KASSRA P. NASSIRI (215405)
(knassiri@nassiri-jung.com)
CHARLES H. JUNG (217909)
(cjung@nassiri-jung.com)
NASSIRI & JUNG LLP
47 Kearny Street, Suite 700
San Francisco, California 94108
Telephone: (415) 762-3100
Facsimile: (415) 534-3200

MICHAEL J. ASCHENBRENER
(maschenbrener@edelson.com)
BRADLEY M. BAGLIEN
(bbaglien@edelson.com)
EDELSON MCGUIRE LLP
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370
Facsimile: (312) 589-6378

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

PALOMA GAOS, an individual, on behalf of herself and all others similarly situated,

Plaintiff,

v.

GOOGLE INC., a Delaware corporation,

Defendant.

Case No. 10-CV-04809-EJD

CLASS ACTION

FIRST AMENDED COMPLAINT

ACTION FILED: 10/25/10

JURY TRIAL DEMANDED

Plaintiff Paloma Gaos brings this suit on behalf of herself and all others similarly situated, and makes the following allegations on information and belief, except as to allegations pertaining to Plaintiff, which are based on her personal knowledge:

I. INTRODUCTION

1. Plaintiff brings this class action complaint against Google Inc. ("Google") for intentionally, systematically and repeatedly divulging its users' search queries to third parties. This practice adversely impacts billions of searches conducted by millions of consumers. Plaintiff's

claims arise under the Stored Communications Act, 18 U.S.C. § 2702, Cal. Civ. Code § 1572, and common law.

2. Google, the largest search engine in the United States, has repeatedly touted the numerous ways in which it protects user privacy, particularly with regard to the terms that consumers search for using the company's search engine. Over protests from privacy advocates, however, Google has consistently and intentionally designed its services to ensure that user search queries, which often contain highly-sensitive and personally-identifiable information ("PII"), are routinely transferred to marketers, data brokers, and sold and resold to countless other third parties.

3. The user search queries disclosed to third parties contain, without limitation, users' real names, street addresses, phone numbers, credit card numbers, social security numbers, financial account numbers and more, all of which increases the risk of identity theft. User search queries also contain highly-personal and sensitive issues, such as confidential medical information, racial or ethnic origins, political or religious beliefs or sexuality, which are often tied to the user's personal information.

4. In many instances, the information contained in disclosed search queries does not directly identify the Google user. Through the reidentification (explained below) or deanonymizing of data, however, the information contained in search queries can and, on information and belief, are associated with the actual names of Google users. Computer science academics and privacy experts are calling for the reexamination of privacy concerns in light of the growing practice and power of reidentification.

5. Google has acknowledged that search query information alone may reveal sensitive PII. And Google has demonstrated that it could easily stop disclosing search query information to third parties, without disrupting the effectiveness of its service to its users, if it wished to do so. But because the real-time transmission of user search queries increases Google's profitability, it chooses not to utilize the demonstrated technology that would prevent the disclosure of its users' PII.

II. PARTIES

6. Plaintiff Paloma Gaos is a resident of San Francisco County, California. Plaintiff has at all material times been a user of Google's search engine services.

7. Defendant Google Inc. ("Google") is a Delaware corporation that maintains its headquarters in Mountain View, California. Google conducts business throughout California and the nation.

III. JURISDICTION AND VENUE

8. This Court has personal jurisdiction over Google because (a) a substantial portion of the wrongdoing alleged in this complaint took place in this state, (b) Google is authorized to do business here, has sufficient minimum contacts with this state, and/or otherwise intentionally avails itself of the markets in this state through the promotion, marketing and sale of products and services in this state, to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, 18 U.S.C. § 2702 and 18 U.S.C. § 2707. This Court has supplemental jurisdiction over the California state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper in this District under 28 U.S.C. § 1391(b) and (c). A substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District.

IV. INTRADISTRICT ASSIGNMENT

11. Pursuant to Civil Local Rule 3-2(e), this case shall be assigned to the San Francisco Division or Oakland Division.

V. STATEMENT OF FACTS

A. Google's Search Business

1. Google's Dominance in Search

12. "Searching" is one of the most basic activities performed in the Internet. Most everyone with access to the Internet uses search engines to find information on the Internet. When using a search engine, users formulate a search query using keywords and phrases reflecting the information sought by the user. The search engine then matches the search query with websites matching the query and provides a list of those matching websites to the user. The user clicks on the link in the resulting list and is redirected to the website containing the sought-after information.

13. Google's core service centers on its proprietary search engine. Google runs millions of servers in data centers around the world and processes over one billions user-generated search requests every day. On information and belief, Google is the most-used search engine in the world and enjoys a market share of over 50% in the United States.

14. Google generates substantial profits from selling advertising. The revenue it generates is derived from offering search technology and from the related sale of advertising displayed on its site and on other sites across the web. On information and belief, over 99% of Google's revenue is derived from its advertising programs, with total advertising revenues estimated at $28 billion in 2010. Google has implemented various innovations in the online advertising market that helped make it one of the biggest advertisers in the world.

15. Google AdWords is Google's main advertising product and source of advertising revenue. The AdWords program allows advertisers to select a list of words that, when entered by users in a search query, trigger their targeted ads. When a user includes words that match an advertiser's selections within a search query, paid advertisements are shown as "sponsored links" on the right side of the search results screen. Accordingly, much of Google's advertising revenue depends directly on the search queries that its users run on Google search.

16. Using technology from its wholly-owned subsidiary DoubleClick, Google can also determine user interests and target advertisements so they are relevant to their context and the user that is viewing them. Google's Analytics product allows website owners to track where and how people use their website, allowing in-depth research to get users to go where you want them to go.

17. Third-party search engine optimization ("SEO") companies help businesses design their websites so that users conducting internet search using search engines like Google get search results containing their business at or near the top of the search results page. SEOs accomplish this task by ensuring that a business's relevant pages are designed to work with Google's search algorithms. Google has a symbiotic relationship with SEOs. Google wants relevant results at the top of their search results page, and SEOs want their customers' relevant webpages to appear at the top of Google's search results. To the extent that SEOs are successful in getting their clients' relevant pages to appear at or near the top of Google's search results page, users are more likely to return to

Google next time they want to search for information on the internet. And the more people use Google for search, the more revenue Google derives from its advertising business.

2. Google's Privacy Promises

18. Leading thinkers in the privacy community have long argued that consumers "treat the search [engine] box like their most trusted advisors. They tell the Google search box what they wouldn't tell their own mother, spouse, shrink or priest."[1] Peer reviewed academic studies confirm this fact, particularly regarding the use of search engines to look up sensitive health information.[2]

19. Google has always recognized that user trust is paramount to its search business success. To that end, Google adopted "Don't be evil" as its motto, and Google states that its Code of Conduct is one of the ways it puts that motto into practice.[3] Google's Code of Conduct recognizes that it is "asking users to trust [it] with their personal information. Preserving that trust requires that each of us respect and protect the privacy of that information. Our security procedures strictly limit access to and use of users' personal information."[4]

20. Because Google's success depends on gaining the trust of its users, Google's Privacy Policy sets forth representations intended to foster the safety and privacy protection offered by Google's search services. As of October 14, 2005, Google's Privacy Policy[5] stated as follows:

> Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:
>
> - We have your consent. We require opt-in consent for the sharing of any sensitive personal information.

---

[1] Christopher Ketchum & Travis Kelly, The Cloud Panopticon (April 9, 2010), http://www.theinvestigativefund.org/investigations/rightsliberties/1274/the_cloud_panopticon (last visited October 24, 2010).

[2] Gunther Eysenbach and Christian Köhler, *How do consumers search for and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews*, BMJ 2002; 324:573, *available at* http://www.bmj.com/cgi/content/full/324/7337/573.

[3] Google's Code of Conduct, http://investor.google.com/corporate/code-of-conduct.html (last visited October 24, 2010).

[4] *Id.*

[5] Google's October 14, 2005 Privacy Policy, http://www.google.com/intl/en/privacy_archive_2005.html (last visited October 24, 2010).

- We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Policy and any other appropriate confidentiality and security measures.
- We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law.

21. Google defines "Personal information" as "information that [the user] provide[s] to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google" and "Sensitive Information" as "information we know to be related to confidential medical information, racial or ethnic origins, political or religious beliefs or sexuality and tied to personal information.[6]

22. Google also stated in its October 14, 2005 Privacy Policy that "We may share with third parties certain pieces of *aggregated, non-personal information*, such as the number of users who searched for a particular term, for example, or how many users clicked on a particular advertisement. Such information does not identify you individually."[7] Google defined "aggregated, non-personal information" as "information that is recorded about users and *collected into groups* so that it no longer reflects or references an individually identifiable user."[8]

23. Google's privacy policy was unchanged until October 3, 2010, when it was revised to exclude any statement about how Google shares search queries with third parties. The representations that Google shares information only in "limited circumstances" remained unchanged.

24. Google makes similar representations about the privacy of its users' search queries on its video "Privacy Channel" on YouTube. The first video that plays when a user visits the Privacy

[6] Google Privacy Center, FAQ, http://www.google.com/intl/en/privacy_faq.html (last visited October 24, 2010).

[7] Google's October 14, 2005 Privacy Policy, *supra*, n.5 (emphasis supplied).

[8] Google's October 14, 2005 Privacy FAQs, http://web.archive.org/web/20070113102317/www.google.com/intl/en/privacy_faq.html (last visited October 24, 2010) (emphasis supplied).

Channel starts with the statement "at Google, we make privacy a priority in everything we do."[9] Google also states in another privacy video that "We don't sell user information to other companies."[10]

25. Earlier this year, Google reiterated its commitment to user privacy to the Federal Trade Commission. In a letter to the FTC, Google wrote that it "supports the passage of a comprehensive federal privacy law that … build[s] consumer trust … enact[s] penalties to deter bad behavior ... include[s] uniform data safeguarding standards, data breach notification procedures, and stronger procedural protections relating to third party access to individuals' information."[11] Google also wrote that it "acts every day to promote and expand free expression online and increase global access to information. As new technology empowers individuals with more robust free expression tools and greater access to information, we believe that governments, companies, and individuals must work together to protect the right to online free expression. Strong privacy protections must be crafted with attention to the critical role privacy plays in free expression. The ability to access information anonymously or pseudonymously online has enabled people around the world to view and create controversial content without fear of censorship or retribution by repressive regimes or disapproving neighbors … If all online behavior were traced to an authenticated identity, the free expression afforded by anonymous web surfing would be jeopardized."[12]

3. Google Admits Search Queries Contain Sensitive, Personal Data

26. In 2006, the Department of Justice sought to compel Google to produce thousands of users' individual search queries.[13] As set forth in the Government's subpoena, it sought only "anonymized" data, namely, the text of the search string entered by Google users, and not "any additional information that may be associated with such a text string that would identify the person

[9] Google's Privacy Principles, http://www.youtube.com/watch?v=5fvL3mNt1g (January 26, 2010) (last visited October 25, 2010).

[10] Google's Privacy Principles, http://googleblog.blogspot.com/2010/01/googles-privacy-principles.html at 1:44 (January 27, 2010, 7:00 p.m.) (last visited October 23, 2010).

[11] Google's April 14, 2010 letter to Donald S. Clark, http://www.scribd.com/doc/30196432/FTC-Roundtable-Comments-Final (last visited October 24, 2010).

[12] *Id.*

[13] *Gonzales v. Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW).

who entered the text string into the search engine, or the computer from which the text string was entered."[14]

27. To its credit, Google fought the government's request. In a declaration submitted to the court describing the kind of personal information that can end up in the company's search query logs, Matt Cutts, a Senior Staff Engineer who specializes in search optimization issues at Google, stated as follows:[15]

> • Google does not publicly disclose the searches [sic] queries entered into its search engine. If users believe that the text of their search queries could become public knowledge, they may be less likely to use the search engine for fear of disclosure of their sensitive or private searches for information or websites.
>
> • There are ways in which a search query alone may reveal personally identifying information. For example, many internet users have experienced the mistake of trying to copy-and-paste text into the search query box, only to find that they have pasted something that they did not intended. Because Google allows very long queries, it is possible that a user may paste a fragment of an email or a document that would tie the query to a specific person. Users could also enter information such as a credit card, a social security number, an unlisted phone number or some other information that can only be tied to one person. Some people search for their credit card or social security number deliberately in order to check for identity theft or to see if any of their personal information is findable on the Web.

28. Similarly, in its Opposition to the Government's Motion to Compel the disclosure of Google users' search queries, the company argued that:

> • Google users trust that when they enter a search query into a Google search box, not only will they receive back the most relevant results, but that Google will keep private whatever information users communicate absent a compelling reason.[16]
>
> • The privacy and anonymity of the service are major factors in the attraction of users – that is, users trust Google to do right by their personal information and to provide them with the best search results. If users believe that the text of their search queries into Google's search engine may become public

[14] *Id*. at 682.

[15] Declaration of Matt Cutts at 9, *Gonzales v. Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW).

[16] Google's Opposition to the Government's Motion to Compel at 1, *supra*, n.12.

knowledge, it only logically follows that they will be less likely to use the service.[17]

- This is no minor fear because search query content can disclose identities and personally identifiable information such as user-initiated searches for their own social security or credit card numbers, or their mistakenly pasted but revealing text."[18]

29. In its order[19] denying the Government's request to discover Google users' search queries, the Court shared Google's concern that disclosing search queries would raise serious privacy issues:

> The Government contends that there are no privacy issues raised by its request for the text of search queries because the mere text of the queries would not yield identifiable information. Although the Government has only requested the text strings entered … basic identifiable information may be found in the text strings when users search for personal information such as their social security numbers or credit card numbers through Google in order to determine whether such information is available on the Internet. The Court is also aware of so-called 'vanity searches,' where a user queries his or her own name perhaps with other information. Google's capacity to handle long complex search strings may prompt users to engage in such searches on Google. Thus, while a user's search query reading '[username] stanford glee club' may not raise serious privacy concerns, a user's search for '[user name] third trimester abortion san jose,' may raise certain privacy issues as of yet unaddressed by the parties' papers. This concern, combined with the prevalence of Internet searches for sexually explicit material — generally not information that anyone wishes to reveal publicly — gives this Court pause as to whether the search queries themselves may constitute potentially sensitive information.

30. Google's awareness of the privacy concerns surrounding search queries was also demonstrated in response to a massive disclosure of user search queries by AOL. In August 2006, AOL released an "anonymized" dataset of 20 million search queries conducted by 658,000 AOL users over a three-month period.[20] That data included search queries revealing names, addresses, local landmarks, medical ailments, credit card numbers and social security numbers.[21]

---

[17] *Id*. at 18.

[18] *Id*.

[19] *Gonzales*, 234 F.R.D. at 687.

[20] Complaint at ¶ 16, *Doe 1 v. AOL LLC*, 2010 WL 2524494 (N.D. Cal. June 23, 2010) (No. C-06-5866-SBA).

[21] *Id* at ¶ 18.

31. In an article about the incident, the *New York Times* wrote that the AOL dataset "underscored how much people unintentionally reveal about themselves when they use search engines," and referred to search queries about "depression and medical leave," "fear that spouse contemplates cheating," "child porno," and "how to kill oneself by natural gas."[22]

32. Even more surprising, however, was that the *New York Times* journalists were able to reidentify individual "anonymized" AOL search users due to the vanity searches they had conducted, and then link other, non-vanity search queries in the dataset to those individuals through the cross-session identifiers (cookies) included in the dataset.[23] One AOL user who was reidentified said she was shocked to learn that AOL had published her search queries: "My goodness, it's my whole personal life. I had no idea somebody was looking over my shoulder."[24]

33. An AOL spokesman, Andrew Weinstein, apologized on behalf of AOL and said he wasn't surprised that the *New York Times* was able to connect the dots and reidentify "anonymous" users in the dataset: "We acknowledged that there was information that could potentially lead to people being identified…"[25]

34. Soon after the release of the search query data by AOL, Google CEO Eric Schmidt spoke about the AOL privacy breach. He called AOL's release of user search data "a terrible thing" and reassured Google users that their search queries were safe and private:

> Well, [this sort of privacy breach is] obviously a terrible thing. And the data as released was obviously not anonymized enough, and maybe it wasn't such a good idea to release it in the first place. Speaking for Google, we exist by virtue of the trust of our end users. So if we were to make a mistake to release private information that could be used against somebody, especially if it could be used against them in a way that could really hurt them in a physical way or something like that, it would be a terrible thing. We have lots and lots of systems in the company to prevent that.
>
> It's funny that we talk about the company being more transparent. But there are many things inside our company that are important that we don't share with everyone, starting with everyone's queries and all the information that that implies. I've always

[22] Michael Barbaro and Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, August 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html.

[23] *Id*.

[24] *Id.*

[25] *Id*.

> worried that the query stream was a fertile ground for governments to randomly snoop on people [for example]. We had a case where we were only a secondary party, where the government gave us a subpoena, which was in our view, over-broad. And this over-broad subpoena we fought in federal court – one of the great things about the American system is that you can actually have a judge make an impartial decision. And the judge ruled largely in our favor. So that's an example of how strongly we take this point.[26]

4. A Brief Primer on "Referrer Headers"

35. Software engineers are generally familiar with the risk of Referrer Header "leakage" of information companies intended to keep confidential and/or are obliged to keep confidential.

36. The HTTP Referrer function is a standard web browser function, provided by standard web browsers since the HTTP 1.0 specification in May 1996.[27] When an internet user visits a web page using their computer or mobile device, every major web browser (*e.g.*, Internet Explorer, Firefox, Chrome, Safari) by default reports the last page that the user viewed before clicking on a link and visiting the current page — that is, the page that "referred" them to the current page. This information is transmitted in the HTTP Referrer Header.

37. The current version of the publicly-available HTTP specification, RFC 2616,[28] provides for HTTP Referrer Headers in its provision 14.36.[29] It is well known that if a site places confidential information, such as a username, in a URL, then the site risks releasing this information whenever a user clicks a link to leave the site. Indeed, the HTTP specification specifically flags this risk; in section 15.1.3, the HTTP specification advises developers of substantially the same problem: "Authors of services which use the HTTP protocol SHOULD NOT use GET based forms for the submission of sensitive data, because this will cause this data to be encoded in the REQUEST-URI."[30]

38. While the HTTP Referrer function is a standard web browser function, Google ultimately determines whether to send referrer header information to third parties and exercises

---

[26] Conversation with Eric Schmidt hosted by Danny Sullivan, http://www.google.com/press/podium/ses2006.html (last visited October 24, 2010).

[27] http://www.w3.org/Protocols/rfc1945/rfc1945

[28] http://www.w3.org/Protocols/rfc2616/rfc2616.html

[29] http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.36

[30] http://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html#sec15.1.3

control over the content of the URL that is referred by this function to the owner of the destination web page.

5. Google Transmits Individual User Search Queries to Third Parties

39. Since the service's launch, and continuing to this day, Google's search engine has included its users' search terms in the URL of the search results page. Thus, for example, a search for "abortion clinics in Indianapolis" would return a page with a URL similar to "http://www.google.com/search?q=abortion+clinics+in+Indianapolis."

40. Because the search terms are included in the search results URL, when a Google user clicks on a link from Google's search results page, the owner of the website that the user clicks on will receive from Google the user's search terms in the Referrer Header.

41. Several web analytics services, including SEOs, include and use functionality to automatically parse the search query information from web server logs, or to otherwise collect the search query from the referrer header transmitted by each visitor's web browser. Google's own analytics products provide webmasters with this information at an aggregate level (*e.g.*, revealing how many visitors were drawn by particular search terms).

6. Google's Transmission of User Search Queries is Intentional

42. Because Google's financial success depends on, among other things, the symbiotic relationship it shares with SEOs and the ability for third parties to engage in web analytics, Google has placed a high priority on revealing individual user search queries to third parties. Notwithstanding its repeated representations to the contrary in its Privacy Policy and to privacy regulators, Google continues to this day to transmit user search queries.

43. Neither Google's search technology nor the nature of the Internet compels Google to divulge user search queries. Google could easily cease transmission of user search queries to third parties, but chooses not to.

44. On September 6, 2010, a former FTC employee, Christopher Soghoian, filed a complaint with the FTC accusing Google of not adequately protecting the privacy of consumers' search queries. Much of the following information comes from Mr. Soghoian's complaint.[31]

45. Starting approximately in November 2008, Google began to test a new method of delivering search results that uses advanced AJAX (Asynchronous JavaScript and XML) technologies.[32] AJAX is one of the key pillars of the Web 2.0 experience.[33] This pilot was initially deployed in the Netherlands,[34] but in subsequent months, was observed by users in other countries.

46. One of the side effects of the AJAX search page is that the URL of the search results page includes the search query terms after a # symbol in the URL. Thus, on an AJAX enabled search page, the URL listed at the top of the page will be similar to:

http://www.google.com/#hl=en&source=hp&q=drug+addiction

47. The addition of the # symbol had a significantly positive, albeit unintentional impact upon Google user privacy. This is because web browsers do not pass on any information after the # symbol in the referrer header. Thus, using the previous example of a search for the query "drug addiction," if a user clicked on the first result, the owner of that web site would only receive "http://www.google.com/" in the referrer header, rather than the search terms that follow the # symbol.

48. This change was immediately noticed by the webmaster and SEO community, who complained to Google:

---

[31] *In the Matter of Google, Inc.*, FTC Complaint, *available at* http://online.wsj.com/public/resources/documents/FTCcomplaint100710.pdf.

[32] Jesse James Garrett, Ajax: A New Approach to Web Applications (February 18, 2005), http://www.adaptivepath.com/ideas/essays/archives/000385.php ("Ajax isn't a technology. It's really several technologies, each flourishing in its own right, coming together in powerful new ways").

[33] Tim O'Reilly, What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software (September 30, 2005), http://oreilly.com/web2/archive/what-is-web-20.html ("AJAX is also a key component of Web 2.0 applications such as Flickr, now part of Yahoo!, 37signals' applications basecamp and backpack, as well as other Google applications such as Gmail and Orkut.")

[34] Ulco, "Google Search in AJAX?!" (November 19, 2008), http://www.ulco.nl/gibberish/google-search-in-ajax.

- "I'm seeing hundreds of these empty google referrers today and wondered what was going on."[35]

- "This means organic searches from Google will now show up as just http://www.google.com/, with no search parameters. In other words, no analytics app can track these searches anymore. I started noticing lots of hits from just 'http://www.google.com/' recently in our own search logs. I thought maybe it was just a bug with *Clicky*. But then one of our users contacted me about this article, and my jaw about broke from hitting the floor so hard."[36]

- "What actually *breaks* if Google makes this switchover, and is in fact broken during any testing they are doing, is much more widespread. Every single analytics package that currently exists, at least as far as being able to track what keywords were searched on to find your site in Google, would no longer function correctly."[37]

49. Responding to complaints from the webmaster community, Google quickly issued a public statement:

> Currently AJAX results are just a test on Google. At this time only a small percentage of users will see this experiment**. It is not our intention to disrupt referrer tracking**, and we are continuing to iterate on this project and are **actively working towards a solution**. As we continue experiments, we hope that this test may ultimately provide an easier solution for our customers and a faster experience for our users.[38]

50. Google soon ended the test of the AJAX search results page, a fact confirmed by Google Senior Engineer Matt Cutts, who specializes in search optimization issues at Google:

> [T]he team didn't think about the referrer aspect. So they stopped [the test]. They've paused it until they can find out how to keep the referrers.[39]

---

[35] Posting of sorabji.com to Clicky.blog, http://getclicky.com/blog/150/googles-new-ajax-powered-search-results-breaks-search-keyword-tracking-for-everyone (February 03 2009, 1:05 p.m.).

[36] Clicky.blog, http://getclicky.com/blog/150/googles-new-ajax-powered-search-results-breaks-search-keyword-tracking-for-everyone (February 03, 2009, 9:50 a.m.).

[37] Posting of Michael VanDeMar to Smackdown!, What Will *Really* Break If Google Switches To AJAX…?, http://smackdown.blogsblogsblogs.com/2009/02/02/what-will-really-break-if-google-switches-to-ajax/ (February 2, 2009, 11:26 a.m.).

[38] Posting of Matt McGee to Search Engine Land, Google AJAX Search Results = Death To Search Term Tracking?, http://searchengineland.com/google-ajax-search-results-death-to-search-term-tracking-16431 (February 3, 2009, 5:41 p.m.) (emphasis supplied).

[39] Posting of Lisa Barone to Outspoken Media, Keynote Address – Matt Cutts, Google, http://outspokenmedia.com/internet-marketing-conferences/pubcon-keynote-matt-cutts/ (March 12, 2009).

51. In March 2009, Google again began to test technology that unintentionally caused the users' search terms to be stripped from the referrer header transmitted to web sites. The following is an example of the format of the new URL that was being tested in March 2009:

> http://www.google.com/url?q=http**://www.webmd.com**&ei=in66ScnjBtKgtwfn0LTiDw&sa=X&oi=smap&resnum=1&ct=result&cd=1&usg=AFQjCNF9RdVC6vXBFOYvdia1s_ZE_BMu8g

52. Michael VanDeMar, a prominent member of the SEO community noticed that he was again seeing AJAX based search results in addition to redirected URLs for every link in the search results page:

> Occasionally you will see these Google redirects in the normal [search engine results pages] as well, although usually not. The thing is, I was seeing them on every search I performed. It struck me as odd, until I suddenly realized that every search was being done via AJAX.[40]

53. Google's Matt Cutts soon responded to VanDeMar by leaving a comment on his blog:

> Hi Michael, I checked with some folks at Google about this. The redirection through a url redirector was separate from any AJAX-enhanced search results; we do that url redirection for some experiments, but it's not related to the JavaScript-enhanced [AJAX] search results.
>
> **The solution to the referrer problem will be coming online in the future. It uses a JavaScript-driven redirect that enables us to pass the redirect URL as the referrer. This URL will contain a 'q' param that matches the user's query.**[41]

54. On April 14, 2009, Google announced that it would be deploying the URL redirection tool for all links in the search results. The company described the details in a blog post to the webmaster community:

> Starting this week, you may start seeing a new referring URL format for visitors coming from Google search result pages. Up to now, the usual referrer for clicks on search results for the term "flowers", for example, would be something like this:

---

[40] Posting of Michael VanDeMar to Smackdown!, Google Re-initiates Testing of AJAX SERP's With Faulty Proposed Fix, http://smackdown.blogsblogsblogs.com/2009/03/13/google-re-initiates-testing-of-ajax-serps-with-faulty-proposed-fix/ (March 13, 2009, 11:14 a.m.).

[41] Posting of Matt Cutts to Smackdown!, *supra*, n.39, http://smackdown.blogsblogsblogs.com/2009/03/13/google-re-initiates-testing-of-ajax-serps-with-faulty-proposed-fix/ (March 17, 2009, 10:10 a.m.) (emphasis supplied).

> http://www.google.com/search?hl=en&q=**flowers**&btnG=Google+Search
>
> Now you will start seeing some referrer strings that look like this:
>
> http://www.google.com/url?sa=t&source=web&ct=res&cd=7&url=http%3A%2F%**2Fwww.example.com**%2Fmypage.htm&ei=0SjdSa-1N5O8M_qW8dQN&rct=j&q=**flowers**&usg=AFQjCNHJXSUh7Vw7oubPaO3tZOzz-F-u_w&sig2=X8uCFh6IoPtnwmvGMULQfw
> ….
> The new referrer URLs will initially only occur in a small percentage of searches. You should expect to see old and new forms of the URLs as this change gradually rolls out.[42]

55. The redirection tool that Michael VanDeMar described in March 2009 did not include the search terms in its URL (and thus, these terms were not subsequently transmitted to webmasters via the browser's referrer header). However, one month later when Google announced that it would be using the redirection tool for all links, the redirection script was changed to include the search terms in the redirection URL (via a new "q" parameter), thus guaranteeing that webmasters would not lose access to user search query data.

56. The new redirection tool also leaks data to web site administrators that had never before been available to anyone but Google: The item number of the search result that was clicked on (*e.g.*, the 3rd link or 5th link from the search results page).[43] The leakage of this additional information was confirmed by Matt Cutts, which he described as a benefit to web site administrators:

> I think if you do experiments, you'll be able to confirm your speculation **… I think this is awesome for webmasters--even more information than you could glean from the previous referrer string**.[44]

57. A May 2009 video featuring Matt Cutts, posted to the official GoogleWebmasterHelp YouTube channel, describes the change in the search query information leaked via the referrer header:

---

[42] Posting of Brett Crosby to Google Analytics Blog, An upcoming change to Google.com search referrals; Google Analytics unaffected, http://analytics.blogspot.com/2009/04/upcoming-change-to-googlecom-search.html (April 14, 2009, 2:50 p.m.).

[43] Posting of Patrick Altoft to Blogstorm, Google Ads Ranking Data to Referrer String, http://www.blogstorm.co.uk/google-adds-ranking-data-to-referrer-string/ (April 15, 2009).

[44] Posting of Matt Cutts to Blogstorm, Google Ads Ranking Data to Referrer String, http://www.blogstorm.co.uk/google-adds-ranking-data-to-referrer-string/#IDComment77457344 (April 15, 2009, 7:28 p.m.) (emphasis supplied).

> [T]here is a change on the horizon and it's only a very small percentage of users right now, but I think that it probably will grow and it will grow over time where Google's referrer, that is whenever you do a Google search and you click on a result, you go to another website and your browser passes along a value called a referrer. That referrer string will change a little bit.
>
> It used to be google.com/search, for example.
>
> Now, it will be google.com/url.
>
> **And for a short time we didn't have what the query was which got a lot of people frustrated**, but the google.com/search, **the new Google referrer string will have the query embedded in it.**
>
> And there's a really interesting tidbit that not everybody knows, which is--it also has embedded in that referrer string a pretty good idea of where on the page the click happened.
>
> So, for example, if you were result number one, there's a parameter in there that indicates the click came from result number one. If you were number four, it will indicate the click came from, result number four. So, now, you don't necessarily need to go scraping Google to find out what your rankings were for these queries. You can find out, "Oh, yeah. I was number one for this query whenever someone clicked on it and came to my website."
>
> So that can save you a ton of work, you don't need to worry nearly as much, you don't have to scrape Google, you don't have to think about ranking reports. Now, we don't promise that these will, you know, be a feature that we guarantee that we'll always have on Google forever **but definitely take advantage of it for now**.
> ….
> [F]or the most part, this gives you a very accurate idea of where on the page you were, so you get all kinds of extra information that you can use in your analytics and to compute your ROIs without having to do a lot of extra work. **So, if you can, it's a good idea to look at that referrer string and start to take advantage of that information.**"[45]

58. In or around July 2010, Google again began stripping the search terms from the Referrer Headers transmitted by a small percentage of browsers. On July 13, 2010, individuals in the SEO community noticed the change made by Google. One commentator in a web forum wrote that:

[45] Matt Cutts, Can you talk about the change in Google's referrer string?, GoogleWebMasterHelp Channel (May 6, 2009), http://www.youtube.com/watch?v=4XoD4XyahVw (last viewed October 24, 2010).

> More and more visits from Google in my server log files are without exact referrer information, and have only 'http://www.google.com', 'http://www.google.com.au', etc. which doesn't allow to find out keyword and SERP [search engine results] page from which this visit was made.[46]

59. On July 13 2010, Matt Cutts posted a message to the same SEO forum:

> Hey everybody, I asked folks who would know about this. It turns out there was an issue a couple weeks ago where some code got refactored, and the refactoring affected referrers for links opened in a new tab or window. Right now the team is **expecting to have a fix out in the next week** or so. Hope that helps.[47]

7. The Science of Reidentification

60. "Reidentification" is a relatively new area of study in the computer science field. Paul Ohm, a professor of law and telecommunications at the University of Colorado Law School, is a leading scholar on how reidentification impacts internet privacy. Much of the following information comes from Professor Ohm's article entitled "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymizaton" published in the UCLA Law Review in August of 2010.[48]

61. In a nutshell, reidentification creates and amplifies privacy harms by connecting the dots of "anonymous" data and tracing it back to a specific individual. Professor Ohm describes it as follows:

> The reverse of anonymization is reidentification or deanonymization. A person, known in the scientific literature as an adversary, reidentifies anonymous data by linking anonymized records to outside information, hoping to discover the true identity of the data subjects.
> . . .
> Reidentification combines datasets that were meant to be kept apart, and in doing so, gains power through accretion. Every successful reidentification, even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification. Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal.[49]

---

[46] Posting of at2000 to Webmaster World, More and more referrals from Google are without exact referrer string, http://www.webmasterworld.com/google/4168949.htm (July 13, 2010, 4:01 a.m.).

[47] Posting of Matt Cutts to Webmaster World, *supra*, n.45 (July 13, 2010, 9:46 p.m.) (emphasis supplied).

[48] 57 UCLA L. REV. 1701 (2010).

[49] *Id*. at *7-8.

62. Reidentification techniques, like those used in the AOL debacle, can be used as links in chains of inference connecting individuals to harmful facts. Reidentification works by discovery pockets of surprising uniqueness in aggregated data sets. Just as human fingerprints can uniquely identify a single person and link that person with "anonymous" information—a print left at a crime scene—so too do data subjects generate "data fingerprints"—combinations of values of data shared by nobody else. What has surprised researchers is that data fingerprints can be found in pools of non-PII data, such as the uniqueness of a person's search queries in the AOL debacle.[50]

63. Once a person finds a unique data fingerprint, he can link that data to outside information, sometimes called auxiliary information. "Anonymous" search query information would protect privacy, if only the adversary knew nothing else about people in the world. In reality, however, the world is awash in data about people, with new databases created, bought and sold every day. "Adversaries" (as defined above) combine anonymized data with outside information to pry out obscured identities.[51]

64. And the amount of information contained in new databases has grown exponentially. What's more, the type of available data is increasingly personal and specific. Take, for example, the phenomenon of Facebook's growth. The data created by Facebook users is highly personal, and includes actual names, religious, sexual and political preferences, identification of friends, pictures, messages intended to be shared with friends, and more. With the exploding popularity of social network sites like Facebook, and personal blogs, the information available to adversaries is not only highly-specific to individuals, it is often user-created, increasing accuracy and veracity of available data. Never before in human history has it been so easy to peer into the private diaries of so many people. Some researchers call this the "age of self-revelation."[52]

65. Reidentification is characterized by accretion, or the growing together of separate parts into a single whole. As Professor Ohm explains:

---

[50] *Id*. at *17.

[51] *Id*.

[52] *Id*. at *17-18.

> The accretion problem is this: once an adversary has linked two anonymized databases together, he can add the newly linked data to his collection of outside information and use it to help unlock other anonymized databases. Success breeds further success . . . ***once any piece of data has been linked to a person's real identity, any association between this data and a virtual identify breaks the anonymity of the latter. This is why we should worry even about reidentification events that seem to expose only non-sensitive information, because they increase the linkability of data, and thereby expose people to potential future harm.***[53]

66. The accretive reidentification problem is exacerbated by the growing prevalence of internet "data brokers." The buying and selling of consumer data is a multibillion-dollar, unregulated business that's growing larger by the day.[54] Data is increasingly bought, sold and resold by data brokers, which amplifies the accretion problem. Advancements in computer science, data storage and processing power, and data accretion by data brokers make it much more likely that an adversary could link at least one fact to any individual and blackmail, discriminate against, harass, or steal the identity of that person.

67. On October 25, 2010, the *Wall Street Journal* reported that a highly-sophisticated data broker, RapLeaf Inc. is accomplishing accretive reidentification of "anonymous" data with astonishing success.[55] According to the report, RapLeaf has been gathering data, including user names and email addresses, from numerous sources across the internet. Using accretive reidentification techniques, RapLeaf is able to cross-index "anonymous" data with email addresses and thereby associate real names with Web-browsing habits and highly-personal information scraped from social network sites such as Facebook. By 2009, RapLeaf had indexed more than 600 million unique email addresses, and was adding more at a rate of 35 million per month.

68. Data gathered and sold by data brokers like RapLeaf can be very specific. RapLeaf deanonymizes and connects to real names a wide variety of data types, including data regarding demographics, interests, politics, lifestyle, finances, donations, social networks, site memberships, purchases, and shopping habits. RapLeaf's segments recently included a person's household income range, age range, political leaning, and gender and age of children in the household, as well as

---

[53] *Id*. at *29 (emphasis supplied).

[54] Rick Whiting, Data Brokers Draw Increased Scrutiny (July 10, 2006), http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=190301136.

[55] Emily Steele, *A Web Pioneer Profiles Users by Name* (October 25, 2010), *available at* http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

interests in topics including religion, the Bible, gambling, tobacco, adult entertainment and "get rich quick" offers. In all, RapLeaf segmented people into more than 400 categories. This aggregated and deeply personal information is then sold to or used by tracking companies or advertisers to rack users across the Internet.

8. Google's Systematic Disclosure of Billons of User Search Queries Each Day Presents an Imminent Threat of Concrete and Particularized Privacy Harm

69. One type of anonymization practice is called "release-and-forget," in which the data administrator will release records, and then forgets, meaning she makes no attempt to track what happens to the records after release.[56] To protect the privacy of the users in the released data, prior to releasing the data, the administrator will single out identifying information and either strip that information from the database, or modify it to make it more general and less specific to any individual.[57] Many of the recent advances in the science of reidentification target release-and-forget anonymization in particular.[58]

70. Google's transmission of search queries is a type of piecemeal "release-and-forget" anonymization.[59] Google transmits a single user search query each time a Google user clicks on a link in Google's search results page. Over the course of just one day, on information and belief, Google transmits millions of search queries to third parties. Google will likely argue that search query information alone contains no personally-identifiable information. Such an argument is practically equivalent to the data administrator who "anonymizes" data before releasing it to the outside world. But, as repeatedly demonstrated, easy reidentification of "anonymous" highlights the flaws in this thinking.

71. Google itself has taken the position that even seemingly benign, "anonymous" information presents serious privacy concerns. For example, in *Gonzales v. Google*, *supra*, n.12, even though the Government was requesting search queries stripped of any "identifying

[56] Ohm, *supra*, n.47 at *9-10.
[57] *Id*. at *11-12.
[58] *Id*. at *10.
[59] *Id*. at *9.

information" (such as the user's IP address), Google argued that releasing such data would nonetheless risk disclosure of user identities.

72. In fact, when a Google user clicks on a link in Google's search results page, the user's search query is not the only information revealed. For the vast majority of Google users, the user's IP address is concurrently transmitted along with the search query. An IP address is similar to a phone number in that it identifies the exact computer being used by the user to search and navigate the internet.

73. In response to an inquiry from Congressman Joe Barton about privacy issues surrounding Google's acquisition of DoubleClick, Google admitted that "information that can be combined with readily available information to identify a specific individual is also generally considered personal information."[60] But Google has repeatedly downplayed the existence of "readily available information" helpful for tying IP addresses to places and individuals. Professor Ohm highlights Google's untenable position as follows:

> For example, websites like Google never store IP addresses devoid of context; instead, they store them connected to identity or behavior. Google probably knows from its log files, for example, that an IP address was used to access a particular email or calendar account, edit a particular word processing document, or send particular search queries to its search engine. By analyzing the connections woven throughout this mass of information, Google can draw some very accurate conclusions about the person linked to any particular IP address.
>
> Other parties can often link IP addresses to identity as well. Cable and telephone companies maintain databases that associate IP addresses directly to names, addresses, and credit card numbers. That Google does not store these data associations on its own servers is hardly the point. Otherwise, national ID numbers in the hands of private parties would not be "personal data" because only the government can authoritatively map these numbers to identities.[61]

74. Similarly, an independent European advisory body on data protection and privacy found that "The correlation of customer behaviour across different personalised services of a search

[60] Letter from Alan Davidson, Google's Senior Policy Counsel and Head of U.S. Public Policy, to Congressman Joe Barton at 12-13 (December 21, 2007), *available at* http://searchengineland.com/pdfs/071222-barton.pdf.

[61] Ohm, *supra*, n.47 at *41.

engine provider … can also be accomplished by other means, based on cookies or other distinguishing characteristics, such as individual IP addresses."[62]

75. Congressman Barton's inquiry in connection with the DoubleClick acquisition also focused on cookies and privacy. Cookies are small data files that store user preferences and other information, and allow websites to recognize the user or computer visiting their site. In its response to Congressman Barton, Google wrote that "online ad-serving technology can be used by advertisers to serve and manage ads across the web … the ad server sets a cookie on the user's computer browser when the user views an ad served through the ad server. That cookie may be read in the future when the ad server serves other ads to the same browser."[63] An ad serving company with any substantial market share would thus be able to readily link the search queries that Google provides to the IP addresses or cookies of internet users visiting the websites they serve.

VI. FACTS RELATING TO PLAINTIFF

76. Plaintiff Paloma Gaos has at all material times been a user of Google's search engine services, including the period prior to November 2008 when Google first began to test advanced AJAX technologies that temporarily eliminated user search queries from referrer headers coming from Google search results pages, and for all periods thereafter when Google was disseminating search queries to third party websites.

77. During all time periods in which Google was transmitting user search queries to third parties, Plaintiff conducted numerous searches, including "vanity searches" for her actual name and the names of her family members, and clicked on links on her Google search results pages.

78. As a result, Google transmitted Plaintiff's full search queries to third parties by sending the URLs containing her search queries to third party websites that appeared in Plaintiff's Google search results page and which Plaintiff clicked on a link.

[62] Article 29 Data Protection Working Party at 21 (January 2008), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

[63] Letter from Davidson to Barton, *supra*, n.58 at 15.

79. In other words, when Plaintiff clicked on each link on her Google search results pages, the owner of the destination website that Plaintiff clicked on received from Google Plaintiff's search terms through the Referral Header function.

80. As a result, Plaintiff has suffered actual harm in the form of Google's unauthorized and unlawful dissemination of Plaintiff's search queries, which contained sensitive personal information, to third parties.

VII. CLASS ACTION ALLEGATIONS

81. Pursuant to Rules 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and all other persons in the following similarly-situated class: ***all persons in the United States who, at any time after October 25, 2006, submitted a search query at Google.com and clicked on any link displayed by Google in its search results*** (the "Class"). Excluded from the Class are Google, its officers and directors, legal representatives, successors or assigns, any entity in which Google has or had a controlling interest, the judge to whom this case is assigned and the judge's immediate family.

82. Plaintiff also seeks to represent a subclass that includes each member of the proposed class described in paragraph 72 who at any time after October resided in the State of California (the "Subclass").

83. The Class and Subclass are each composed of numerous people, whose joinder in this action would be impracticable. The disposition of their claims through this class action will benefit Class and Subclass members, the parties and the courts. Upon information and belief, Google's search engine has been used by hundreds of millions of users during the relevant time period.

84. There is a well-defined community of interest in questions of law and fact affecting the Class and Subclass. These questions of law and fact predominate over individual questions affecting individual Class and Subclass members, including, but not limited to, the following:

a. whether and to what extent Google has disclosed its users' search queries to third parties, and whether the disclosure is ongoing;

b. whether Google's conduct described herein violates Google's Privacy Policy and representations to Plaintiff, the Class and the Subclass;

c. whether Google's conduct described herein violates the Electronic Communications Privacy Act, 18 U.S.C. § 2702 *et seq.*;

d. whether Google's conduct described herein violates Cal. Civ. Code §§ 1572 & 1573;

e. whether Google's conduct described herein constitutes a breach of contract;

f. whether Google unlawfully misrepresented that it would not share users' search queries and personal information with third parties;

g. whether Google is unjustly enriched as a result of its conduct described herein; and

h. whether Plaintiff and members of the Class and Subclass are entitled to injunctive and other equitable relief.

85. Google has engaged, and continues to engage, in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, the Class and the Subclass. Similar or identical statutory and common law violations, business practices and injuries are involved. Individual questions, if any, pale by comparison to the numerous common questions that dominate.

86. The injuries, actual and imminent, sustained by Plaintiff, the Class and the Subclass flow, in each instance, from a common nucleus of operative facts. In each case, Google caused or permitted unauthorized communications of private and personally-identifying information to be delivered to third parties without adequate or any notice, consent or opportunity to opt out.

87. Given the similar nature of the Class and Subclass members' claims and the absence of material differences in the statutes and common laws upon which the Class and Subclass members' claims are based, a nationwide class will be easily managed by the Court and the parties.

88. Because of the relatively small size of the individual Class and Subclass members' claims, no Class or Subclass user could afford to seek legal redress on an individual basis.

89. Plaintiff's claims are typical of those of the Class and Subclass as all members of the Class and Subclass are similarly affected by Google's uniform and actionable conduct as alleged herein.

90. Google has acted and failed to act on grounds generally applicable to Plaintiff and members of the Class and Subclass, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and Subclass.

91. Plaintiff will fairly and adequately protect the interests of the Class and Subclass and has retained counsel competent and experienced in class action litigation. Plaintiff has no interests antagonistic to, or in conflict with, the Class and Subclass that Plaintiff seek to represent.

92. Plaintiff reserves the right to revise the above class definitions based on facts learned in discovery.

COUNT I
(Violation of the Electronic Communications Privacy Act)
(on behalf of Plaintiff, the Class and the Subclass)

93. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

94. The Electronic Communications Privacy Act (the "ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12).

95. The ECPA also broadly defines the contents of a communication. Pursuant to the ECPA, "contents" of a communication, when used with respect to any wire, oral, or electronic communications, include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication. The definition thus includes all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive.

96. Pursuant to the ECPA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A).

97. Pursuant to the ECPA, Google operates an "electronic communications service" as defined in 18 U.S.C. § 2510(15). Pursuant to the Stored Communications Act of 1986 (the "SCA"), Google also provides a "remote computing service" to the public. 18 U.S.C. § 2711(2).

98. In relevant part, 18 U.S.C. § 2702(a) of the ECPA provides as follows:

> (a) **Prohibitions.—** Except as provided in subsection (b) or (c)—
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
> (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

99. As alleged herein, by disclosing the private search queries of Plaintiff and members of the Class without authorization, Google has knowingly divulged the contents of communications of Plaintiff and members of the Class while those communications were in electronic storage on its service, in violation of 18 U.S.C. § 2702(a)(1).

100. As alleged herein, by disclosing the private search queries of Plaintiff and members of the Class without authorization, Google has knowingly divulged the contents of communications of Plaintiff and members of the Class carried or maintained on its systems, in violation of 18 U.S.C. § 2702(a)(2).

101. Google intentionally disclosed its users' communications to third parties to enhance its profitability and revenue. The disclosures were not necessary for the operation of Google's systems or to protect Google's rights or property.

102. As a result of Google's unauthorized and unlawful disclosure of Plaintiff and Class members' private search queries, Plaintiff and members of the Class have suffered damages from Google's violations of 18 U.S.C. § 2702 in an amount to be determined at trial.

103. Plaintiff and Class members are "person[s] aggrieved by [a] violation of [the SCA] in which the conduct constituting the violation is engaged in with a knowing or intentional state or mind…" within the meaning of 18 U.S.C. § 2707(a).

104. Plaintiff and members of the Class therefore seek remedy as provided for by 18 U.S.C. § 2707(b) and (c), including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and attorneys' fee and other litigation costs reasonably incurred.

COUNT II
(Fraudulent Misrepresentation)
(on behalf of Plaintiff, the Class and the Subclass)

105. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

106. Google falsely represented in its Privacy Policy and elsewhere that it would not make users' personal information and search queries available to any third party.

107. Google made these false statements in order to induce users to use Google's search engine service.

108. In contradiction to its representations and as described herein, Google sent and made available to third parties Plaintiff and Class members' private search queries.

109. Plaintiff and members of the Class relied on Google's fraudulent misrepresentations in agreeing to use Google's search services, including use of Google to search for sensitive personal information, because users believed that Google did not transmit such information to third parties.

110. As a result of Defendant's fraudulent misrepresentations, Plaintiff and the Class have suffered harm, including but not limited to the disclosure of their sensitive personal information, in an amount to be determined at trial.

COUNT III
(Negligent Misrepresentation)
(On behalf of Plaintiff, the Class and the Subclass)

111. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

112. In an effort to induce users to use Google's search service, Defendant negligently and/or recklessly represented in its Privacy Policy and elsewhere that it would not make users' personal information and search queries available to any third party.

113. In contradiction to its representations and as described herein, Google sent and made available to third parties Plaintiff and Class members' private search queries.

114. The purpose of Google's representations was to induce users to use Google's search engine service.

115. Plaintiff and members of the Class relied on Google's negligent and/or reckless misrepresentations in agreeing to use Google's search services, including use of Google to search for sensitive personal information, because users believed that Google did not transmit such information to third parties.

116. As a result of Defendant's negligent and/or reckless misrepresentations, Plaintiff and the Class have suffered harm, including but not limited to the disclosure of their sensitive personal information, in an amount to be determined at trial.

COUNT IV
(Public Disclosure of Private Facts)
(on behalf of Plaintiff and the Subclass)

117. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

118. By its conduct, Google has knowingly and intentionally caused the public disclosure of Plaintiff and members of the California Subclass' private search queries. These private search queries were not newsworthy, were not generally available to the public, and are facts that a reasonable person would not wish disclosed.

119. Plaintiff and members of the Subclass have suffered harm as a result of Google's public disclosure of their private search queries in an amount to be determined at trial.

120. Plaintiff and members of the Subclass are entitled to actual and punitive damages and injunctive relief for these torts.

COUNT V

(Violation of Cal. Civ. Code §§ 1572 & 1573)
(on behalf of Plaintiff and the Subclass)

121. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

122. California Civil Code § 1572 provides in relevant part that actual fraud exists when a party to a contract suppresses "that which is true, by one having knowledge or belief of the fact" "with intent to deceive another party thereto, or to induce him to enter into the contract."

123. California Civil Code § 1573 provides in relevant part that constructive fraud exists "[i]n any such act or omission as the law specially declares to be fraudulent, without respect to actual fraud."

124. Google's Privacy Policy constitutes a valid and enforceable agreement with Plaintiff and members of the Subclass.

125. Google violated § 1572 through its repeated and explicit false assertions that it would not share its users' search queries with third parties without consent or absent a compelling reason, as described herein. Google further violated this section by suppressing its knowledge of this fact.

126. Additionally and/or alternatively, Google violated § 1573 by breaching its duty to protect its users' identities from third parties and gaining an advantage in doing so, by misleading its users to their prejudice, as described herein.

127. Plaintiff, on behalf of herself and the Subclass, seek damages from Google, including but not limited to disgorgement of all proceeds Google obtained from its unlawful business practices.

COUNT VI
(Breach of Contract)
(on behalf of Plaintiff, the Class, and the Subclass)

128. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

129. The provisions of Google's Privacy Policy (the "Agreement") constitute a valid and enforceable contract between Plaintiff and the Class on the one hand, and Google on the other.

130. Under the Agreement, Plaintiff and the Class agreed to use Defendant's services and transmit sensitive personally-identifiable information to Google in exchange for Google's promise that it would not share that personal information with third parties without users' authorization.

131. Google materially breached the terms of the Agreement through its unlawful conduct alleged herein, including the disclosure of Plaintiff's and the Class's private search queries to third parties.

132. As a result of Google's misconduct and breach of the Agreement described herein, Plaintiff and the Class suffered injury. Plaintiff, on behalf of herself, the Class and Subclass, seek damages from Google in an amount to be determined at trial.

COUNT VIII
(Unjust Enrichment (In the Alternative))
(on behalf of Plaintiff, the Class and the Subclass)

133. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

134. Plaintiff and members of the Class and Subclass have conferred a benefit upon Google. Google has received and retained valuable information belonging to Plaintiff and members of the Class and Subclass, and as a result of sharing its users' search queries with third parties without their consent, Google has improved the quality of its search engine and enjoyed increased revenues from advertisers.

135. Google appreciates or has knowledge of said benefit.

136. Under principles of equity and good conscience, Google should not be permitted to retain the benefits that it unjustly received as a result of its actions.

137. Plaintiff, on her own behalf and on behalf of the Class, seeks the imposition of a constructive trust on and restitution of the proceeds of Google received as a result of its conduct described herein, as well as attorney's fees and costs pursuant to Cal. Civ. Proc. Code § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

A. Certify this case as a class action on behalf of the Class and Subclass defined above, appoint Plaintiff as representative of the Class and Subclass, and appoint her counsel as counsel for the Class and Subclass, pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Declare that Google's actions, as described herein, violate the Electronic Communications Privacy Act (18 U.S.C. § 2702 *et seq.*), Cal. Civ. Code §§ 1572-73, constitute violations of the common law and unjust enrichment;

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff, the Class, and the Subclass, including, *inter alia*, an order prohibiting Google from engaging in the wrongful and unlawful acts described herein;

D. Awarding damages, including statutory damages where applicable, to Plaintiff, the Class and the Subclass, in an amount to be determined at trial;

E. Awarding all economic, monetary, actual, consequential, and compensatory damages caused by Google's conduct, and if its conduct is proved willful, award Plaintiff, the Class and the Subclass exemplary damages;

F. Award restitution against Google for all money to which Plaintiff and the Class are entitled in equity;

G. Order Google to disgorge revenues and profits wrongfully obtained;

H. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

I. Awarding Plaintiff the Class and the Subclass interest, to the extent allowable; and

J. Awarding such other and further relief as equity and justice may require.

Dated: May 2, 2011

Respectfully submitted,
EDELSON MCGUIRE, LLC

/s/ Michael Aschenbrener
Michael Aschenbrener
Attorneys for Plaintiff

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: May 2, 2011

Respectfully submitted,
EDELSON MCGUIRE, LLC

/s/ Michael Aschenbrener
Michael Aschenbrener
Attorneys for Plaintiff