider could be liable under the SCA for providing non-content information about a user to a third party that already has *other* information about that user. Indeed, plaintiff's contention that LinkedIn should somehow be held responsible for third parties' collection of web browsing histories contravenes the rule that secondary liability cannot be imposed under the SCA. *See Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1004-09 (9th Cir. 2006).[14]

C. The State Law Claims All Fail As A Matter Of Law.

1. The Section 17200 and 17500 Claims Fail.

The claims under the UCL and FAL both require that plaintiff "lost money or property as a result of" the alleged conduct. *See* Mot. at 14-15. Without citation to the Complaint or cases, the Opposition insists that plaintiff "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." *See* Opp. at 18-19. The Complaint does not (and could not) allege that plaintiff ever paid any money to LinkedIn. *See* Mot. at 15 & n.6; *see also id.* at 3 n.1. Instead, relying only on various articles, plaintiff argues that *aggregated* data about individuals has value. *See* Opp. at 19. But plaintiff does not mention the many decisions holding that "personal information does not constitute property" for purposes of the UCL or FAL. *In re Facebook Priv. Litig.*, 2011 WL 2039995, at *6-7; *see In re Zynga Privacy Litig.*, C-10-04680, slip op. at 4 (N.D. Cal. June 15, 2011) (same); *In re Google Inc. Street View Elec. Commc'ns Litig.*, No. C 10-MD-02184 JW, 2011 WL 2571632, at *17 (N.D. Cal. June 29, 2011); *Fogelstrom v. Lamps Plus, Inc.*, No. B.221376, 2011 WL 1601990, at *4 (Cal. Ct. App. Apr. 29, 2011) (no economic injury through disclosure of address); Mot. at 15-16 (collecting additional cases). Plaintiff cites only *Doe 1 v. AOL, LLC*, 719 F. Supp. 2d 1102, 1113-14 (N.D. Cal. 2010) (*see* Opp. at 19-20), but ignores that the case was brought by plaintiffs who "paid fees" to the defendant website. 719 F. Supp. 2d at 1111. As the *In re Facebook Privacy Litigation* court

[14] Ironically, plaintiff seeks to distinguish one case by contending that there "the third party . . . already had possession of the contents of the communication, and sought only to place a name with an anonymous posting." Opp. at 16-17 (discussing *Jessup-Morgan*, 20 F. Supp. 2d at 1108). That is exactly what plaintiff has alleged here.

noted, "*AOL* does not stand for the broad proposition that personal information of any kind 'equates to money or property.'" *See* 2011 WL 2039995, at *6-7.

In addition, for both the UCL and FAL, plaintiff must—but does not—allege that he "actually relied on false or misleading advertisements" or statements. *Laster v. T-Mobile USA Inc.*, 408 F. Supp. 2d 1181, 1194 (S.D. Cal. 2005); Mot. at 16. Relying only on *Shin v. BMW of N. Am.*, No. CV 09-00398 AHM (AJWx), 2009 WL 2163509 (C.D. Cal. July 16, 2009), plaintiff contends that it is sufficient that he "believed[] that Defendant would not share his personally identifiable information." Opp. at 20 (citing Compl. ¶ 64). But what is still missing here is any allegation that plaintiff's purported belief was based on any statement or representation by LinkedIn—or that plaintiff even read LinkedIn's privacy policy.

Plaintiff also has not adequately alleged the unlawful, unfair, or fraudulent conduct required by the UCL. First, because the claims under the SCA, the CLRA, and the California Constitution must be dismissed as a matter of law, Plaintiff cannot state a claim for unlawful conduct. Second, to state a UCL fraud claim, plaintiff must meet the requirement of Rule 9(b). *See* Mot. at 17 (citing cases). Plaintiff ignores this Ninth Circuit rule and, citing no cases, simply asserts that "members of the public are likely to be deceived." Opp. at 20-21 (citation omitted). Because the Complaint offers no particulars that could satisfy Rule 9(b)—not even that plaintiff read LinkedIn's privacy policy—the fraud claim must be dismissed.[15]

Finally, plaintiff contends he has alleged "unfair" conduct under one of several tests courts have articulated. *See* Opp at 21-22. But the Complaint does not in fact include any allegations that plaintiff now says are required—namely that plaintiff "sustained a *substantial consumer injury*, there was *no* countervailing benefit to consumers at all, and [p]laintiff could not have avoided the injury." Opp. 21-22 (emphasis added). Nor has plaintiff tethered the alleged valuation to any constitutional or statutory policy, given that the alleged conduct does not violate the constitutional right plaintiff invokes. *See* Mot. at 20. And, the unfair conduct

[15] The Complaint does not even meet the watered-down standard plaintiff proposes, as it does not allege that members of the public were likely to be deceived by LinkedIn's practices. *See* Opp. at 21 (citing Compl. ¶¶ 25, 29, which merely quote portions of LinkedIn's privacy policy).

claim also is subject to Rule 9(b), a standard plaintiff cannot plausibly claim to meet. *See* Mot. at 17.

2. Plaintiff Cannot State A Claim Under The CLRA.

The CLRA claim fails for several independent reasons. First, plaintiff does not allege he is a "consumer" as required by the statute—one "who seeks or acquires, *by purchase or lease*, any goods or services." Cal. Civ. Code § 1761(d) (emphasis added); *see* Mot. at 18. The Opposition contends plaintiff is a "consumer" because LinkedIn "offered its service to Plaintiff, and other consumers, for a price of $24.95 per month." Opp. at 23 (citing Compl. ¶ 3). But the Complaint never mentions any price for LinkedIn (*see* Compl. ¶ 3), and, more significantly, never alleges that *plaintiff* paid any fees to LinkedIn—the requirement under the CLRA. *See* Mot. at 18. Plaintiff's assertion that he is a "consumer" because "he exchanged valuable consideration, in the form of personal information, for Defendant's service" (Opp. at 23) is not made in the Complaint and is contrary to the cases cited above holding that an Internet user's personal information is not property.

Second, the LinkedIn website is not a "good" or "service" under the CLRA. *See* Mot. at 18-19. Plaintiff's basic response is that LinkedIn's User Agreement—not part of the Complaint—refers to LinkedIn's website as a "service." Opp. at 23. But no case suggests this is determinative of whether LinkedIn is a "service" under the CLRA. The website is necessarily comprised of software, and this Court has held that software is not a "good" or "service" under the CLRA. *See Ferrington v. McAfee, Inc.*, No. 10-1455-LHK, 2010 WL 3910169, at *9 (N.D. Cal. Oct. 5, 2010). Third, the prongs of the CLRA that the Complaint seeks to invoke all sound in fraud, and so must be pled with the particularity required by Rule 9(b). *See* Mot. at 19. Plaintiff offers no response to this rule, requiring dismissal of the CLRA claim.

3. The California Privacy Claims Are Deficient.

The Complaint does not plausibly approach the standard required to state an invasion of privacy claim under the California Constitution or common law for the simple reason that the conduct alleged was not an "egregious breach of social norms." *Fogelstrom*, 2011 WL 16019909, at *3; *see Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008); Mot.

20-21. Citing no other cases, Plaintiff's only response is to contend that cases such as *Ruiz* and *Folgelstrom* are inapplicable because "[t]hose cases involved disclosure of a single piece of unlinked information (social security numbers or ZIP codes)." Opp. at 7. But that is just what plaintiff alleges here, as the Complaint offers no facts suggesting that any third party *has linked* his User ID to a previously anonymous browsing history or any other information.

4. Plaintiff Has Not Alleged Damages Sufficient To Support Contract-Based Claims.

The claims for breach of contract and breach of the implied covenant both require—but lack—cognizable damages. *See* Mot. at 21-23. Plaintiff's one sentence response is to incorporate the argument that plaintiff lost money or property sufficient to state a claim under the UCL. *See* Opp. at 24. As discussed above, courts consistently have rejected this argument. *See Ruiz v Gap, Inc.*, 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009) (plaintiff "cannot show he was actually damaged by pointing to his fear of future identity theft"); *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 326-27 (E.D.N.Y. 2005); *Dyer v. Nw. Airlines Corp.*, 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004); Mot. at 7, 14-15, 21-22.

5. Plaintiff's Conversion Claim Must Be Dismissed.

The conversion claim fails because the Complaint does not allege plaintiff's exclusive possession of tangible *personal property* (or intangible property merged with or reflected in something tangible) or cognizable damages. *See* Mot. at 23-24. Plaintiff first responds by assuming his premise, contending that he had an exclusive right to his LinkedIn User ID (ignoring that he did not create it) and his Internet browsing history (ignoring that *LinkedIn* is not alleged to have transmitted or even used that history). *See* Opp. at 24. But as explained above, courts repeatedly have held that such information cannot be considered *property* of a user. *See also* Mot. at 23-24. Nor can such information qualify as *tangible* property, or intangible property that has "some connection to a document or tangible object," as even plaintiff acknowledges is required under California law. Opp. at 24 n.20; *see* Mot. at 23. And, as the Opposition does not dispute, there is no allegation of cognizable damages caused by the purported conversion. *See* Mot. at 24.

6. Plaintiff's Unjust Enrichment Claim Fails As A Matter of Law.

As this and other courts in this District repeatedly have held, there is generally no independent cause of action for unjust enrichment in California. *Ferrington*, 2010 WL 3910169, at *17; *see* Mot. at 24-25. Plaintiff argues that litigants may seek restitution through an unjust enrichment claim. *See* Opp. at 8 (citing *SOAProjects, Inc. v. SCM Microsystems, Inc.*, No. 10-CV-01773-LHK, 2010 WL 5069832 (N.D. Cal. Dec. 7, 2010)). But such relief is available only where it is alleged the defendant received a benefit and unjustly retained that benefit at plaintiff's expense. *SOAProjects, Inc.*, at *10 (finding no restitution warranted and dismissing claim with prejudice). Here, no such allegation is or could be made. *See e.g., In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) ("we are unaware of any court that has held the value of [] collected [personal] information constitutes . . . unjust enrichment to collectors"); *see also* Mot. at 7.

In addition, because unjust enrichment is in the nature of a quasi-contract remedy, a plaintiff may not allege unjust enrichment while also alleging breach of an express contract covering the same subject matter. *See* Mot. at 24-25 (citing cases). Plaintiff argues that restitution may still be available where a contract was procured by fraud or is unenforceable for some reason. *See* Opp. at 8 (citing *SOAProjects*, 2010 WL 5069832, at *9). But plaintiff does not contend that any agreement with LinkedIn was procured by fraud or is unenforceable; to the contrary, he seeks to enforce the agreement alleged. *See* Compl. ¶¶ 90-91; Mot. at 24-25.

III. CONCLUSION

The Complaint should be dismissed with prejudice.

DATED: August 15, 2011

COVINGTON & BURLING LLP

By: /s/
Simon J. Frankel
Attorneys for Defendant
LINKEDIN CORPORATION