1 | **REESE RICHMAN LLP**
Michael R. Reese (Cal. Bar No. 206773)
2 | Kim E. Richman
Belinda L. Williams
3 | 875 Avenue of the Americas, 18th Floor
New York, NY 10001
4 | Telephone: (212) 643-0500
Facsimile: (212) 253-4272
5 | Email: mreese@reeserichman.com
        krichman@reeserichman.com
6 | bwilliams@reeserichman.com

7 | - and -

8 | **MILBERG LLP**
Sanford P. Dumain
9 | Peter E. Seidman (*pro hac vice*)
Melissa Ryan Clark (*pro hac vice*)
10 | Charles Slidders
One Pennsylvania Plaza, 49th Floor
11 | New York, NY 10119
Telephone: (212) 594-5300
12 | Facsimile: (212) 868-1229
Email: sdumain@milberg.com
13 | pseidman@milberg.com
        mclark@milberg.com
14 | cslidders@milberg.com

15 | *Attorneys for Plaintiffs*

16 | **UNITED STATES DISTRICT COURT**
NORTHERN DISTRICT OF CALIFORNIA
17 | (SAN JOSE DIVISION)

18 |

19 | KEVIN LOW, individually and on behalf of) CASE NO. CV 11-01468 (LHK)
all others similarly situated,)
) AMENDED COMPLAINT
20 | Plaintiff,)
) **CLASS ACTION**
21 | v.)
) JURY TRIAL DEMANDED
22 | LINKEDIN CORPORATION, a California)
Corporation,)
23 |)
Defendant.)
24 |)

25 |

26 |

27 |

28 |

AMENDED CLASS ACTION COMPLAINT | - |

Plaintiffs Kevin Low and Alan Masand bring this action individually and on behalf of all others similarly situated (the "Class," as defined below), by their undersigned counsel, against defendant LinkedIn Corporation ("LinkedIn," the "Company," or "Defendant").

This case arises from Defendant's intentional and knowing transmission of Plaintiffs' and the other Class members' personally identifiable information, browsing history among LinkedIn profiles ("LinkedIn Browsing History"), and other personal information to advertisers, Internet marketing companies, data brokers, web tracking companies, and other third parties (collectively, "Third Parties"), without the consent or knowledge of LinkedIn users, in violation of federal and state laws, and in violation of the Company's published privacy policy. Plaintiffs and the Class seek damages and equitable relief.

Plaintiffs allege the following upon personal knowledge as to their own acts and upon information and belief based on the investigation conducted by Plaintiffs' counsel, including consultation with a technology expert, as to all other matters.

PARTIES
Plaintiffs

1.   Plaintiff **Kevin Low** resides in San Francisco, California. Mr. Low was a registered user of LinkedIn during the time relevant to this action.

2.   Plaintiff **Alan Masand** resides in Astoria, New York. Mr. Masand was a registered user of LinkedIn during the time relevant to this action. In November 2011, also during the relevant time period, Mr. Masand became a paid user of LinkedIn when he purchased a "Job Seeker Premium" subscription.

3.   Plaintiffs' LinkedIn Browsing Histories and their LinkedIn user identification numbers ("LinkedIn IDs")—sent in connection with third party cookie identification numbers ("cookie IDs")—were transmitted to Third Parties by LinkedIn. For example:

- On or about March 24, 2011, via Mr. Low's computer, located at his home in San Francisco, California, LinkedIn provided Mr. Low's personal identity to Scorecard Research, linking it to Scorecard's secretly embedded tracking device that surreptitiously recorded Mr. Low's internet browsing history.

- On or about March 24, 2011, via Mr. Low's computer located at his home

in San Francisco, California, LinkedIn provided Mr Low's personal identity to Quantcast, linking to it to Quantcast's secretly embedded tracking device that surreptitiously recorded Mr. Low's internet browsing history.

- On or about March 24, 2011, via Mr. Low's computer located at home in San Francisco, California, LinkedIn provided Mr. Low's identity to Nielsen Netratings ("imrworldwide"), linking it to Nielsen's secretly embedded tracking device that surreptitiously recorded Mr. Low's internet browsing history.

See Exhibit A for transmission detail; *see* ¶36 for a test transmission involving Mr. Masand's account.

4.   In addition to these examples, LinkedIn's wrongful disclosure of information was ongoing; on information and belief, this wrongful conduct occurred every time Plaintiffs visited a LinkedIn profile page.

5.   LinkedIn disclosed Plaintiffs' personally identifiable information without their consent. In particular, LinkedIn provided Third Parties their LinkedIn IDs (which corresponds to their profiles) and their LinkedIn Browsing History. This information gave the Third Parties the ability to correlate Plaintiffs' actual identities with their broader Internet browsing histories. Plaintiffs' browsing histories include visits to websites that they consider private, including political, religious, and health-related websites. Had they known of these practices and been given the choice, Plaintiffs would not have disclosed this information to the Third Parties. Plaintiffs were embarrassed and humiliated by the disclosure of their personally identifiable browsing history. Moreover, Plaintiffs' browsing histories and personal identities are valuable personal property with a market value. The market value of Plaintiffs' browsing histories and personally identifiable information increase when the two types of personal information are correlated with one another. As a result of Defendant's unlawful conduct, Plaintiffs relinquished this valuable personal property without the compensation to which they were each due.

6.   The Plaintiff Class consists of all persons who reside in the United States and who signed up for and used LinkedIn's services any time after March 25, 2007.[1] The Class includes

---

[1] Excluded from the Class are Defendant; any parent, subsidiary, or affiliate of Defendant; or any employees, officers, or directors of Defendant; legal representatives, successors, or assigns of Defendant; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

members who had a free subscription as well as members who paid a fee for LinkedIn's "premium" services.

7. Plaintiffs and the Class were injured by Defendant's unauthorized and public disclosure of their personally identifiable information.

Defendant

8. Defendant **LinkedIn** is a consumer-oriented web-based social networking site that presents itself as an online community offering professionals ways to network *via* e-mail and instant messaging. It was founded in 2002 and, in February 2008, announced "LinkedIn mobile" for web-enabled wireless phones that use wireless application protocol. LinkedIn mobile allows users to access LinkedIn from any mobile device. LinkedIn also provides services to advertisers and marketers. It sells premium marketing services to individuals and organizations seeking to utilize the vast database of LinkedIn user data, thereby monetizing its users' personal information.

9. LinkedIn is a California corporation with its principal place of business in the San Jose Division of the Northern District of California. Specifically, LinkedIn is located at 2029 Stierlin Court, Mountain View, California, which is located within Santa Clara County, California. It conducts business throughout California and the United States. LinkedIn reported more than 90 million registered users as of January 1, 2011, spanning more than 200 countries and territories worldwide. The Company states that "on average, a new member joins every second of every day, or approximately one million every 12 days." (*See http://press.linkedin.com/about/*). In January 2011, LinkedIn filed for an initial public offering and is reportedly valued at $2.51 billion.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (a) and 1332 (d), because the amount in controversy exceeds $5,000,000 exclusive of interests and costs and more than two-thirds of the members of the Class are citizens of states different from that of Defendant. This Court also has federal question

jurisdiction as this Complaint alleges violations of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*

11.   Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391 as Defendant LinkedIn's principal executive office and headquarters are located in California.

TECHNICAL BACKGROUND

12.   This case, in part, is about the linkage of personally identifiable information with personal data obtained through cookies. Cookies are files of data and/or text sent by a website to an Internet user's computer (and stored on his or her hard drive) to track the user's movements on the Internet. Many websites place cookies that track an Internet user's movement within their own websites. Amazon.com, for example, might use a cookie to improve its users' online experience, e.g., to remember a user's login and password, the user's preferences for viewing the website, the content of the user's shopping cart, or recommend items related to the user's previous purchases or page views.

13.   A third-party cookie, also known as a tracking cookie, is a type of cookie placed by a marketing company, advertising company, data aggregator, or the like (i.e., a "Third Party"). These cookies track a broader type of behavior than just movement within a single website. Third Party cookies collect personal data; they track Internet behavior and record patterns, Internet surfing habits, and demographic information from data across thousands of websites (the "Private Browsing History"), and then, *inter alia*, tailor and target advertisements based on this data or use the data for other purposes the Internet user neither intended nor consented to. For example, because of Third Party cookies, someone who browses various sports websites and makes sports-related purchases might see an advertisement for ESPN on a webpage, while someone who frequents furniture websites and decorating blogs might see an advertisement for West Elm on the same webpage. Or, the data might be sold to a political campaign organization or interest group.

14.   A cookie is placed on a user's computer upon his or her first visit to a website, or, in the case of a Third Party cookie, during the user's first visit to a website within the Third Party's network. Once the cookie is placed, the user's Internet browsing information is stored

on the cookie, and later transmitted to the cookie owner's server to update the file associated with its anonymous cookie ID. The transmission between the cookie and the server occurs through invisible code embedded in various parts of a website. For example, a Third Party's advertisement may have code that calls information from a cookie to its server. A website might also have small, 1 pixel x 1 pixel, transparent images—called a web beacons—that cause a user's computer to send cookie information to the website's or Third Party's server. The tracking devices are invisible, and transmit information about an Internet user's browsing history and behavior without any prompting by the user.

15.   Before any cookie data can be transmitted to a Third Party, the website that the user is visiting must initiate a command telling the Internet user's computer to communicate with that Third Party. The website uses the Internet user's browser as a tool to cause this communication, and dictates which servers the Internet user's browsers should communicate with, and what information it should send to those servers.

16.   For example, with regard to LinkedIn's conduct:

1. An Internet user visits a LinkedIn profile page while logged in to LinkedIn.

2. LinkedIn loads the LinkedIn-related content of that webpage; Spaces are left open on the page for advertisements and other content (such as beacons) to be provided by Third Parties.

3. LinkedIn invisibly sends a command to the Internet user's browser to initiate the loading of advertisements and other content on the webpage. The LinkedIn command:

- Designates the Third Party with which the browser should communicate and from which the browser should obtain the advertisements and other content.

- Requires that the communication include:

  o From the Internet user's hard drive, the cookie identification number of any cookie that is associated with the designated Third Party; *with*

  o The URL[2] of the LinkedIn profile the user is viewing, which includes a LinkedIn ID.

_____

[2] A URL (Uniform Resource Locator), more commonly known as a web address, is the unique, global address of each resource and file on the Web. A URL combines the domain name (e.g., google.com) with additional information like the protocol (e.g., http) and/or the path

4. The Third Party receives, bundled together in a single communication prompted by LinkedIn, the Third Party's cookie identification number and the LinkedIn ID of the page being viewed.

5. The Third Party sends information back to the browser to load advertising and other content in the designated areas of the LinkedIn webpage, and continues to track the user and communicate with the cookie through that content.

17.   Below is an excerpt from a relevant test transmission associated with a test profile, that demonstrates the type of information sent to the Third Party:

> GET /cgi-bin/m1?ci=us-603751h&cg=0&cc=1&si=http%3A//www.linkedin.com/profile/view%3F**id**%3D**110198243**%26authType%3Dname%26authToken%3D2uu_%26goback%3D%252Enmp_*1_*1_*1_*1_*1%26trk%3Dnus_variable_vname&rp=http%3A//www.linkedin.com/home%3Ftrk%3Dhb_tab_home_top&ts=compact&rnd=1300470040318&ja=1 HTTP/1.1
> Host: secure-us.imrworldwide.com
> Referer:
> http://www.linkedin.com/profile/view?id=**110198243**&authType=name&authToken=2uu_&goback=%2Enmp_*1_*1_*1_*1_*1&trk=nus_variable_vname
>
> HTTP/1.1 200 OK
> Set-Cookie: V5=AStfNjA7EigrEhowDBgjIy06GyAHO1InHlL9uQ; expires=Mon, 15-Mar-2021 17:40:40 GMT; <u>domain=.imrworldwide.com</u>; path=/cgi-bin
> Set-Cookie: IMRID=**TYOZGIpsDDwAADNSOeY**; expires=Mon, 15-Mar-2021 17:40:40 GMT; path=/cgi-bin; domain=.imrworldwide.com[3]

(Emphasis added.) In the example above, the LinkedIn ID and the corresponding cookie identifier are indicated in bold. Thus, merely logging in and looking at a profile page caused LinkedIn to transmit the ID bundled with the viewer's tracking cookie ID to IMRWorldwide/Nielsen Netratings. During testing, LinkedIn also sent the test profile's LinkedIn ID to Quantcast, Scorecard Research, and Doubleclick.

18.   LinkedIn could have designed its URL structures so that they did not contain the LinkedIn ID, or could use embedding techniques, such as "iframes," that would deliberately

---

(information regarding the particular sub-part of the website). For example, the URL to reach Google's main search page is http://www.google.com. One of the URLs to reach Google's email service is http://www.google.com/mail (and "mail" is the "path" of the URL). Both of these URLs are at the same "domain name."

[3] This shows that LinkedIn is communicating with IMR Worldwide/Nielsen Ratings. The bolded lettering is the cookie ID number of the cookie on the user's computer. Notably, the cookie is not set to expire, and will continue tracking the user's Private Browsing History (unless deleted), for another decade. The cookie is used to collect the user's browsing habits on other, non-LinkedIn sites, but it is the LinkedIn transmission that allows the browsing history to become linked with the ID.

remove the user ID when it is being transferred to a Third Party. LinkedIn failed to use these security measures to protect its users' information.

<div align="center">

FACTUAL ALLEGATIONS

</div>

LinkedIn Allows Third Party Data Aggregators to Match Plaintiffs' and Class members' Actual Identities with Their Previously-Anonymous Private Browsing History

19.   LinkedIn's privacy policy states that the Company uses cookies "[i]n the course of serving advertisements," but assured Plaintiffs and Class members that "[a]ny information provided to third parties through cookies **will not be personally identifiable**" and "**LinkedIn does not store unencrypted personally identifiable information in the cookies**." (emphasis added).

20.   Contrary to these representations, LinkedIn provides additional, detailed information that gives these Third Parties the ability to 1) match Plaintiffs' and Class members' actual identities, by name and LinkedIn profile, with their previously-anonymous Private Browsing History; 2) view Plaintiffs' and Class members' LinkedIn Browsing History, i.e., determine which particular profiles within LinkedIn each Plaintiff and class member viewed, and 3) identify the personal relationships maintained by Plaintiffs and Class members. In short, because LinkedIn divulges information about its users and their LinkedIn Browsing Histories, the Third Parties are able to place a LinkedIn user's actual identity with his/her personal, Private Browsing History.

21.   LinkedIn failed to take steps to encrypt its users' LinkedIn IDs or eliminate them from transmissions to Third Parties. The Company did not have proper security in place and failed to use commercially reasonable methods to prevent its users' LinkedIn IDs (and thus identities) from being associated with their Private Browsing History. As a result of this failure, LinkedIn provided personally identifiable information to Third Parties that possess extensive, private information about users.

22.   By placing names with personal, private data, LinkedIn violated its promises in its privacy policy that it would keep such information private. LinkedIn connected its users' identities with cookie ID numbers without their informed consent, and in a manner that has

caused or is likely to cause substantial injury to subscribers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by subscribers. LinkedIn caused its subscribers' personal browsing history to be associated with them by name, thereby exposing potentially controversial political views or other sensitive information.

23. LinkedIn also exposed its subscribers' interactions and connections with other profiles, thereby exposing potentially sensitive affiliations, that could, in turn, reveal a user's political views, sexual orientation, or business relationships.

The Sign-Up Process and LinkedIn ID

24. When Plaintiffs first signed up for LinkedIn, they were required to provide their first name, last name, and email address; create a password; provide their country and zip code; indicate whether they are currently employed, looking for a job, or a student; and provide details about their employment or school (e.g., job title and company; general industry (if unemployed); or their education and field of interest). Then, also during the set-up process, LinkedIn offered to search Plaintiffs' email contacts to locate people the Plaintiffs already knew on LinkedIn. Even if they or anyone else had chosen to "skip this step," they would have been asked on the next page to confirm their email account, and told that "we'll also check your [email] contacts to see who you already known [sic] on LinkedIn." After confirming his/her email address, LinkedIn will prompt the user to identify people with whom s/he wishes to connect and offer a "premium account with plans starting from $24.99."

25. After Plaintiffs provided this detailed, private information, LinkedIn processed that information and stored it as a user profile for each Plaintiff. It also stored records of any LinkedIn connections Plaintiffs identified during the set-up process. And LinkedIn assigned each Plaintiff a unique user identification number that is associated with their names and LinkedIn profiles (the "LinkedIn ID").

26. The LinkedIn ID was then correlated with the profile and made visible to those who viewed Plaintiffs' profiles. For example, when viewing a LinkedIn profile, the URL will read, in part, as follows:

http://www.linkedin.com/profile/view?**id=12345678**....

In the URL, "12345678" would be the LinkedIn ID of the user's page that is being viewed.

27.   LinkedIn has apparently acknowledged the significance of the LinkedIn ID, and recently changed the way the ID can be used to locate a profile page. Prior to the filing of the initial complaint, anyone could insert a LinkedIn ID into a URL and visit the corresponding LinkedIn member's public profile. Now, since the filing of the initial complaint, the LinkedIn ID can only be used in a URL to access the profile of someone with whom a member *already* has a LinkedIn connection.

The Process that Divulged Plaintiffs' and Class members' Personal, Private Information

28.   Every time Plaintiffs visited a LinkedIn profile page when logged in, LinkedIn caused the Internet user's browser to transmit information to a third party. Part of that transmission included the URL of the profile page the user was viewing (the "Viewed Page"). By including the profile's LinkedIn ID in the transmission, LinkedIn enabled Third Parties to identify Plaintiff by name and determine which LinkedIn profiles Plaintiffs had viewed (the "LinkedIn Browsing History").

29.   Moreover, LinkedIn divulged this personal, private information together with a Third Party cookie identification number, which corresponds to the Third Party's (otherwise-anonymous) record of webpages that the user has visited in the previous minutes, months, or years—no matter how personal or private.

30.   LinkedIn provides detail that goes far beyond what a Third Party would normally obtain through a cookie, providing "social information"—such as the name of the user and the other LinkedIn profiles they view and interact with—to the otherwise anonymous tracking process.

LinkedIn Allows Third Parties to De-Anonymize its User IDs

31.   In addition to receiving information about what pages a LinkedIn user viewed, LinkedIn's misconduct provided the Third Parties with means to determine which LinkedIn IDs correspond to which profiles, and in particular, which LinkedIn ID corresponds to the Plaintiffs (and thus, their cookie IDs).

32.   Before the complaint was filed, Third Parties could determine which LinkedIn ID corresponded to which user simply by inserting an ID in the appropriate place within the LinkedIn profile URL. The essential form of the LinkedIn profile URL is: http://www.linkedin/com/profile/view?id=[insert ID number here]. LinkedIn thus provided an extremely simple avenue by which the Third Parties could translate the LinkedIn ID into to names and other personal information.

33.   Even now, it is a simple matter for a Third Party to associate a LinkedIn ID with the user. The Third Party need only wait until any one person, who is not connected to the user on LinkedIn (a "stranger"), visits the user's public profile. Although one cannot input a stranger's LinkedIn ID directly into a URL to visit his/her profile page, one *can* view a stranger's profile in various circumstances, e.g., by searching for that stranger's name or clicking a link to the stranger's profile. When visiting a stranger's profile, the URL created by LinkedIn includes parameters, used to control access to strangers' profiles, that act like passwords. Because LinkedIn transmits profile URLs to Third Parties, a URL containing the user's LinkedIn ID, *and* the password-like parameters, will be transmitted to the Third Party after any one visit to the user's profile by a stranger. In other words, if the Third Party received a LinkedIn ID, but was unable to de-anonymize it, as soon as a stranger visited the profile page associated with that ID, the Third Party would receive a working link to the ID's corresponding profile.

34.   The Third Parties can also determine which profile among the Viewed Pages belongs to the user (cookie ID holder). For example, because LinkedIn users generally view their own page more than any other, Third Parties can determine which LinkedIn ID corresponds with each Plaintiff or Class member based simply on the frequency that the LinkedIn ID is transmitted with their cookie IDs.

35.   In addition, certain of LinkedIn's URL structures correspond only to the Internet user's own profile. For example, when a user is signed in to his/her own LinkedIn account and clicks "View Profile," LinkedIn will generate a URL that appears as follows: "http://www.linkedin.com/profile/view?id=[LinkedIn ID number]&trk=tab_pro." This URL structure is only generated when one clicks the "View Profile" link. Accordingly, a Third Party

receiving a URL in this form would know that the LinkedIn ID it includes corresponds to the

user's own profile. The "View Profile" URL thus definitively and easily correlates a LinkedIn

user with its own LinkedIn ID number.

36. In a test run with Mr. Masand's account, the following transmission was

prompted by LinkedIn:

GET /adi/linkedin.dart/nprofile-view-
success;optout=false;lang=en;tile=1;sz=300x250;v=4;u=16iB1Kt5t5lAVnhQJhp7ES;mo
d=400;title=ic;func=finc;coid=10602;ind=80;csize=e;zip=11732;cntry=us;reg=70;sub=1;
jpos=0;con=i;edu=18946;gy=2009;gdr=m;age=23;seg=278;seg=454;seg=230;grp=1153;
grp=126907;grp=43643;grp=958;grp=1227037;grp=1852200;grp=86621;grp=1889180;g
rp=874127;grp=678237;sjt=2019;dcopt=ist;uprofile%3D36277434%3Bcompany%3D10
602%3Bpcntry%3Dus;s=0;ord=526988775? HTTP/1.1
Host: **ad.doubleclick.net**
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
Referer: **http://www.linkedin.com/profile/view?id=XXXXXXXX[4]&trk=tab_pro**
Cookie:
id=2235194150010079|3385069/1043781/15296|t=1315849600|et=730|cs=002213fd480
5441dcdaad43eed

(Emphasis added.) In this test transmission, LinkedIn caused the browser to send a transmission

to Doubleclick. The transmission included a URL that had a unique structure signifying that it

corresponded to Mr. Masand's own profile and which contained Mr. Masand's LinkedIn ID; and

the cookie ID number of the cookie that corresponded to Mr. Masand's browsing history.

LinkedIn's Conduct is a Meaningful Invasion of Plaintiffs' and Class members' Privacy

37. In a year-long investigation into online tracking, the *Wall Street Journal* recently

"exposed a fast-growing network of hundreds of companies that collect highly personal details

about Internet users—their online activities, political views, health worries, shopping habits,

financial situations and even, in some cases, their real names—to feed the $26 billion U.S.

online-advertising industry," thereby demonstrating how lucrative this industry has become.

Available at http://online.wsj.com/article_email/SB10001424052748703529004576

160764037920274 -lMyQjAxMTAxMDIwODEyNDgyWj.html (last visited March 25, 2011).

---

[4] "XXXXXXXX" is the redacted LinkedIn ID.

38.   Third Parties, like Scorecard Research, Quantcast, and Nielsen Netratings

("imrworldwide"), track consumer and Internet behavior to compile marketable, demographic

profiles and statistics. The Third Parties market themselves based on the level of detail about a

consumer that they are able to ascertain, analyze, and compile. These companies are

technologically sophisticated and are able to analyze and cross-reference data from various

sources, distinguish between multiple users of the same computer, and even identify when a

single user utilizes various computers.

39.   For example, Quantcast's website states, in part:

People Versus Cookies

Quantcast provides audience data for both unique cookies counts and people. The Quantcast statistical direct measurement model **takes into account numerous factors to build a translation of cookies to people** that is unique to each digital media property.

(Emphasis added.).

40.   The Quantcast website also includes a white paper entitled "Cookie Corrected Audience Data," which states, in part:

Addressing this challenge requires **innovation in bridging the inherent differences between the directly measureable cookies and estimates of people. This is not unlike challenges that the media industry has previously faced in bridging the "what" (raw traffic) and the "who" (actual people)** in Print. The magazine industry provides an analogy to the challenges in the digital space in that circulation is a "census" level data point (it represents the reported number of magazines printed and distributed) which is coupled with panel data for people-based adjustments (readers per copy, demographics, etc). . . .

The Quantcast model l**everages census level data, directly measured in cooperation with online media publishers, integrated with panel sources in a hybrid statistical model that accounts for the complicating factors of online media measurement, namely cookie deletion and multiple machine usage.**

*   *   *

This whitepaper provides an overview of Quantcast's approach to translating **raw cookie data into actionable, people-based audience intelligence** as part of our broader pixel and panel methodology. It explains of how we model cookies, account for deletion and non-acceptance, and incorporate this data within the broader set of audience measurement challenges.

*   *   *

The Quantcast Approach

Quantcast has a hybrid approach to web site audience measurement that leverages access to multiple complementary data sources. The Quantcast Quantified Publisher program captures over 75 billion media consumption events every month, generated by more than 1.4 billion cookies (data as of June, 2008). **What's more, many of our Quantified Publisher partners share anonymous identifiers with us that are independent of cookies**. Our model also includes several panels which provide for **people-based reference points and calibration which are free of cookie deletion. <u>We triangulate across this mass of data with different collection processes, biases and issues. Our models take into account visit frequency, time periods, the likelihood of multiple computer usage and even the impact of multiple people using the same computer to deliver people based estimates. . . .</u>**

Translating Unique Cookie Counts to People

. . . Quantcast statisticians are dedicated to understanding the dynamic, property-driven factors that impact cookie per machine, number of unique users per machine, as well as the number of machines that are used by people. The primary factors impacting translation from cookies to people are: • *Time period under analysis –* . . . • *Typical visit frequency –* . . . • *Percentage of usage from work or public machines –* . . . • *Type of site –* . . . .

(Emphasis added).

41. Similarly, Nielsen Netratings' website states, in part:

Nielsen's comprehensive and innovative online measurement methodologies **analyze consumer behavior** and trends, advertising effectiveness, brand advocacy, social media buzz and more to provide a **360 degree view of how consumers engage with online media.** Our approach doesn't stop at the computer screen because **we understand that online audiences don't just consume digital "cookies" -- they're a shopper, a car-pooling power mom, a TV watcher, a tweeter and a texter.**

(Emphasis added.)

42. Many if not all of the Third Parties compensate LinkedIn to place advertisements on or collect data from the Company's website. In turn, LinkedIn commands Plaintiffs' and Class members' computers to reach out to these Third Parties to pull advertisements and beacons to display on LinkedIn webpages, and causes Plaintiffs' and Class members' computers to transmit the LinkedIn ID of the Viewed Page contemporaneously with the cookie ID of the cookie placed by the Third Party. Through this invisible action, which occurs without the knowledge or consent of Plaintiffs or Class members, and which does not require Plaintiffs or Class members to click on or interact with any advertisement or Third Party, LinkedIn allows the Third Parties to ascertain marketable, private information about LinkedIn's members.

43. Consequently, Plaintiffs, who have used the Internet to search and view webpages regarding any number of personal, sensitive topics, have profiles of their browsing history

maintained by Third Parties, together with the demographics inferable by his or her search history, that can be marketed and sold in order to provide targeted advertising among a variety of mediums. That information is typically anonymous, correlated only with a cookie ID or IP address, but if the user is on LinkedIn, that profile and Private Browsing History can be identified by name; the users' work, educational, and other LinkedIn profile information can be added; and it can also include the users' friends, family, real-life connections, and information about who that person is interested in observing on LinkedIn.

Personally Identifiable Information and Internet Browsing Behaviors Are Valuable, Marketable Commodities

44.   By collecting personal information from the computers and mobile devices "[w]ebsites and stores can . . . 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." Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), *available at* http://ssrn.com/abstract=1478214. 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, "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").

45.   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." *See* MediaPost, http://mediapost.com/events/?/showID/OMMAGlobalNewYork.09.NewYorkCity/

type/Exhibitor/itemID/647/OMMAGlobalNewYork-Exhibitors%20and%20Sponsors.html (last visited Mar. 25, 2011).

46.   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 given them 70% of the sale. One Allow Ltd. customer received payment of $8.95 for letting Allow tell a credit-card company he is shopping for new plastic. *Id.* In January 2011, at the World Economic Forum in Davos, Switzerland, one discussion centered on turning personal data into an "asset class." During the course of the discussion, Michele Luzi, director at consulting firm Bain & Co. stated, "We are trying to shift the focus from purely privacy to what we call property rights." *Id.*

47.   LinkedIn has profited handsomely from its customers and from the wrongful distribution of their data. From January 2010 to September 2010 the Company earned $161.4 million in revenue from three products: marketing solutions (advertising), premium subscriptions, and hiring solutions (job listings). Advertising accounted for 32% of the Company's revenue ($51.37 million) during that period, and 30% of revenue ($23.8 million) in 2009. Premium subscriptions accounted for 27% of revenue ($44.1 million) from January to September 2010, and 41% of revenue ($33.2 million) in 2009. (*See* http://mashable.com/2011/01/28/linkedins-ipo-an-overview/).

48.   Personal information is property. There is a market for personal data and data regarding individuals' opinions and interests. Individuals can market their own personal information for profit, through, for example, focus groups (which pay individuals to express their interests and opinions), or companies like Allow Ltd., which allow users to sell information to marketers regarding their name, address, employment, and shopping interests and intent (e.g., products the individual is interested in; whether the user is interested in applying for a credit card). The value of such information is diminished, if not eliminated, if that information is publicly distributed or leaked. In addition, personal information has value to companies, like Defendant and the Third Parties, because it can be compiled and sold as demographic data and

advertising analytics, or sold on a per-name basis (for example, companies like infoUSA compile lists of consumer information, and sell name and contract information categorized by demographic data, interests, or other behavioral information).

LinkedIn Violates Its Own Privacy Policy

49.   LinkedIn's privacy policy fails to inform LinkedIn users that the Company transmits its members' LinkedIn-related browsing history or that it allows Third Parties to link their personal identity or LinkedIn profile information with their Private Browsing History. On the contrary, LinkedIn states unequivocally that: **"We do not sell, rent, or otherwise provide your personal identifiable information to any third parties for marketing purposes."**

50.   LinkedIn fails to disclose that it allows marketers to identify otherwise-anonymous cookie information. Instead, it gives users comfort that LinkedIn will not provide any personally identifiably information to third parties or store it with cookies:

> F.   Cookies
>
> In the course of serving advertisements or optimizing the Services to our Users, we may allow authorized third parties to place or recognize a unique cookie on your browser. **Any information provided to third parties through cookies will not be personally identifiable but may provide general segment information (e.g., your industry or geography, career field, or information about your professional or educational background) for greater customization of your user experience.** Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. **LinkedIn does not store unencrypted personally identifiable information in the cookies.**

See Exhibit B (emphasis added).

51.   Regarding "Advertising and Web Beacons," LinkedIn states that advertisements may be targeted to users "based on **anonymized information,**" and states that**: "LinkedIn does not provide personally identifiable information to any third party ad network."** *See* Exhibit B (emphasis added).

52.   Regarding the use of "Log files, IP addresses and information about your computer and mobile device," LinkedIn represented to Plaintiffs and Class members that: "**The linkage between your IP address and your personally identifiable information is not shared with third parties without your permission**," providing exceptions only for consent and

1 compliance with subpoena or other legal process, investigation, or enforcement. *See* Ex. B

2 (emphasis added).

3   53.   With respect to "Sharing Information with Third Parties," LinkedIn makes the

4 following representations:

> 5 **LinkedIn takes the privacy of our Users very seriously, and we do not sell,**
> 6 **rent, or otherwise provide your personally identifiable information to third**
> **parties for marketing purposes.** Further, we will only share your personally
> 7 identifiable information with third parties to carry out your instructions or to
> provide the Services or information unless compelled by law, or as necessary to
> 8 enforce our User Agreement or protect the rights, property, or personal safety of
> LinkedIn, its Users, and the public. For example, we use a credit card processing
> 9 company to bill Users for subscription fees. These third parties do not retain,
> share, or store any personally identifiable information except to provide these
> 10 services, and they are bound by confidentiality agreements limiting the use of
> your information.

11 Ex. B (emphasis added).

12   54.   LinkedIn's statements that: "maintaining your trust is our top concern" and

13 "LinkedIn takes the privacy of our Users very seriously, and we do not sell, rent, or otherwise

14 provide your personally identifiable information to third parties for marketing purposes"; and its

15 representations that it is a licensee of the "TRUSTe Privacy Program" and that it participates in

16 the EU Safe Harbor Privacy Framework as set forth by the U.S. Department of Commerce;

17 falsely indicated to Plaintiffs and Class members that LinkedIn was guarding their personal

18 information.

19   55.   Here, LinkedIn's privacy policy explicitly assures that its members' personally

20 identifiable information will not be provided to Third Parties (but it is). Even had the privacy

21 policy not made such plain assurances, or had it accurately described LinkedIn's divulgement of

22 members' personally identifiable information and LinkedIn-related browsing history, LinkedIn

23 could not be excused from its misconduct as a result of any part of its privacy policy.

24   56.   LinkedIn's privacy policy, which has been described as a "6,250-word essay" (*see*

25 http://www.pcadvisor.co.uk/news/index.cfm?newsid=3223258&pn=2), is dense and confusing. It

26 is widely accepted that such privacy policies are ineffective when it comes to providing

27 consumers with useful and accurate information or disclosure. In a preliminary staff report

28 prepared by the Federal Trade Commission, entitled, *Protecting Consumer Privacy in an Era of*

AMENDED CLASS ACTION COMPLAINT   - 17 -

Rapid Change, the Federal Trade Commission stated that, "[T]he notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand" and that they are wholly inadequate in an age in which companies "collect and use consumers' information in ways that often are invisible to consumers." FTC Report at iii. The FTC also found that "privacy notices are often opaque, lack uniformity, and are too long and difficult to navigate. Too frequently they bury disclosures of important information. . . . A particularly strong illustration of where privacy policies have been ineffective is in the mobile context where, because of the small size of the device, a privacy notice can be spread out over 100 separate screens. Indeed, it is difficult to imagine consumers scrolling through each screen or making informed choices based on the information contained in them." *Id.* at 70. *See also*, Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S L.J. & Pol'y for Info. Soc'y 543, 565 (2008) (estimating that it would take consumers hundreds of hours to read the privacy policies they might typically encounter in one year on the Internet).

57.   LinkedIn's customers, including Plaintiffs and the Class, pay for LinkedIn's services either monetarily, or by providing their personally identifiable information. Personally identifiable information constitutes valuable property that was exchanged not only for Defendant's services, but also in exchange for Defendant's promises that it would not make "[a]ny information provided to third parties through cookies. . . personally identifiable" and that it "does not provide personally identifiable information to any third party ad network." As a result of LinkedIn's misconduct, and its role in contributing to the breach of Plaintiffs' personally identifiable information and association of that information with otherwise-anonymous browsing history, LinkedIn caused Plaintiffs and the Class to lose the value of their personally identifiable information.

CLASS ACTION ALLEGATIONS

58.   Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23 on behalf of a Class defined as follows: All persons who reside in the United States and who, any time after March 25, 2007, signed up for LinkedIn's services.

59. Excluded from the Class are Defendant; any parent, subsidiary, or affiliate of Defendant or any employees, officers, or directors of Defendant; legal representatives, successors, or assigns of Defendant; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

60. **Numerosity**. The Class members are so numerous and dispersed nationwide that joinder of all members is impracticable. Upon information and belief, the Class members number in the hundreds of thousands, if not millions. The exact number of Class members is unknown, but can be determined from Defendant's computerized and other records. Plaintiffs reasonably estimate and believe that there are thousands of persons in the Class.

61. **Commonality**. There are numerous and substantial questions of law and fact that are common to all members of the Class, which predominate over any question affecting only individual Class members. The members of the Class were and continue to be subjected to the same practices of the Defendant. The common questions and issues raised by Plaintiffs' claims include:

- whether Defendant shared Plaintiffs' and the Class's personal information with third-party advertisers and online tracking companies;

- whether LinkedIn violated its own Terms and Privacy Policies by sharing of Plaintiffs' personal information with third-party advertisers, and online tracking companies;

- whether LinkedIn breached its contract with consumers, and if so, the appropriate measure of damages and remedies against Defendant for such breach;

- whether LinkedIn breached the covenants of good faith and fair dealing, and if so, the appropriate measure of damages and remedies against Defendant for such breach;

- whether Defendant violated the SCA; California Business and Professions Code § 17200 *et seq*.; California Business and Professions Code § 17500 *et seq*.; Consumer Legal Remedies Act, California Civil Code § 1750; Article I, Section 1 of the California Constitution; and other violations of common law;

- whether Plaintiffs and the Class have been damaged as a result of Defendant' alleged violations as alleged herein; and, if so, the appropriate relief for Defendant' violations; and

- whether Defendant have been unjustly enriched as a result of its unlawful conduct, and, if so, whether Defendant should disgorge inequitably obtained

money that they have been unjustly enriched by; and, the nature and extent of any other remedies, and injunctive relief, to which Plaintiffs and the Class are entitled.

62.   **Typicality**. Plaintiffs' claims are typical of the claims of all of the other members of the Class, because their claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendant.

63.   **Adequacy**. Plaintiffs will fairly and adequately protect the interests of all members of the class in the prosecution of this Action and in the administration of all matters relating to the claims stated herein. Plaintiffs are each similarly situated with, and have suffered similar injuries as, the members of the Class he seeks to represent. Plaintiffs have retained counsel experienced in handling class action lawsuits. Neither Plaintiffs nor their counsel have any interest that might cause them not to vigorously pursue this action.

64.   **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy, since individual joinder of the Class members is impracticable. Even if individual Class members were able to afford individual litigation, it would be unduly burdensome to the Courts in which the individual litigation would proceed. Defendant have subjected the Class to the same violations as referenced herein. Accordingly, class certification is appropriate under Rule 23 because common issues of law and fact regarding Defendant' uniform violations predominate over individual issues, and class certification is a superior method of resolving these claims. No unusual difficulties are likely to be encountered in the management of this action as a class action. Defendant acted and continue to act in a manner that is generally applicable to all members of the Class, making final injunctive relief appropriate.

FIRST CAUSE OF ACTION
(Stored Communications Act, 18 U.S.C. § 2701 *et seq*.)

65.   Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

66. Defendant violated the Stored Communications Act (SCA) by disclosing Plaintiffs' and Class members' LinkedIn-related browsing history. Plaintiffs and Class members suffered injury-in-fact, and the SCA provides for statutory damages.

67. Defendant also violated the SCA by disclosing information regarding the Viewed Page. Plaintiffs and Class members suffered injury-in-fact, and the SCA provides for statutory damages.

68. Defendant also violated the SCA by disclosing Plaintiffs' and Class members' LinkedIn IDs. Plaintiffs and Class members suffered injury-in-fact, and the SCA provides for statutory damages.

69. Defendant provides electronic communication service to the public *via* their LinkedIn accounts. 18 U.S.C. § 2510(15).

70. Defendant provides remote computing service to the public because they provide computer storage and processing services by means of an electronic communications system. 18 U.S.C. § 2711(2).

71. The LinkedIn users' personal identification numbers and personal information that are stored by Defendant are electronic communications within the meaning of 18 U.S.C. § 2510 (12).

72. Defendant holds their users' personal identification number and personal information in electronic storage within the meaning of 18 U.S.C. § 2510(17).

73. Defendant knowingly divulged confidential and private information relating to Plaintiffs' electronic communications in violation of 18 U.S.C. § 2701 *et seq.* of the SCA.

74. In part, 18 U.S.C. § 2702(a)(1)-(2) of the SCA provides that a person or entity shall not: "(1) . . . knowingly divulge to any person or entity the contents of a communication . . . ; and (2) . . . shall not knowingly divulge to any person or entity the contents of any communication . . . ."

75. Section 2707 of the SCA provides for a civil cause of action and allows for damages, and declaratory and equitable relief.

76. By engaging in the foregoing acts, Defendant knowingly divulge the contents of communication carried and maintained by Defendant on behalf of and received by transmissions from their users in violation of 18 U.S.C. § 2702(a)(2).

77. Defendant engaged in the foregoing acts without obtaining the lawful consent of the user.

78. Plaintiffs and the Class are entitled to statutory damages of no less than $1,000.00 (one thousand dollars) per violation. Because Defendant' violations were willful and intentional, Plaintiffs and the Class are entitled to recover punitive damages as provided by 18 U.S.C. § 2702(c).

SECOND CAUSE OF ACTION
(Article I, Section 1 of the California Constitution)

79. Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

80. Defendant disclosed Plaintiffs' and Class members' personal information, including their LinkedIn-related browsing history. Accordingly, Plaintiffs' and Class members' personal privacy rights were violated; they suffered injury-in-fact and are entitled to damages.

81. Defendant disclosed Plaintiffs' and Class members' personal information by causing the transmission of their LinkedIn IDs (which conveyed their actually identities) along with a cookie identifier that correlated with their previously-anonymous, Private Browsing History. Accordingly, Plaintiffs' and Class members' personal privacy rights were infringed upon; they suffered injury-in-fact and/or were harmed and are entitled to damages.

82. The California Constitution expressly grants an inalienable right to privacy.

83. Plaintiffs had a legally protected informational privacy interest in the confidential and sensitive information that Defendant obtained from them and unlawfully disseminated.

84. Plaintiffs had a legally protected autonomy privacy interest in making intimate personal decisions regarding their use of the Internet without observation, intrusion or interference.

85. Plaintiffs reasonably expected that their confidential and sensitive information and intimate personal decisions would be kept private.

86. Defendant committed a "serious invasion of privacy" by revealing Plaintiffs' PII in conjunction with data tracking cookies, thereby enabling third parties to collect and stockpile information—about individuals who can be identified by name—without the individuals' consent or control.

<div align="center">

THIRD CAUSE OF ACTION
(Violation of California Business and Professions Code § 17500, *et seq.*
Untrue and Misleading Statements)

</div>

87. Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this Complaint.

88. Plaintiffs assert this cause of action against Defendant for violations of California Business and Professions Code § 17500 *et seq*. for untrue and misleading statements.

89. At all relevant times, Defendant engaged in a scheme of offering its LinkedIn services to Plaintiffs by way of, *inter alia*, commercial marketing and advertising, the World Wide Web (Internet), product packaging and labeling, and other promotional materials. These materials misrepresented and/or omitted the truth about the extent to which Defendant would share valuable personal information with third parties. Defendant knew, or should have known, that these statements were deceptive, misleading, or untrue.

90. Said advertisements and inducements were made within the State of California and come within the definition of advertising as contained in Business and Professions Code § 17500 *et seq*. in that such promotional materials were intended as inducements to purchase and use products and services offered by Defendant and are statements disseminated by Defendant to Plaintiffs and were intended to reach Plaintiffs. Defendant knew, or should have known, that these statements were misleading and deceptive.

91. In furtherance of said plan and scheme, Defendant have prepared and distributed within the State of California *via* commercial marketing and advertising, the World Wide Web (Internet), product packaging and labeling, and other promotional materials, statements that

1 misleadingly and deceptively represent the truth about personal information that LinkedIn users

2 entrust to Defendant.

3   92.   Consumers, including Plaintiff, were among the intended targets of such

4 representations.

5   93.   The above acts of Defendant, in disseminating said misleading and deceptive

6 statements throughout the State of California to consumers, including Plaintiff, were and are

7 likely to deceive reasonable consumers, including Plaintiff, by obfuscating the truth about

8 Defendant' use of their personal information.

9   As a result of the above violations, Plaintiffs have suffered injury in fact and lost money

10 or property. Plaintiffs and the Members of the Class, pursuant to Business and Professions Code

11 § 17535, are entitled to an order of this Court enjoining such future conduct on the part of

12 Defendant, and such other orders and judgments that may be necessary to return Defendant' ill-

13 gotten gains and restore to any person in interest any money paid for Defendant' services as a

14 result of the wrongful conduct of Defendant.

15   **FOURTH CAUSE OF ACTION**
                              (Breach of Contract)
16

17   94.   Plaintiffs hereby incorporate by reference the allegations contained in all of the

18 preceding paragraphs of this complaint.

19   95.   Plaintiffs submit personal information to LinkedIn and LinkedIn promises that it

20 will not share this information with third-party advertisers without Plaintiffs' consent, and the

21 consent of each Class member, respectively.

22   96.   The LinkedIn Privacy Policy states that LinkedIn will not divulge personal

23 information to outside advertising companies without the user's consent. Despite this promise,

24 LinkedIn did in fact knowingly share users' personal information with third-party advertisers in

25 violation of its own Agreement with its users.

26   97.   Plaintiffs never consented to the sharing of their personal information to third-

27 party advertisers.

28   98.   Plaintiffs have performed their obligations under the contract.

AMENDED CLASS ACTION COMPLAINT   - 24 -

99.   LinkedIn materially breached its contractual obligations through its conduct as alleged herein, including its transmission of Plaintiffs' personal information to third-party advertisers, as well as Plaintiffs' personal identification numbers without consent.

100.   Plaintiffs and the Class have been damaged as a direct and proximate result of LinkedIn's breach of their agreements with Plaintiffs and the Members of the Class.

FIFTH CAUSE OF ACTION
(Common Law Invasion of Privacy)

101.   Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

102.   Defendant disclosed Plaintiffs' and Class members' personal information, including their LinkedIn-related browsing history. Accordingly, Plaintiffs' and Class members' personal privacy rights were infringed upon; they suffered injury-in-fact and/or were harmed and are entitled to damages.

103.   Defendant disclosed Plaintiffs' and Class members' personal information by causing the transmission of their LinkedIn IDs (which conveyed their actually identities) along with a cookie identifier that correlated with their previously-anonymous, Private Browsing History. Accordingly, Plaintiffs' and Class members' personal privacy rights were infringed upon; they suffered injury-in-fact and/or were harmed and are entitled to damages.

104.   Plaintiffs each had a legally protected informational privacy interest in the confidential and sensitive information that Defendant obtained and unlawfully disseminated.

105.   Plaintiffs and the Class members had a legally protected autonomy privacy interest in making intimate personal decisions regarding their use of their computers and mobile devices without observation, intrusion or interference.

106.   Plaintiffs and the Class members reasonably expected that their confidential and sensitive information and intimate personal decisions would be kept private.

107.   Defendant intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by making public Plaintiffs' personally identifying information in conjunction with her personal identification number and data tracking cookies.

1 108. As a consequence, Plaintiffs were personally injured and suffered emotional
2 distress damages.

SIXTH CAUSE OF ACTION
(Conversion)

5 109. Plaintiffs hereby incorporate by reference the allegations contained in all of the
6 preceding paragraphs of this complaint.

7 110. Plaintiffs' personal browsing history and other personally identifiable information
8 – including full name, email address, mailing address, zip code, telephone number, and credit
9 card number – is valuable property owned by Plaintiffs.

10 111. Defendant unlawfully exercised dominion over said property and thereby
11 converted Plaintiffs' and the Class members' respective personal information by providing it to
12 third parties in violation of the Stored Communications Act, 18 U.S.C. § 2701 *et seq*., and in
13 violation of its contracts with Plaintiffs and the respective Class members.

14 112. Plaintiffs and the Class were damaged thereby.

SEVENTH CAUSE OF ACTION

(Unjust Enrichment)

17 113. Plaintiffs hereby incorporate by reference the allegations contained in all of the
18 preceding paragraphs of this complaint.

19 114. By engaging in the conduct described in this Complaint, Defendant have
20 knowingly obtained benefits from Plaintiffs under circumstances that make it inequitable and
21 unjust for Defendant to retain them.

22 115. Defendant has received a benefit from Plaintiffs and Defendant have received and
23 retained money from advertisers and other third parties as a result of sharing the personal
24 information of Defendant's users' with those advertisers without Plaintiffs' knowledge or
25 consent as alleged in this Complaint.

26 116. Plaintiffs did not expect that Defendant would seek to gain commercial advantage
27 from third parties by using their personal information without their consent.

28

1   117.   Defendant knowingly used Plaintiffs' personal information without their

2 knowledge or consent to gain commercial advantage from third parties and had full knowledge

3 of the benefits they have received from Plaintiffs. If Plaintiffs had known Defendant was not

4 keeping their personal information from third parties, they would not have consented and

5 Defendant would not have gained commercial advantage from third parties.

6   118.   Defendant will be unjustly enriched if Defendant is permitted to retain the money

7 paid to them by third parties, or resulting from the commercial advantage they gained, in

8 exchange for Plaintiffs' personal information.

9   119.   Defendant should be required to provide restitution of all money obtained from

10 their unlawful conduct.

11   120.   Plaintiffs and the members of the Class are entitled to an award of compensatory

12 and punitive damages in an amount to be determined at trial or to the imposition of a

13 constructive trust upon the wrongful revenues and/or profits obtained by and benefits conferred

14 upon Defendant as a result of the wrongful actions as alleged in this complaint.

15   121.   Plaintiffs and the Class have no remedy at law to prevent Defendant from

16 continuing the inequitable conduct alleged in this complaint and the continued unjust retention of

17 the money Defendant received from third-party advertisers.

18   **EIGHTH CAUSE OF ACTION**
                           (Negligence)
19

20   122.   Plaintiffs incorporate the above allegations by reference as if fully set forth

21 herein.

22   123.   LinkedIn owed a duty to Plaintiffs and Class members to comply with its stated

23 privacy policy and terms of service, and to protect its users' information from disclosure to or

24 access by unauthorized third parties.

25   124.   LinkedIn breached its duty by allowing Referer Headers—send to Third Parties

26 that include data aggregators and marketers—to include unencrypted LinkedIn IDs. LinkedIn

27 also breached its duty by allowing unauthorized third parties to access users' LinkedIn profiles

28

by using their IDs. This exposure and transfer of Plaintiffs' and class members' information was done without customers' knowledge or permission.

125.   LinkedIn's negligent actions directly and proximately caused Plaintiffs and Class members harm.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff Low, on behalf of himself and the Class, requests the following relief:

A.   An order certifying that this action is properly brought and may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs be appointed as Class Representatives, and that Plaintiffs' counsel be appointed Class Counsel;

B.   An award of damages as alleged above;

C.   Restitution of all monies unjustly obtained or to be obtained from Plaintiffs and members of the Class;

D.   Declaratory and injunctive relief;

E.   An award of reasonable attorneys' fees and costs; and

F.   Such other relief at law or equity as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand trial of their claims by jury to the extent authorized by law.

DATED: December 2, 2011   Respectfully submitted,

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

- and -
REESE RICHMAN LLP

AMENDED CLASS ACTION COMPLAINT   - 28 -

Michael R. Reese (Cal. Bar No. 206773)
Kim E. Richman
Belinda L. Williams
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643-0500

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that, on December 2, 2011, I electronically filed the foregoing with the Clerk of the Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record via transmission of Notices of Electronic Filing generated by the ECF System.

/s/ Peter E. Seidman
PETER E. SEIDMAN

AMENDED CLASS ACTION COMPLAINT