IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS

Franchise Dynamics, LLC, individually and on behalf of all others similarly situated, Plaintiffs, v. Google, Inc., a Delaware Corporation Defendant.	

CLASS ACTION COMPLAINT

Plaintiff, Franchise Dynamics, LLC, by and through its attorneys, Clint Krislov, Krislov & Associates, Ltd., makes this its complaint against Defendant, Google, Inc. ("Defendant"). In support of its Complaint, Plaintiff states as follows:

NATURE OF THE ACTION

1. This lawsuit is brought by Plaintiff on behalf of a proposed class of similarly situated individuals who suffered privacy intrusions resulting from Defendant's intentional circumvention of privacy settings on Apple, Inc.'s internet browser "Safari." As set forth in detail *infra*, the Defendant (in utter disrespect for its declared mission "Don't be evil.") did mislead through intentional manipulation and exploitation of Safari's cookie blocking policy and bypassed the security settings set by Plaintiff and the below proposed class in Safari on their respective internet browsing devices. Defendant then placed third-party cookies on Plaintiff's and the proposed class' internet browsing devices and, *inter alia*, tracked and compiled data on Plaintiff's and the proposed class' internet activity without their knowledge or consent. In fact, Defendant's intrusion occurred not only without Plaintiff's and the proposed class' consent, but

in direct contravention to Defendant's promise, pursuant to its privacy policy, that Safari users would be immune from such tracking. With this data, Defendant was then able to sell and direct personalized, interest-based advertisements towards Plaintiff and the proposed class on the basis of their tracked internet activity. As a result, Defendant reaped extensive profits by violating the privacy rights of Safari users on a massive scale, disgorging them of the economic value of their own information. Plaintiff seeks monetary and injunctive relief.

2. Defendant's actions violated (1) the Federal Wiretap Act, 18 U.S.C. § 2511 (2) Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (3) the Stored Electronic Communication Act, 18 U.S.C. § 2701, (4) the Illinois Computer Crime Prevention Law, 720 ILCS 5/17-51, (5) the Illinois Consumer Fraud and Deceptive Business Practices Act, 815ILCS 505/1, *et seq*., (6) Breach of Contract, and (7) Unjust Enrichment.

JURISDICTION AND VENUE

3. This Court has personal jurisdiction over the Defendant because Defendant conducts substantial business in the State and maintains continuous and systematic contact with the State. Defendant also has agents and representatives in the State and maintains an office at 20 West Kinzie St., Chicago Illinois. This Court has personal jurisdiction over the Plaintiff because Plaintiff is domiciled in the State and was injured in the State.

4. This court has subject matter jurisdiction over this action and Defendant pursuant to 28 U.S.C. § 1331 because this action arises under federal statutes, namely the Federal Wiretap Act, 18 U.S.C. § 2511, the Stored Electronic Communications Act, 18 U.S.C. § 2701, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Subject matter jurisdiction over this matter is also proper pursuant to 28 U.S.C. § 1332(d)("CAFA") because the amount in controversy exceeds $5,000,000 and concerns more than 100 class members.

5. Venue is proper in this District because Defendant maintains an office in the District and because a substantial part of the events or omissions giving rise to Plaintiff's claim occurred in this District.

PARTIES

6. Plaintiff, Franchise Dynamics, LLC ("Plaintiff") is an Illinois corporation with its principal office at 905 W 175th Street, Suite 2-SW, Homewood, Illinois 60430. Plaintiff maintained computers manufactured by Apple, Inc. and its employees used Apple, Inc.'s Safari browser to navigate the internet. Plaintiff and Plaintiff's employees' internet activity was tracked through Defendant's placement of tracking cookies on those computers, without Plaintiff's or Plaintiff's employees' knowledge or consent, after they visited websites subject to Defendant's "cookie synching" mechanism. Plaintiff and Plaintiff's employees used Safari under the default privacy settings set to block third-party cookies.

7. Defendant, Google, Inc., is a Delaware corporation with its principal executive offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

JURY DEMAND

8. Plaintiff and the Plaintiff Class demand a jury trial on all issues so triable.

SUBSTANTIAL ALLEGATIONS

9. According to Defendant's 10-K filing for the fiscal year ending December 31, 2011, Defendant "is a global technology leader focused on improving the ways people connect with information" whose "innovations in web search and advertising have made [it's] website a top internet property and [it's] brand one of the most recognized in the world."

10. Moreover, Defendant's own statements reveal its reliance on advertising revenue:

> We generate revenue primarily by delivering relevant, cost-effective online advertising. Businesses use our AdWords program to promote

> their products and services with targeted advertising. In addition, the third parties that comprise the Google Network use our AdSense program to deliver relevant ads that generate revenue and enhance the user experience.

Under the section labeled "ITEM 1A. RISK FACTORS," Defendant more specifically describes the extent of its financial reliance on generating sales for client advertisers through its services:

> We generated 96% of our revenues in 2011 from our advertisers. Our advertisers can generally terminate their contracts with us at any time. Advertisers will not continue to do business with us if their investment in advertising with us does not generate sales leads, and ultimately customers, or if we do not deliver their advertisements in an appropriate and effective manner. If we are unable to remain competitive and provide value to our advertisers, they may stop placing ads with us, which would negatively affect our revenues and business.

11. In the same section Defendant also reveals the intensely competitive nature of the market it participates in:

> Our business is rapidly evolving and intensely competitive, and is subject to changing technology, shifting user needs, and frequent introductions of new products and services. We have many competitors in different industries, including general purpose search engines, vertical search engines and e-commerce sites, social networking sites, traditional media companies, and providers of online products and services. Our current and potential competitors range from large and established companies to emerging start-ups. Established companies have longer operating histories and more established relationships with customers and users, and they can use their experience and resources in ways that could affect our competitive position, including by making acquisitions, investing aggressively in research and development, aggressively initiating intellectual property claims (whether or not meritorious) and competing aggressively for advertisers and websites. Emerging start-ups may be able to innovate and provide products and services faster than we can.

Defendant also notes in its 10-K that "[o]ur advertisers typically advertise in multiple media, both online and offline."

12. Most of Defendant's advertising clients pay on a cost-per-click basis. Defendant also offers a cost-per-impression basis which charges advertisers each time their ad displays to a user.

13. Defendant's complete circumvention of Safari's and users' privacy protection, as described *infra*, violates a Consent Decree previously executed between Defendant and the Federal Trade Commission (FTC):

> It is ordered that respondent [Google], in or affecting commerce, shall not misrepresent in any manner, expressly or by implication: (A) the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) The purposes for which it collects and uses information, and (2) the extent to which consumers may exercise control over collection, use, or disclosure of covered information.[1]

THE BEHAVIORAL ADVERTISING MARKET

14. In general, behaviorally targeted advertisements based on a user's tracked internet activity sell for at least *twice* as much as non-targeted, run-of-network ads.[2] In the behavioral advertising market, "the more information is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."[3]

15. In general, behaviorally-targeted advertisements produce 670% more clicks on ads per impression than run-of-network ads. Behaviorally-targeted ads are also over twice as likely to convert users into buyers of an advertised product as compared to run-of-network ads: Run-of-network ads have an average conversion rate of 2.8% while behaviorally-targeted ads have an average conversion rate of 6.8%.[4]

---

[1] *Google, Inc.*, FTC File No. 102 3136 (3/30/11), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf
[2] Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads, Network Advertising Initiative (NAI), http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf (2010).
[3] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at 37.
[4] Howard Beales, *The Value of Behavioral Targeting*, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (2010).

16. Internet users in the United States ascribe real and substantial monetary value to their internet privacy. Specifically, a study conducted in 2002 found that United States subjects valued, *inter alia*, restriction against improper access to their computers in the range between $11.33 and $16.58.[5]

17. In fact, Defendant acknowledges that tracked online activity has tangible economic value to internet users. Defendant provides continuing monetary compensation to internet users who sign up for its Screenwise Trends panel, in the form of gift cards worth up to $25 for initially signing up, and additional gifts every three months thereafter while the internet user remains on Screenwise.[6] In order to be compensated, a user on Screenwise must simply "add a browser extension that will share with Google the sites you visit and how you use them." Defendant launched the Screenwise Project January 2012.

18. Companies which collect online information from internet users, such as Defendant, can identify users through pseudonymous identification. For instance, a user who is logged into an online account might visit a webpage and as a result of being logged in, have his email or account ID included in the URL. The browser will send a request to the ad servers containing the URL, and the ad server will associate its own "anonymous" ID with the user's ID or email address contained in the URL. Another method by which Defendant can obtain pseudonymous identification is described below:

> The logic is straightforward: in the course of a typical day, you might comment on a news article about your hometown, tweet a recipe from your favorite cooking site, and have a conversation on a friend's blog. By these actions, you have established a public record of having visited these three specific URLs. How many other people do you expect will have visited all three, and at roughly the same times that you did? With a very high probability, no one else. This means that an algorithm combing through a database of anonymized clickstreams can

[5] Il-Horn Hann, et al., *The Value of Online Information Privacy: Evidence from the USA and Singapore*, http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (2002).
[6] http://www.google.com/landing/screenwisepanel/

> easily match your clickstream to your identity. And that's in the course of a single day. Don't forget that tracking logs usually stretch to months and years.[7]

In fact, the FTC has recognized the blurring distinction between personally identifiable information (PII) and non-PII, noting that "businesses combine disparate bits of 'anonymous' consumer data from numerous different online and offline sources into profiles that can be linked to a specific person."[8]

THE GOOGLE DISPLAY NETWORK AND DOUBLECLICK.NET

19. As defined by Defendant, "[t]he Google Network is a large group of websites and other products, such as email programs and blogs, who have partnered with Google to display AdWords ads. Advertisers have the option of running their ads on Google as well as the Google Network for no extra cost. AdWords are placed based either on searches or website content, so the Google Network has two components: the Search Network and the Display Network."

20. The Google Search Network is limited to Google search result pages, result pages from Google powered search sites, pages related to search results, site directory pages on partner search sites (e.g. AOL.com) and other Google search sites (e.g. Google Images, Maps, Shopping). On the Search Network, advertisements are targeted at users based solely on the user's input search terms.

21. The Google Display Network (formerly known as the "Google Content Network") encompasses third-party sites other than search networks that have partnered with Defendant to display Google Ads ("Display Partners"). Unlike the Search Network, targeted advertisements on the Display Network are based on "themes" in advertisers' keyword lists. However, in order to display appropriate advertisements, Defendant utilizes third-party tracking

[7] Arvind Naraayanan, *There Is No Such Thing As Anonymous Online Tracking*, http://cyberlaw.stanford.edu/node/6701.
[8] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at 36.

cookies to track a user's internet activity and display targeted advertisements matching the theme of an advertiser's keyword list based on that user's internet activity.

22. These third-party tracking cookies originate from DoubleClick.net, Defendant's ad servicing subsidiary. Cookies from DoubleClick.net are automatically written onto a user's internet browsing device whenever a user visits a webpage on the Google Display Network in order to fill Google ad templates on the webpage.

23. Doublclick.net cookies compile data on the user which includes but is not necessarily limited to their Internet Protocol (IP) address, web browser, operating system, internet service provider, bandwidth, referral URL, and the time of day. DoubleClick.net cookies also match a "DoubleClick ID" to the user.

24. DoubleClick.net cookies are persistent cookies which remain on a user's device after they close their browser session, and are set to expire after a specified period of time.

25. By recording URL entries, Defendant compiles data on the websites the user visited, as well as the user's searches. Many websites include a user's username and/or email address in their URLs if the user is signed into that website's account, which information is recorded by the cookies, as described *supra*.

26. Upon information and belief, Defendant identifies and tracks users with its tracking cookies from DoubleClick.net, long after termination of their browsing session, through pseudonymous identification described *supra* at ¶ 18.

27. Moreover, all cookies, in general, are associated with the user's computer or device operating system login username. For instance, a user who has a username of "johndoe" in Windows and an unidentified password to log onto Windows on their computer will have cookies stored on their computer with a file name of "cookie:johndoe@doubleclick."

28. Defendant unlawfully collected personally identifiable information (PII). Among the methods by which Defendant could obtain such information was via POST tracking from its third-party tracking cookies, which records information that a user submits to other websites in an online form with their name, web alias, address, email, phone number, credit card number, social security number, etc.

THE COOKIE SYNCHING MECHANISM

29. The innovation of social advertising led Defendant to incorporate the +1 button (formerly known as "Buzz") on the Google Display Network in September 2011. When a user clicks the +1 button and they are signed into a Google account (Gmail, Google+, etc.), Defendant records that information and makes it displayable to all of that user's Google+ friends and Gmail contacts. Defendant also compiles this information to target advertisements to that user's friends and contacts in the future. The +1 button thus acts as a sort of online "referral" advertising service.

30. In order for the +1 button to provide data that can be linked to the user's Google account friends and contacts, Defendant must be able to detect the Google identity of the user that clicks the +1 button on a third-party site. However, the advertisements displayed on third-party sites are loaded from DoubleClick.net, which maintains its own ID of the user on its cookies separate from the user's Google ID.

31. Thus, in order to identify the user clicking a +1 button, Defendant introduced an additional "Google Social Cookie" with an encryption of the user's Google ID that would load in addition to DoubleClick.net tracking cookies. This method is known as "cookie synching."

32. Actual clicking of the +1 button is not required to load the Google Social Cookie onto a user's internet browsing device pursuant to Defendant's "cookie synching" mechanism.

When a user requests access to a website that is part of the Google Display Network, that website is rendered on the user's browser and sends an ad request to the DoubleClick.net server to fill an ad block on the webpage. The ad response then embeds a Google.com "iframe"[9] inside the empty ad block. This iframe makes a request to a Google cookie server to determine whether the user is logged into a Google account.

33. If the user is logged in to a Google account, the Google cookie server redirects the request to Google account servers to identify the user's Google account ID. This request is then redirected as a Social Cookie set on DoubleClick.net servers, and the Social Cookie with an encryption of the user's Google account ID is written onto the user's browser from DoubleClick.net.

34. If the user is not logged in, an "empty" Social Cookie is placed on the user's browser.

35. The Social Cookies remain on the user's internet browsing device after the user terminates their internet session by closing their browser for 24 hours (if the user is logged into a Google account) or 12 hours (if the user is not logged in).

36. The Google Social Cookie is loaded in addition to the ordinary DoubleClick.net tracking cookies, which are also written onto user's internet browsing device whenever the user accesses a webpage displaying DoubleClick.net adds, i.e. websites that are part of the Google Display Network.

37. The above described cookie synching mechanism is not necessary to make Defendant's +1 buttons clickable, but necessary to serve Defendant's information collecting purposes.

[9] An "iframe" is a type of HTML frame device used to display an additional webpage within a single browser window. In effect, it allows a webpage to be displayed within another webpage.

DEFENDANT'S CONDUCT WITH RESPECT TO SAFARI

38. On February 17, 2012, Jonathan R. Mayer, a graduate student in computer science and law at Stanford University, released a blog post[10] identifying "four advertising companies that unexpectedly place trackable cookies in Safari." In that post, Mayer offered a comprehensive analysis of Safari's third-party cookie[11] blocking policy as well as Defendant's method for circumventing it.

39. Safari is different from other browsers in that it blocks third-party cookies, unless the user voluntarily interacts with the third-party domain. The increased level of privacy and protection is one of Apple's primary selling points for its Safari browser, as indicated in its promotional materials. Moreover, Safari's "Privacy" preference settings option to block cookies is denoted by a radio button labeled "Block cookies: From third parties and advertisers," indicating Safari's and the user's intent to surf the internet without allowing advertising related tracking. Thus, by virtue of using Safari as their browser on privacy settings set to block third-party cookies, Safari users explicitly deny consent to Defendant's behavioral tracking practice.

40. Moreover, Safari users were unable to opt-out of receiving advertising cookies from Defendant because no such option was available. A February 14, 2012 internet snapshot (obtained by PCWorld.com) taken of Defendant's since changed privacy policy concerning "Advertising Cookie Opt-out Plugin" reveals that Google itself led users to believe they would be immune from unwanted third-party advertising related tracking, despite not providing an opt-out plugin for Safari:

[10] Jonathan Mayer, *Safari Trackers*, http://webpolicy.org/2012/02/17/safari-trackers/

[11] A third-party cookie is an HTTP script placed on the user's computer from a domain other than the one the user is visiting, in contrast to first-party cookies, which are placed from the same domain the user has accessed.

> While we don't yet have a Safari version of the Google advertising cookie opt-out plugin, Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie.

Defendant's removal of this language, immediately after having its circumvention of Safari's privacy settings exposed, indicates knowledge of its own false promise. By this false promise, Defendant induced Plaintiff and the below proposed class to rely on the Safari browser settings to avoid being tracked, effectively discouraging them from choosing another browser with a functional opt-out function.

41. By default, Safari is set to block incoming requests from third-party domains to write cookies onto the user's internet browsing device. However, Safari does not block third-party cookies where an HTTP request to a third-party domain is caused by submission of an HTML form. In other words, Safari is intended to allow third-party cookies to be written on a user's internet browsing device when a user voluntarily fills out a webform[12] from the third-party domain and submits it. Safari also allows third-party cookies to be written when a user voluntarily clicks on a pop-up add that loads in a separate window.

42. As described *supra*, in browsers other than Safari, in the last step after a user loads a website on the Google Display Network that contains a Google ad, Google servers set a Social Cookie on DoubleClick.net that is written onto the user's internet browsing device. When a user is not logged into a Google account, the Social Cookie is written onto the user's internet browsing device from DoubleClick.net with a value of "NO_DATA" and the cookie is set to expire after 12 hours. When a user is logged in, an encryption of the user's Google account ID is written on the Social Cookie and the cookie is set to expire after 24 hours. Under Safari's default privacy settings, this request would be denied altogether, preventing the Social Cookie

[12] A "webform" is an input template that allows a user to enter data, that upon submission, is sent to the domain server for processing. http://en.wikipedia.org/wiki/Html_form.

(linked to an account ID or empty), *as well as* ordinary third-party DoubleClick.net tracking cookies, from being written onto the user's internet browsing device.

43. However, when a user is in Safari, Defendant's code is set to provide a unique response at the last step. Rather than immediately setting the Social Cookie on DoubleClick.net, Google servers respond with an HTML webform and a JavaScript to automatically submit the webform. The webform contains no content or information, is not viewable or detectable by the user, and is submitted without the action, consent, or knowledge of the user. In effect, the pseudo-webform triggers Safari (under the webform exception described in ¶ 41) to then allow *all* cookies from DoubleClick.net to be written to the user's internet browsing device and track the user's internet activity, thereby bypassing Safari's third-party cookie blocking protection. After the form is submitted, Defendant *then* makes its request to set the Social Cookie on DoubleClick.net and onto the user's internet browsing device as described *supra*.

44. The unique code written for the cookie synching mechanism in Safari could serve no other legitimate purpose; its only purpose was to bypass the cookie blocking protection of Safari and intentionally place third-party cookies on Safari users' computers.

45. Defendant's tracking of the user through the third-party cookie placed on the user's internet browsing device through the above described circumvention method is not limited to the 12 or 24 hour period of expiration set for the Social Cookies. Once Safari is triggered to allow a third-party cookie from a certain domain, it continues to allow cookies from the same third-party domain to be written onto the user's internet browsing device, because Safari is designed to allow a website domain to write additional cookies once the user has granted it initial access. Thus, if the cookie expires, or a user manually deletes it, Google and DoubleClick.net servers will freely write new cookies onto the user's device.

46. Additionally, Google ads periodically send requests to DoubleClick.net including its cookie writing script, regardless of whether the user interacts with the domain website again, visits another webpage, or takes any action at all. Nonetheless, *every time* a user visits another webpage that is part of the Google Display Network or contains DoubleClick.net ads, DoubleClick.net servers send requests to ensure a DoubleClick.net cookie is written onto the user's internet browsing device. If no such cookie is on the user's internet browsing device (e.g. the user deletes it manually) DoubleClick.net resends a cookie request.

47. Defendant knew its practices would bypass Safari's security settings and breach users' privacy. By virtue of Defendant's position in the industry as a technology and advertising giant, and given the uniqueness of the code written exclusively for Safari, which could serve no purpose other than to bypass the browser's security settings, Defendant had knowledge of the consequences stemming from that code. Defendant had adequate resources and knowledge to test its Safari code and ensure it would not cause unwanted intrusion onto Plaintiff's and the below proposed class' privacy rights. Instead, Defendant willfully ignored the consequences stemming from such code which allowed placement of tracking cookies on the Plaintiff's and the below proposed class' devices. Accordingly, Defendant purposely, intentionally or knowingly caused the intrusion of Plaintiff's and the below proposed class' privacy.

48. Defendant's circumvention of Safari's privacy settings through its cookie synching mechanism affected *all* users visiting webpages on the Google Display Network, regardless of whether they were signed into a Google account or had no Google accounts whatsoever.

49. Plaintiff and the below proposed class all visited websites subject to the cookie synching mechanism and suffered intrusions into their privacy as a result of *all* of Defendant's practices as described *supra*.

50. By virtue of choosing to use the Safari browser, Plaintiff and the below proposed class intended to block third-party tracking cookies and thus did not consent to Defendant's internet tracking, information collecting or tailored advertisements.

51. As a result of Defendant's placement of these cookies onto Plaintiff's and the proposed class' internet browsing devices, Defendant extensively tracked their internet activity without their knowledge or consent, allowing Defendant to compile data on their surfing habits, as described *supra*.

52. Defendant obtained information of great commercial value to Defendant and to vendors, which Plaintiff and the proposed class, or Defendant could sell for substantial monetary gain, e.g. via Screenwise Trends.

53. As a result of obtaining this data, Defendant was able to target personalized interest based advertisements at Plaintiff and the proposed class, which Defendant would not have otherwise been able to do without bypassing Safari's security settings.

54. By engaging in this illicit conduct, Defendant was able to produce additional clicks and impressions of its advertiser clients' adds and as a result, generate additional revenue it would not otherwise have been able to absent the illicit conduct. Defendant was also able to charge higher prices to advertisers for displaying tailored ads and unlawfully realized this additional revenue. Defendant was also able to satisfy its advertiser clients, increase its value to prospective clients, and maintain its at-will or renewable contracts with existing advertising clients because of these improperly created ads and sales leads. Accordingly, Defendant

obtained and realized an unlawful competitive advantage over competing firms in the advertising market, and at the expense of Plaintiff's and the proposed class' privacy rights.

55. Defendant deprived Plaintiff and the proposed class of the economic value they could have obtained by selling or consensually allowing collection of this information via Screenwise Trends, or otherwise.

56. Defendant intruded upon the privacy rights of Plaintiff and the Plaintiff Class, collecting information on their most intimate and personal online interactions without their knowledge or consent.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action on behalf of himself and others similarly situated pursuant to Fed. R. Civ. P. 23(b)(3). Plaintiff seeks certification of a plaintiff class ("Plaintiff Class") defined as follows:

> All individuals in the United States who (1) used Apple, Inc.'s Safari web browser, (2) left their privacy settings at the default setting or manually set privacy preferences to block cookies from third parties and advertisers, and (3) had their internet activity intercepted and tracked without their knowledge or consent by the Defendant's bypassing of said privacy settings.

This class is properly maintainable as a class action because it meets the following requirements of Fed. R. Civ. P. 23:

58. Numerosity: The class is so numerous that joinder of all members is impracticable. Apple, Inc.'s Safari browser is automatically included in every Mac computer, iPhone, iPad and iPod Touch that Apple, Inc. sells. Also, Safari is downloadable to and useable on virtually every computer, mobile phone, tablet or electronic device that provides internet access. Defendant's privacy circumvention only required users to visit a website that was part of the Google Display Network or other affiliated website with Google display ads (e.g.

Youtube.com). Defendant's Google Ads displayed on a plethora of high-traffic websites visited by Safari users every day (e.g. nytimes.com, washingtonpost.com). Defendant is in possession and control of information readily identifying the users affected. The number of users so affected is likely in the millions.

59. Commonality: Common questions of law and fact exist as to all members of the class, and predominate over any questions affecting solely individual members of the class. Such questions include:

a. Whether Defendant intentionally circumvented the privacy of class members;

b. The nature of information the Defendant obtained, or was capable of obtaining from the class members' tracked internet activity;

c. Whether Defendant obtained an unlawful competitive advantage and the amount of revenue Defendant realized pursuant thereto;

d. Whether Defendant's conduct warrants punitive damages;

e. Whether Defendant is liable under the federal and state laws upon which Plaintiff and the Plaintiff Class base their claims *infra*.

60. Typicality: Plaintiff's claims are typical of those of the class and are based on the same legal and factual theories. Defendant's cookie synching mechanism circumvented Plaintiff's and the class members' privacy settings identically, regardless of whether or not Plaintiff and the class members were members of Google+, signed into a Google account or clicked a +1 Google Ad. Defendant's non-consensually placed third-party cookies tracked substantially the same information from Plaintiff and the class members. Defendant used said obtained information for the same purpose of targeted advertising as to Plaintiff and the class members.

61. Adequacy of Representation: Plaintiff will adequately and fairly protect the interests of the class members. Plaintiff has retained counsel that is competent and experienced in class action litigation, and has the resources to zealously litigate the case to its conclusion. Plaintiff has no interest that conflicts with, or is otherwise antagonistic to the interests of class members.

62. Type(b)(3): Common questions of law or fact predominate over any questions affecting only individual members and a class action is superior to all other available methods for fairly and efficiently adjudicating this controversy. Efficient individual litigation of the class members' claims is economically impossible given the small amount of damages relative to the cost of individual litigation. Litigation of this controversy on a class basis will ensure uniformity of decision, and will foster economies of time, effort and expense.

COUNT I
Violation of the Federal Wiretap Act (18 U.S.C. § 2511)

63. Plaintiff and the Plaintiff Class hereby incorporate the foregoing paragraphs as if fully stated herein.

64. The relevant language of the Wiretap Act states as follows:

> (1) Except as otherwise specifically provided in this chapter any person who—
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

65. Defendant intentionally and willfully intercepted Plaintiffs' and the Plaintiff Class' electronic communications as described *supra*, without their knowledge or consent.

66. The cookies then tracked the internet communications Plaintiff and the Plaintiff Class made to and from other websites as described *supra*.

67. By virtue of the fact that Defendant hosted and made compatible its websites and affiliated website services on the Safari browser, Defendant agreed to be bound by the client program's technical specifications and design. Part of Safari's design was to allow its users to limit websites' access to their computers and internet browsing devices through privacy settings set to block third-party cookies. Accordingly, Defendant and its affiliated websites were not parties to *any* communications from which they were intended to be blocked under Safari's privacy settings.

68. The cookies tracked Plaintiff's and the Plaintiff Class' communications that were made to websites other than Defendant's or websites affiliated with the Defendant as Plaintiff and the Plaintiff Class traversed from website to website. Defendant and DoubleClick were supposed to be blocked under Plaintiff's and the Plaintiff Class' privacy settings and were not parties to these communications.

69. As a result of Defendant's interception of Plaintiffs' and the Plaintiff Class' electronic communications, Plaintiff and the Plaintiff Class suffered damage or loss and Defendant profited from the sale of its personalized and interest based advertising at the expense of Plaintiff's and the Plaintiff Class' privacy rights.

70. Defendant purposefully bypassed Plaintiff's and the Plaintiff Class' privacy settings in Safari in order to information concerning their internet activity for business generating purposes, all without Plaintiff's and the Plaintiff Class' consent. Defendant intercepted Plaintiff's and the Plaintiff Class' electronic communications with tortious and criminal purpose as follows:

a. Defendant intercepted Plaintiff's and the Plaintiff Class' electronic communications for the purpose of committing an invasion of privacy, intrusion upon seclusion.

b. Defendant intercepted Plaintiff's and the Plaintiff Class' communications for the purpose of violating Illinois Computer Crime Prevention Law (ICCPL), § 17-51 ("Computer tampering") as further described *infra* in Count IV.

c. Defendant intercepted Plaintiff's and the Plaintiff Class' communications for the purpose of violating the ICCPL, § 17-50 ("Computer fraud") by purposely accessing, causing to be accessed or obtaining use of data on Plaintiff's and the Plaintiff Class' internet communications devices as part of a deception to profit from collection of Plaintiff's and the Plaintiff Class' internet activity and information without their consent.

d. Defendant intercepted Plaintiff's and the Plaintiff Class' communications for the purpose of violating the Federal Computer Fraud and Abuse Act 18 U.S.C. § 1030 as further described *infra* in Count II.

e. Defendant intercepted Plaintiff's and the Plaintiff Class' communications for the purpose of violating the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.* as described *infra* in Count V.

COUNT II
Violation of the Federal Computer Fraud and Abuse Act (18 U.S.C. § 1030)

71. Plaintiff and the Plaintiff Class hereby incorporate the foregoing paragraphs as if fully stated herein.

72. Defendant intentionally accessed Plaintiff's and the Plaintiff Class' internet browsing devices without authorization and in excess of authorization as described *supra*.

73. (2)(c): Defendant obtained information from protected computers. Plaintiffs' and the Plaintiff Class' internet browsing devices are "protected computers" within the meaning of 18 U.S.C. § 1030(c)(2)(B) because they are "used in or affecting interstate or foreign commerce or communication." Plaintiff's and the Plaintiff Class' internet browsing devices are used to purchase items online from various states throughout the United States, as well as to communicate with individuals, vendors and websites all over the United States and world. By installing third-party tracking cookies without Plaintiff's and the Plaintiff Class' authorization, Defendant obtained information, *inter alia*, concerning Plaintiff's and the Plaintiff Class' internet activity.

74. Defendant knowingly caused the transmission of a program, information, code or command, through implantation of tracking cookies onto Plaintiff's and the Plaintiff Class' internet browsing devices. By implantation of such cookies, Defendant intentionally caused damage, without authorization, to Plaintiff's and the Plaintiff Class' internet browsing devices.

75. Defendant's above described actions caused damage to Plaintiff's and the Plaintiff Class' internet browsing devices through the impairment of the integrity of data or information pertaining to their web surfing activity, personal or private information, and any other data that was obtained or used as a result of Defendant's breach of security. Additionally, the monetary value of Plaintiff's and the Plaintiff Class' information was taken or diminished as a result of Defendant's unlawfully obtaining it.

76. Defendant's above described conduct caused damage or loss without authorization to the Plaintiff and the Plaintiff Class in excess of $5,000 over a one-year period, as described *supra*.

COUNT III
Violation of the Stored Electronic Communications Act (18 U.S.C. § 2701)

77. Plaintiff and the Plaintiff Class hereby incorporate the foregoing paragraphs as if fully stated herein.

78. Defendant, without authorization or by exceeding authorization, intentionally placed tracking cookies onto Plaintiff's and the Plaintiff Class' internet browsing devices.

79. Through implantation of cookies on Plaintiff's and the Plaintiff Class' internet browsing devices, Defendants accessed data concerning Plaintiff's and the Plaintiff Class' internet activity, as such data passed through the Random Access Memory (RAM)[13] on Plaintiff's and the Plaintiff Class' internet browsing devices, or otherwise.

80. Defendant thereby obtained access to Plaintiff's and the Plaintiff Class' internet communications while they remained in electronic storage on their internet browsing devices.

81. Defendant accessed electronic communications of Plaintiff and the Plaintiff Class which were not electronic communications originating from the Defendant, or intended to be communicated to the Defendant. Plaintiff's and the Plaintiff Class' communications, e.g. input of URLs, were to webservers not belonging to Defendant, i.e., not to DoubleClick.net, Google.com, etc.

82. Defendant was not a provider of the electronic communications service through which it accessed Plaintiff's and the Plaintiff Class' communications.

83. The cookies implanted by Defendant were of temporary nature and were set to expire after a specified period of time, depending on the user's Google login status.

84. Plaintiff's and Plaintiff Class' internet browsing devices are a "facilities" through which electronic communication service was provided, and through which Defendant accessed Plaintiff's and the Plaintiff Class' electronic communications.

[13] RAM is used to temporarily read, write and store data on a computing device for access and processing from the central processing unit (CPU).

85. Plaintiff and the Plaintiff Class suffered damage or loss as a result of Defendant's practices as describe *supra*.

COUNT IV
Violation of Illinois Computer Crime Prevention Law, § 17-51(a)(4)

86. Plaintiff and the Plaintiff Class hereby incorporate the foregoing paragraphs as if fully stated herein.

87. The Defendant knowingly and without authorization or in excess of authorization from Plaintiff and the Plaintiff Class, inserted a program onto Plaintiff's and the Plaintiff Class' computers knowing or having reason to know said program would alter, delete or remove data from that computer.

88. The Defendant knowingly and without authorization or in excess of authorization from Plaintiff and the Plaintiff Class inserted a program onto Plaintiff's and the Plaintiff Class' computers knowing or having reason to know said program would cause loss to Plaintiff and the Plaintiff Class.

89. Plaintiff and the Plaintiff Class suffered loss as a result of Defendant's practices as describe *supra*, e.g. by depriving them of the economic value of information concerning their internet activity at the expense of their privacy rights.

COUNT V
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act 815, ILCS 505/1, *et seq.*

90. Plaintiff and the Plaintiff Class hereby incorporate the foregoing paragraphs as if fully stated herein.

91. Defendant engaged in deceptive practices through fraud, deception, false pretense, false promise, misrepresentation or the concealment, suppression or omission of materials facts. As stated *supra*, Defendant explicitly mislead Plaintiff and the Plaintiff Class by stating in its

privacy policy that Safari users, although unable to opt-out of tracking cookies, would be immune from such tracking cookies under Safari's default privacy settings blocking third-party cookies. Plaintiff and the Plaintiff Class thus had a reasonable expectation their privacy would not be violated by tracking cookies. Contrary to this assertion, Defendant included unique code specifically designed to surpass those exact privacy settings in Safari. Defendant intended Plaintiff and the Plaintiff Class to rely on this representation, thereby encouraging them to continue using Safari rather than another internet browser with a functional opt-out option.

92. Defendant's acts constitute unfair practices because they offend public policy on several levels. For instance, Defendant's acts constitute a violation of several statutes, as alleged in the various counts of this complaint. Moreover, Defendant's acts violate the terms of its consent decree with the FTC as described in ¶ 13 and also violate the FTC's recommendation to include "Do Not Track" mechanisms for users to opt out of online behavioral tracking.[14]

93. Additionally, Defendant's acts are unethical, immoral, oppressive or unscrupulous as directed toward Plaintiff and the Plaintiff Class. Plaintiff and the Plaintiff Class were unable to invoke an effective alternative to avoid having information concerning their internet activity tracked and collected because Defendant concealed its practices, mislead Plaintiff and the Plaintiff Class about its practices, and thus deprived Plaintiff and the Plaintiff Class of knowledge of such practices.

94. Defendant's practices caused substantial injury to Plaintiff and the Plaintiff Class, from which Plaintiff and the Plaintiff Class received no benefit, and which injury Plaintiff and the Plaintiff Class could not have reasonably avoided, as described *supra* at ¶ 93. Defendant's practices caused injury to millions of users, multiple times per day; virtually every time a user browsed the internet on Safari.

[14] http://www.ftc.gov/os/testimony/110714internetprivacytestimony.pdf

95. As a result of Defendant's conduct, Plaintiff and the Plaintiff Class suffered actual economic damages as described *supra*, e.g. through deprivation of the economic value of information concerning their internet activity. Had Plaintiff and the Plaintiff Class been informed of this practice, they could have either used another browser, or signed up for Screenwise Trends to receive compensation for their information.

COUNT VI
Breach of Contract

96. Plaintiff and the Plaintiff Class hereby incorporate the foregoing paragraphs as if fully stated herein.

97. Defendant maintained a contract with Plaintiff and the Plaintiff Class in the form of Defendant's privacy policy. For instance, as noted *supra*, Defendant's cookie opt-out policy promised to Plaintiff and the Plaintiff Class that Safari's privacy settings for blocking cookies would have the same effect as opting out of Defendant's tracking cookies.

98. Plaintiff and the Plaintiff Class abided by their responsibilities under the privacy policy.

99. Defendant breached said contract by intentionally bypassing Safari's privacy settings and implanting tracking cookies on Plaintiff's and the Plaintiff Class' internet browsing devices, in direct contravention to the promise made by Defendant.

100. As a result of Defendant's breach, Plaintiff and the Plaintiff Class had their personal information and internet activity unlawfully tracked and obtained, and sustained resulting damages as described *supra*.

COUNT VII
Unjust Enrichment

101. Plaintiff and the Plaintiff Class hereby incorporate the foregoing paragraphs as if fully stated herein.

102. As a result of Defendant's practices, Defendant received additional revenue and economic benefits through sale of behaviorally targeted ads it would not have been able to sell without intruding upon the privacy rights of Plaintiff and the Plaintiff Class.

103. Defendant was so enriched at the expense of Plaintiff's and the Plaintiff Class' privacy rights.

104. Defendant could not have been so enriched without impoverishing Plaintiff's and the Plaintiff Class' privacy rights and depriving them of the economic value of information concerning their internet activity.

105. Defendant lacked justification for its practices and lacked Plaintiff's and the Plaintiff Class' consent.

106. Plaintiffs and the Plaintiff Class have no other adequate remedy at law.

WHEREFORE, Plaintiff and the Plaintiff Class request the following relief:

A. An order certifying that this action may be maintained as a class action pursuant Fed. R. Civ. P. 23(b)(3) and appointment of Plaintiff and his counsel to represent the Plaintiff Class;

B. Compensatory damages incurred by Plaintiff and the Plaintiff Class;

C. Restitution or disgorgement of profits, in the amount of revenue by which Defendant was unjustly enriched through its unlawful conduct;

D. Injunctive relief permanently restraining Defendant from bypassing Plaintiff's and the Plaintiff Class' privacy protections to place tracking cookies on their internet browsing devices without their consent;

E. Requiring Defendant to delete all PII and non-PII collected from Plaintiff and the Plaintiff Class without their consent;

F. Statutory damages of $100 a day for each day of violation of the Wiretap Act for Plaintiff and the Plaintiff Class pursuant to 18 U.S.C. § 2520(c)(2)(B);

G. Damages constituting Plaintiff's and the Plaintiff Class' actual damages and total revenues realized by Defendant resulting from its violation of the Wiretap Act pursuant to 18 U.S.C. § 2520(c)(2)(A);

H. Punitive damages for Defendant's wanton, reckless, or malicious conduct;

I. Reasonable attorney's fees and court costs incurred in connection with this act; and

J. Any other relief the court deems equitable and just.

Dated: April 19, 2012

Respectfully Submitted,

/s/ Clinton A. Krislov
Attorney for Plaintiff

Clinton A. Krislov
KRISLOV & ASSOCIATES, LTD.
20 North Wacker Dr., Ste. 1350
Chicago, IL 60606
Tel: (312) 606-0500
Fax: (312) 606-0207
Firm Number: 21169

Mark Baiocchi
LAW OFFICES OF MARK BAIOCCHI
1755 S. Naperville Road, Suite 100
Wheaton, IL 60187
Tel: (630) 983-4200
Fax: (630) 983-4223