

1 KASSRA P. NASSIRI (215405)

(knassiri@nassiri-jung.com)

2 CHARLES H. JUNG (217909)

(cjung@nassiri-jung.com)

3 NASSIRI & JUNG LLP

47 Kearny Street, Suite 700

4 San Francisco, California 94108

Telephone: (415) 762-3100

5 Facsimile: (415) 534-3200

6 MICHAEL J. ASCHENBRENER

(maschenbrener@edelson.com)

7 EDELSON MCGUIRE LLC

350 North LaSalle Street, Suite 1300

8 Chicago, Illinois 60654

Telephone: (312) 589-6370

9 Facsimile: (312) 589-6378

10
11 Attorneys for Plaintiff

12 **UNITED STATES DISTRICT COURT**

13 **NORTHERN DISTRICT OF CALIFORNIA**

14 **SAN JOSE DIVISION**

15
16 PALOMA GAOS, an individual, on behalf of
herself and all others similarly situated,

17 Plaintiff,

18 v.

19 GOOGLE INC., a Delaware corporation,

20 Defendant.

Case No.

CLASS ACTION

CLASS ACTION COMPLAINT

ACTION FILED: 10/25/10

JURY TRIAL DEMANDED

21
22 Plaintiff Paloma Gaos brings this suit on behalf of herself and all others similarly situated,
23 and makes the following allegations on information and belief, except as to allegations pertaining to
24 Plaintiff, which are based on her personal knowledge:

25 **I. INTRODUCTION**

26 1. Plaintiff brings this class action complaint against Google Inc. (“Google”) for
27 intentionally, systematically and repeatedly divulging its users’ search queries to third parties. This
28 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, the California Online Privacy

1 Act of 2003, Cal. Bus. & Prof. Code § 22575 *et seq.*, the California Consumer Legal Remedies Act,
2 Cal. Civ. Code § 1750 *et seq.*, the California False Advertising Law, Cal. Bus. & Prof. Code § 17500
3 *et seq.*, the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*, and
4 common law.

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

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

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

23 5. Google has acknowledged that search query information alone may reveal sensitive
24 PII. And Google has demonstrated that it could easily stop disclosing search query information to
25 third parties, without disrupting the effectiveness of its service to its users, if it wished to do so. But
26 because the real-time transmission of user search queries increases Google’s profitability, it chooses
27 not to utilize the demonstrated technology that would prevent the disclosure of its users’ PII.
28

1 **II. PARTIES**

2 6. Plaintiff Paloma Gaos is a resident of San Francisco County, California. Plaintiff has
3 at all material times been a user of Google’s search engine services and has conducted “vanity
4 searches,” including searches for her actual name and the names of her family members and has
5 clicked on links contained in Google’s search results.

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

9 **III. JURISDICTION AND VENUE**

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

16 9. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, 18 U.S.C. §
17 2702 and 18 U.S.C. § 2707. This Court has supplemental jurisdiction over the California state law
18 claims pursuant to 28 U.S.C. § 1367.

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

22 **IV. INTRADISTRICT ASSIGNMENT**

23 11. Intradistrict assignment to the San Jose Division is proper because a substantial
24 portion of the events and conduct giving rise to the violations of law complained of herein occurred
25 in San Jose County.

26 //

27 //

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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. Google has implemented various innovations in the online advertising market that helped make it one of the biggest advertisers in the world.

15. Using technology from its wholly-owned subsidiary DoubleClick, Google can 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.

16. Third-party search engine optimization ("SEO") companies help businesses design their websites so that users conducting internet searches 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 tuned 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

1 Google's search results. To the extent that SEOs are successful in getting their clients' relevant
2 pages to appear at or near the top of Google's search results page, users are more likely to return to
3 Google next time they want to search for information on the internet. And the more people use
4 Google for search, the more revenue Google derives from its advertising business.

6 **2. Google's Privacy Promises**

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

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

17 19. Because Google's success depends on gaining the trust of its users, Google's Privacy
18 Policy sets forth representations intended to foster the safety and privacy protection offered by
19 Google's search services. As of October 14, 2005, Google's Privacy Policy⁵ stated as follows:

21
22 ¹ Christopher Ketcham & Travis Kelly, *The Cloud Panopticon* (April 9, 2010),
23 http://www.theinvestigativefund.org/investigations/rightsliberties/1274/the_cloud_panopticon (last
visited October 24, 2010).

24 ² Gunther Eysenbach and Christian Köhler, *How do consumers search for and appraise health*
25 *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>.

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

28 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).

1 Google only shares personal information with other companies or individuals
2 outside of Google in the following limited circumstances:

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

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

24 21. Google also stated in its October 14, 2005 Privacy Policy that “We may share with
25 third parties certain pieces of *aggregated, non-personal information*, such as the number of users
26 who searched for a particular term, for example, or how many users clicked on a particular
27 advertisement. Such information does not identify you individually.”⁷ Google defined “aggregated,
28 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

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

27 ⁷ Google’s October 14, 2005 Privacy Policy, *supra*, n.5 (emphasis supplied).

28 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).

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

4 23. Google makes similar representations about the privacy of its users’ search queries on
5 its video “Privacy Channel” on YouTube. The first video that plays when a user visits the Privacy
6 Channel starts with the statement that “at Google, we make privacy a priority in everything we do.”⁹
7 Google also states in another privacy video that “We don’t sell user information to other
8 companies.”¹⁰

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

23
24
25 ⁹ Google’s Privacy Principles, <http://www.youtube.com/watch?v=5fvL3mNtl1g> (January 26, 2010)
(last visited October 25, 2010).

26 ¹⁰ Google’s Privacy Principles, [http://googleblog.blogspot.com/2010/01/googles-privacy-](http://googleblog.blogspot.com/2010/01/googles-privacy-principles.html)
[principles.html](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).

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

28 ¹² *Id.*

1 **3. Google Admits Search Queries Contain Sensitive, Personal Data**

2 25. In 2006, the Department of Justice sought to compel Google to produce thousands of
3 users' individual search queries.¹³ As set forth in the Government's subpoena, it sought only
4 "anonymized" data, namely, the text of the search string entered by Google users, and not "any
5 additional information that may be associated with such a text string that would identify the person
6 who entered the test string into the search engine, or the computer from which the test string was
7 entered."¹⁴

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

- 12 • Google does not publicly disclose the searches [sic] queries entered
13 into its search engine. If users believe that the text of their search
14 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.
- 15 • There are ways in which a search query alone may reveal personally
16 identifying information. For example, many internet users have
17 experienced the mistake of trying to copy-and-paste text into the
18 search query box, only to find that they have pasted something that
they did not intended. Because Google allows very long queries, it is
19 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
20 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
21 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.

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

24
25
26 _____
¹³ *Gonzales v. Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW).

27 ¹⁴ *Id.* at 682.

28 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).

- 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 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

28. In its order¹⁹ 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.

¹⁶ Google’s Opposition to the Government’s Motion to Compel at 1, *supra*, n.13.

¹⁷ *Id.* at 18.

¹⁸ *Id.*

¹⁹ *Gonzales*, 234 F.R.D. at 687.

1
2 29. Google’s awareness of the privacy concerns surrounding search queries was also
3 demonstrated in response to a massive disclosure of user search queries by AOL. In August 2006,
4 AOL released an “anonymized” dataset of 20 million search queries conducted by 658,000 AOL
5 users over a three-month period.²⁰ That data included search queries revealing names, addresses,
6 local landmarks, medical ailments, credit card numbers and social security numbers.²¹

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

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

17 32. An AOL spokesman, Andrew Weinstein, apologized on behalf of AOL and said he
18 wasn’t surprised that the *New York Times* was able to connect the dots and reidentify “anonymous”
19 users in the dataset: “We acknowledged that there was information that could potentially lead to
20 people being identified...”²⁵

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

25 ²¹ *Id.* at ¶ 18.

26 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>.

27 ²³ *Id.*

28 ²⁴ *Id.*

²⁵ *Id.*

1
2 33. Soon after the release of the search query data by AOL, Google CEO Eric Schmidt
3 spoke about the AOL privacy breach. He called AOL's release of user search data "a terrible thing"
4 and reassured Google users that their search queries were safe and private:

5 Well, [this sort of privacy breach is] obviously a terrible thing. And the data as
6 released was obviously not anonymized enough, and maybe it wasn't such a good
7 idea to release it in the first place. Speaking for Google, we exist by virtue of the trust
8 of our end users. So if we were to make a mistake to release private information that
9 could be used against somebody, especially if it could be used against them in a way
10 that could really hurt them in a physical way or something like that, it would be a
11 terrible thing. We have lots and lots of systems in the company to prevent that.

12 It's funny that we talk about the company being more transparent. But there are many
13 things inside our company that are important that we don't share with everyone,
14 starting with everyone's queries and all the information that that implies. I've always
15 worried that the query stream was a fertile ground for governments to randomly
16 snoop on people [for example]. We had a case where we were only a secondary party,
17 where the government gave us a subpoena, which was in our view, over-broad. And
18 this over-broad subpoena we fought in federal court – one of the great things about
19 the American system is that you can actually have a judge make an impartial
20 decision. And the judge ruled largely in our favor. So that's an example of how
21 strongly we take this point.²⁶

22 4. A Brief Primer on "Referrer Headers"

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

25 35. The HTTP Referrer function is a standard web browser function, provided by
26 standard web browsers since the HTTP 1.0 specification in May 1996.²⁷ When an internet user visits
27 a web page using their computer or mobile device, every major web browser (*e.g.*, Internet Explorer,
28 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.

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>

1 36. The current version of the publicly-available HTTP specification, RFC 2616,²⁸
2 provides for HTTP Referrer Headers in its provision 14.36.²⁹ It is well known that if a site places
3 confidential information, such as a username, in a URL, then the site risks releasing this information
4 whenever a user clicks a link to leave the site. Indeed, the HTTP specification specifically flags this
5 risk; in section 15.1.3, the HTTP specification advises developers of substantially the same problem:
6 “Authors of services which use the HTTP protocol SHOULD NOT use GET based forms for the
7 submission of sensitive data, because this will cause this data to be encoded in the REQUEST-
8 URI.”³⁰

10 **5. Google Transmits Individual User Search Queries to Third Parties**

11 37. Since the service’s launch, and continuing to this day, Google’s search engine has
12 included the search terms in the URL of the search results page. Thus, for example, a search for
13 “abortion clinics in Indianapolis” would return a page with a URL similar to
14 “http://www.google.com/search?q=abortion+clinics+in+Indianapolis.”

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

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

23 **6. Google’s Transmission of User Search Queries is Intentional**

24 40. Because Google’s financial success depends on, among other things, the symbiotic
25 relationship it shares with SEOs and the ability for third parties to engage in web analytics, Google

26
27 ²⁸ <http://www.w3.org/Protocols/rfc2616/rfc2616.html>

28 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>

1 has placed a high priority on revealing individual user search queries to third parties.

2 Notwithstanding its repeated representations to the contrary in its Privacy Policy and to privacy
3 regulators, Google continues to this day to transmit user search queries.

4 41. Neither Google's search technology nor the nature of the internet compels Google to
5 divulge user search queries. Google could easily cease transmission of user search queries to third
6 parties, but chooses not to.

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

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

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

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

18 45. The addition of the # symbol had a significantly positive, albeit unintentional impact
19 upon Google user privacy. This is because web browsers do not pass on any information after the #
20 symbol in the referrer header. Thus, using the previous example of a search for the query "drug
21

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

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

27 ³³ Tim O'Reilly, What Is Web 2.0 Design Patterns and Business Models for the Next Generation of
28 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>.

1 addiction,” if a user clicked on the first result, the owner of that web site would only receive
2 “http://www.google.com/” in the referrer header, rather than the search terms that follow the #
3 symbol.

4 46. This change was immediately noticed by the webmaster and search engine
5 optimization community, who complained to Google:

- 6 • “I’m seeing hundreds of these empty google referrers today and wondered
7 what was going on.”³⁵
- 8 • “This means organic searches from Google will now show up as just
9 http://www.google.com/, with no search parameters. In other words, no
10 analytics app can track these searches anymore. I started noticing lots of hits
11 from just ‘http://www.google.com/’ recently in our own search logs. I thought
12 maybe it was just a bug with *Clicky*. But then one of our users contacted me
13 about this article, and my jaw about broke from hitting the floor so hard.”³⁶
- 14 • “What actually *breaks* if Google makes this switchover, and is in fact broken
15 during any testing they are doing, is much more widespread. Every single
16 analytics package that currently exists, at least as far as being able to track
17 what keywords were searched on to find your site in Google, would no longer
18 function correctly.”³⁷

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

21
22
23
24
25 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.).

26 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.).

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

1
2 Currently AJAX results are just a test on Google. At this time only a small
3 percentage of users will see this experiment. **It is not our intention to disrupt**
4 **referrer tracking**, and we are continuing to iterate on this project and are **actively**
5 **working towards a solution**. As we continue experiments, we hope that this test may
6 ultimately provide an easier solution for our customers and a faster experience for our
7 users.³⁸

8
9 48. Google soon ended the test of the AJAX search results page, a fact confirmed by
10 Google Senior Engineer Matt Cutts, who specializes in search optimization issues at Google:

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

13
14 49. In March 2009, Google again began to test technology that unintentionally caused the
15 users' search terms to be stripped from the referrer header transmitted to web sites. The following is
16 an example of the format of the new URL that was being tested in March 2009:

17 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

18
19 50. Michael VanDeMar, a prominent member of the SEO community noticed that he was
20 again seeing AJAX based search results in addition to redirected URLs for every link in the search
21 results page:

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

26
27 51. Google's Matt Cutts soon responded to VanDeMar by leaving a comment on his
28 blog:

29
30 ³⁸ Posting of Matt McGee to Search Engine Land, Google AJAX Search Results = Death To Search
31 Term Tracking?, <http://searchengineland.com/google-ajax-search-results-death-to-search-term-tracking-16431> (February 3, 2009, 5:41 p.m.) (emphasis supplied).

32
33 ³⁹ Posting of Lisa Barone to Outspoken Media, Keynote Address – Matt Cutts, Google,
34 <http://outspokenmedia.com/internet-marketing-conferences/pubcon-keynote-matt-cutts/> (March 12,
35 2009).

36
37 ⁴⁰ Posting of Michael VanDeMar to Smackdown!, Google Re-initiates Testing of AJAX SERP's
38 With Faulty Proposed Fix, <http://smackdown.blogspot.com/2009/03/13/google-re-initiates-testing-of-ajax-serps-with-faulty-proposed-fix/> (March 13, 2009, 11:14 a.m.).

1 Hi Michael, I checked with some folks at Google about this. The redirection through
2 a url redirector was separate from any AJAX-enhanced search results; we do that url
3 redirection for some experiments, but it's not related to the JavaScript-enhanced
4 [AJAX] search results.

5 **The solution to the referrer problem will be coming online in the future. It uses a**
6 **JavaScript-driven redirect that enables us to pass the redirect URL as the**
7 **referrer. This URL will contain a 'q' param that matches the user's query.**⁴¹

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

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

14 <http://www.google.com/search?hl=en&q=flowers&btnG=Google+Search>

15 Now you will start seeing some referrer strings that look like this:

16 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=AFQjCNHJXSUh7Vw7oubPaO3tZOz-z-F-u_w&sig2=X8uCFh6IoPtnwmvGMULQfw

17

18 The new referrer URLs will initially only occur in a small percentage of searches.
19 You should expect to see old and new forms of the URLs as this change gradually
20 rolls out.⁴²

21 53. The redirection tool that Michael VanDeMar described in March 2009 did not include
22 the search terms in its URL (and thus, these terms were not subsequently transmitted to webmasters
23 via the browser's referrer header). However, one month later when Google announced that it would
24 be using the redirection tool for all links, the redirection script was changed to include the search

25 ⁴¹ Posting of Matt Cutts to Smackdown!, *supra*, n.40,
26 <http://smackdown.blogspot.com/2009/03/13/google-re-initiates-testing-of-ajax-serps-with-faulty-proposed-fix/> (March 17, 2009, 10:10 a.m.) (emphasis supplied).

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

1 terms in the redirection URL (via a new “q” parameter), thus guaranteeing that webmasters would
2 not lose access to user search query data.

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

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

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

14 [T]here is a change on the horizon and it's only a very small percentage of users right
15 now, but I think that it probably will grow and it will grow over time where Google's
16 referrer, that is whenever you do a Google search and you click on a result, you go to
17 another website and your browser passes along a value called a referrer. That referrer
18 string will change a little bit.

19 It used to be google.com/search, for example.

20 Now, it will be google.com/url.

21 **And for a short time we didn't have what the query was which got a lot of people
22 frustrated, but the google.com/search, the new Google referrer string will have the
23 query embedded in it.**

24 And there's a really interesting tidbit that not everybody knows, which is--it also has
25 embedded in that referrer string a pretty good idea of where on the page the click
26 happened.

27 So, for example, if you were result number one, there's a parameter in there that
28 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

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

28 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).

1 to go scraping Google to find out what your rankings were for these queries. You can
2 find out, "Oh, yeah. I was number one for this query whenever someone clicked on it
3 and came to my website."

4 So that can save you a ton of work, you don't need to worry nearly as much, you don't
5 have to scrape Google, you don't have to think about ranking reports. Now, we don't
6 promise that these will, you know, be a feature that we guarantee that we'll always
7 have on Google forever **but definitely take advantage of it for now.**

8
9 [F]or the most part, this gives you a very accurate idea of where on the page you
10 were, so you get all kinds of extra information that you can use in your analytics and
11 to compute your ROIs without having to do a lot of extra work. **So, if you can, it's a
12 good idea to look at that referrer string and start to take advantage of that
13 information.**⁴⁵

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

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

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

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

27 7. The Science of Reidentification

28 58. "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

29 ⁴⁵ Matt Cutts, Can you talk about the change in Google's referrer string?, GoogleWebMasterHelp
30 Channel (May 6, 2009), <http://www.youtube.com/watch?v=4XoD4XyahVw> (last viewed October
31 24, 2010).

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

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

1 a leading scholar on how reidentification impacts internet privacy. Much of the following
2 information comes from Professor Ohm’s article entitled “Broken Promises of Privacy: Responding
3 to the Surprising Failure of Anonymization” published in the UCLA Law Review in August of
4 2010.⁴⁸

5 59. In a nutshell, reidentification creates and amplifies privacy harms by connecting the
6 dots of “anonymous” data and tracing it back to a specific individual. Professor Ohm describes it as
7 follows:

8 The reverse of anonymization is reidentification or deanonymization. A person,
9 known in the scientific literature as an adversary, reidentifies anonymous data by
10 linking anonymized records to outside information, hoping to discover the true
11 identity of the data subjects.

12
13 Reidentification combines datasets that were meant to be kept apart, and in doing so,
14 gains power through accretion. Every successful reidentification, even one that
15 reveals seemingly nonsensitive data like movie ratings, abets future reidentification.
16 Accretive reidentification makes all of our secrets fundamentally easier to discover
17 and reveal.⁴⁹

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

25 61. Once a person finds a unique data fingerprint, he can link that data to outside
26 information, sometimes called auxiliary information. “Anonymous” search query information would
27 protect privacy, if only the adversary knew nothing else about people in the world. In reality,
28 however, the world is awash in data about people, with new databases created, bought and sold

29 ⁴⁸ 57 UCLA L. REV. 1701 (2010).

30 ⁴⁹ *Id.* at *7-8.

31 ⁵⁰ *Id.* at *17.

1 every day. “Adversaries” (as defined above) combine anonymized data with outside information to
2 pry out obscured identities.⁵¹

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

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

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

22 64. The accretive reidentification problem is exacerbated by the growing prevalence of
23 internet “data brokers.” The buying and selling of consumer data is a multibillion-dollar,
24 unregulated business that’s growing larger by the day.⁵⁴ Data is increasingly bought, sold and resold
25 by data brokers, which amplifies the accretion problem. Advancements in computer science, data
26 storage and processing power, and data accretion by data brokers make it much more likely that an

27 ⁵¹ *Id.*

28 ⁵² *Id.* at *17-18.

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>.

1 adversary could link at least one fact to any individual and blackmail, discriminate against, harass, or
2 steal the identity of that person.

3
4 65. On October 25, 2010, the *Wall Street Journal* reported that a highly-sophisticated
5 data broker, RapLeaf Inc., is accomplishing accretive reidentification of “anonymous” data with
6 astonishing success.⁵⁵ According to the report, RapLeaf has been gathering data, including user
7 names and email addresses, from numerous sources across the internet. Using accretive
8 reidentification techniques, RapLeaf is able to cross-index “anonymous” data with email addresses
9 and thereby associate real names with Web-browsing habits and highly-personal information scraped
10 from social network sites such as Facebook. By 2009, RapLeaf had indexed more than 600 million
11 unique email addresses, and was adding more at a rate of 35 million per month.

12 66. Data gathered and sold by data brokers like RapLeaf can be very specific. RapLeaf
13 deanonymizes and connects to real names a wide variety of data types, including data regarding
14 demographics, interests, politics, lifestyle, finances, donations, social networks, site memberships,
15 purchases, and shopping habits. RapLeaf’s segments recently included a person’s household income
16 range, age range, political leaning, and gender and age of children in the household, as well as
17 interests in topics including religion, the Bible, gambling, tobacco, adult entertainment and “get rich
18 quick” offers. In all, RapLeaf segmented people into more than 400 categories. This aggregated and
19 deeply personal information is then sold to or used by tracking companies or advertisers to track
20 users across the Internet.

21 **8. Google’s Systematic Disclosure of Billions of User Search Queries Each**
22 **Day Presents an Imminent Threat of Concrete and Particularized**
23 **Privacy Harm**

24 67. One type of anonymization practice is called “release-and-forget,” in which the data
25 administrator will release records, and then forgets, meaning she makes no attempt to track what
26 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

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

⁵⁶ Ohm, *supra*, n.48 at *9-10.

1 information from the database, or modify it to make it more general and less specific to any
2 individual.⁵⁷ Many of the recent advances in the science of reidentification target release-and-forget
3 anonymization in particular.⁵⁸

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

12 69. Google itself has taken the position that even seemingly benign, “anonymous”
13 information presents serious privacy concerns. For example, in *Gonzales v. Google, supra*, n.12,
14 even though the Government was requesting search queries stripped of any “identifying
15 information” (such as the user’s IP address), Google argued that releasing such data would
16 nonetheless risk disclosure of user identities.

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

22 71. In response to an inquiry from Congressman Joe Barton about privacy issues
23 surrounding Google’s acquisition of DoubleClick, Google admitted that “information that can be
24 combined with readily available information to identify a specific individual is also generally
25

26
27 ⁵⁷ *Id.* at *11-12.

28 ⁵⁸ *Id.* at *10.

⁵⁹ *Id.* at *9.

1 considered personal information.”⁶⁰ But Google has repeatedly downplayed the existence of
2 “readily available information” helpful for tying IP addresses to places and individuals. Professor
3 Ohm highlights Google’s untenable position as follows:
4

5 For example, websites like Google never store IP addresses devoid of context;
6 instead, they store them connected to identity or behavior. Google probably knows
7 from its log files, for example, that an IP address was used to access a particular email
8 or calendar account, edit a particular word processing document, or send particular
9 search queries to its search engine. By analyzing the connections woven throughout
10 this mass of information, Google can draw some very accurate conclusions about the
11 person linked to any particular IP address.

12 Other parties can often link IP addresses to identity as well. Cable and telephone
13 companies maintain databases that associate IP addresses directly to names,
14 addresses, and credit card numbers. That Google does not store these data
15 associations on its own servers is hardly the point. Otherwise, national ID numbers in
16 the hands of private parties would not be “personal data” because only the
17 government can authoritatively map these numbers to identities.⁶¹

18 72. Similarly, an independent European advisory body on data protection and privacy
19 found that “The correlation of customer behaviour across different personalised services of a search
20 engine provider ... can also be accomplished by other means, based on cookies or other
21 distinguishing characteristics, such as individual IP addresses.”⁶²

22 73. Congressman Barton’s inquiry in connection with the DoubleClick acquisition also
23 focused on cookies and privacy. Cookies are small data files that store user preferences and other
24 information, and allow websites to recognize the user or computer visiting their site. In its response
25 to Congressman Barton, Google wrote that “online ad-serving technology can be used by advertisers
26 to serve and manage ads across the web ... the ad server sets a cookie on the user’s computer
27 browser when the user views an ad served through the ad server. That cookie may be read in the
28 future when the ad server serves other ads to the same browser.”⁶³ An ad serving company with any

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

27 ⁶¹ Ohm, *supra*, n.48 at *41.

28 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.59 at 15.

1 substantial market share would thus be able to readily link the search queries that Google provides to
2 the IP addresses or cookies of internet users visiting the websites they serve.

3 4 **VI. CLASS ACTION ALLEGATIONS**

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

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

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

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

- 22 a. whether and to what extent Google has disclosed its users’ search queries to third
23 parties, and whether the disclosure is ongoing;
- 24 b. whether Google’s conduct described herein violates Google’s Privacy Policy and
25 representations to Plaintiff, the Class and the Subclass;
- 26 c. whether Google’s conduct described herein violates the Electronic
27 Communications Privacy Act, 18 U.S.C. § 2702 *et seq.*;
- 28 d. whether Google’s conduct described herein violates Cal. Bus. & Prof. Code §
22575 et seq.;

- 1
- 2 e. whether Google’s conduct described herein violates California’s Unfair
- 3 Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq.*);
- 4 f. whether Google’s conduct described herein violates Cal. Bus. & Prof. Code §
- 5 17500 *et seq.*;
- 6 g. whether Google’s conduct described herein violates the California Legal
- 7 Remedies Act (Cal. Civ. Code § 1750, *et seq.*);
- 8 h. whether Google is unjustly enriched as a result of its conduct described herein;
- 9 and
- 10 i. whether Plaintiff and members of the Class and Subclass are entitled to injunctive
- 11 and other equitable relief.

12 78. Google has engaged, and continues to engage, in a common course of conduct giving

13 rise to the legal rights sought to be enforced by Plaintiff, the Class and the Subclass. Similar or

14 identical statutory and common law violations, business practices and injuries are involved.

15 Individual questions, if any, pale by comparison to the numerous common questions that dominate.

16 79. The injuries, actual and imminent, sustained by Plaintiff, the Class and the Subclass

17 flow, in each instance, from a common nucleus of operative facts. In each case, Google caused or

18 permitted unauthorized communications of private and personally-identifying information to be

19 delivered to third parties without adequate or any notice, consent or opportunity to opt out.

20 80. Given the similar nature of the Class and Subclass members’ claims and the absence

21 of material differences in the statutes and common laws upon which the Class and Subclass

22 members’ claims are based, a nationwide class will be easily managed by the Court and the parties.

23 81. Because of the relatively small size of the individual Class and Subclass members’

24 claims, no Class or Subclass user could afford to seek legal redress on an individual basis.

25 82. Plaintiff’s claims are typical of those of the Class and Subclass as all members of the

26 Class and Subclass are similarly affected by Google’s uniform and actionable conduct as alleged

27 herein.

28

1 89. Pursuant to the ECPA, “electronic storage” means any “temporary storage of a wire
2 or electronic communication incidental to the electronic transmission thereof.” 18 U.S.C. §
3 2510(17)(A).

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

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

8 (a) **Prohibitions.**— Except as provided in subsection (b) or (c)—

9 (1) a person or entity providing an electronic communication service to the public shall
10 not knowingly divulge to any person or entity the contents of a communication while in
11 electronic storage by that service; and

12 (2) a person or entity providing remote computing service to the public shall not
13 knowingly divulge to any person or entity the contents of any communication which is
14 carried or maintained on that service—

15 (A) on behalf of, and received by means of electronic transmission from (or created by
16 means of computer processing of communications received by means of electronic
17 transmission from), a subscriber or customer of such service;

18 (B) solely for the purpose of providing storage or computer processing services to such
19 subscriber or customer, if the provider is not authorized to access the contents of any such
20 communications for purposes of providing any services other than storage or computer
21 processing; and

22 (3) a provider of remote computing service or electronic communication service to the
23 public shall not knowingly divulge a record or other information pertaining to a
24 subscriber to or customer of such service (not including the contents of communications
25 covered by paragraph (1) or (2)) to any governmental entity.

26 92. As alleged herein, Google has knowingly divulged the contents of communications of
27 Plaintiff and members of the Class while those communications were in electronic storage on its
28 service, in violation of 18 U.S.C. § 2702(a)(1).

 93. As alleged herein, 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).

 94. 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.

- 1
- 2 a. In violation of § 1770(a)(5) by representing that goods or services have
- 3 characteristics and benefits that they do not have;
- 4 b. In violation of § 1770(a)(7) by representing that goods or services are of a
- 5 particular standard, quality, or grade, or that goods are of a particular style or
- 6 model, if they are of another;
- 7 c. In violation of § 1770(a)(14) by representing that a transaction confers or involves
- 8 rights, remedies, or obligations which it does not have or involve, or which are
- 9 prohibited by law; and
- 10 d. In violation of § 1770(a)(16) by representing that the subject of a transaction has
- 11 been supplied in accordance with a previous representation when it has not.

12 102. Plaintiff and the Subclass have suffered harm as a direct and proximate result of the

13 Google's violations of law and wrongful conduct.

14 103. On information and belief, Google continues to disseminate its users' search queries

15 to third parties and there is no indication that Google will stop this conduct in the future. Google's

16 unlawful and unfair business practices will continue to cause harm to Plaintiff and members of the

17 Subclass.

18 104. Under California Civil Code § 1780(a) & (b), Plaintiff and the Class seek injunctive

19 relief requiring Google to cease and desist the illegal conduct described herein, and any other

20 appropriate remedy for violations of the CLRA. For the sake of clarity, Plaintiff explicitly disclaims

21 any claim for damages under the CLRA at this time.

22 **COUNT III**

23 **(Violation of Cal. Bus. & Prof. Code § 17500 *et seq.*)**

24 **(on behalf of Plaintiff and the Subclass)**

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

26 106. The acts, omissions and practices of Google alleged herein include untrue or

27 misleading statements made in connection with the provision of services which were known, or

28 which by the exercise of reasonable care should have been known, to be untrue or misleading, in

violation of California Business & Professions Code § 17500 *et seq.* These untrue or misleading

statements include, but are in no way limited to, the following:

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- a. Representing that Google respects and protects the privacy of its users’ personal information;
 - b. Representing that Google’s security procedures strictly limit access to and use of users’ personal information;
 - c. Representing that Google only shares personal information in limited circumstances;
 - d. Representing that Google requires opt-in consent for the sharing of any sensitive personal information;
 - e. Representing that Google shares only aggregated, non-personal search query information with third parties;
 - f. Representing that Google does not share any information that could identify an individual user;
 - g. Representing that Google doesn’t sell user information to other companies;
 - h. Representing that Google does not publicly disclose the search queries entered into its search engine;
 - i. Representing that Google will keep private whatever information users communicate absent a compelling reason; and
 - j. Other untrue or misleading statements as alleged above.

20 107. Plaintiff and members of the California Subclass have suffered harm as a result of
21 Google’s violations, including suffering the public disclosure of their private information.

22 108. On information and belief, Google continues to disseminate its users’ search queries
23 to third parties and there is no indication that Google will stop this conduct in the future. Google’s
24 unlawful and unfair business practices will continue to cause harm to Plaintiff and members of the
25 Subclass.

26 109. Google’s unfair or deceptive practices occurred primarily and substantially in
27 California. Decisions concerning the retention and safeguarding the disclosure of user information
28 were made in California, Google maintains a substantial part of its computer systems in California,

1 and the disclosure of its Subclass users' information took place primarily and substantially in
2 California.

3 110. Pursuant to California Business & Professions Code § 17535, Plaintiff seeks an order
4 of this Court permanently enjoining Google from continuing to engage in the unfair and unlawful
5 conduct described herein. Plaintiff also seeks attorneys' fees and pursuant to California Code of
6 Civil Procedure § 1021.5, as well as such other and further relief as the Court deems appropriate.
7

8 **COUNT IV**
(Violation of Cal. Bus. & Prof. Code § 17200, *et seq.*)
(on behalf of Plaintiff and the Subclass)

9 111. Plaintiff incorporates the foregoing allegations as if fully set forth herein.
10

11 112. California's Unfair Competition Law ("UCL") protects both consumers and
12 competitors by promoting fair competition in commercial markets for goods and services. Cal. Bus.
& Prof. Code § 17200, *et seq.*

13 113. The UCL prohibits any unlawful, unfair or fraudulent business act or practice. A
14 business practice need only meet one of the three criteria to be considered unfair competition. An
15 unlawful business practice is anything that can properly be called a business practice and that at the
16 same time is forbidden by law.

17 114. As described herein, Google's nonconsensual disclosure of its users' search queries
18 contrary to Google's representations is a violation of the UCL.

19 115. Google has violated the "unlawful" prong of the UCL in that Google's conduct
20 violated the 18 U.S.C. § 2702(a)(1) and/or (a)(2), California Civil Code § 1750 *et seq.*, California
21 Business and Professions Code § 22575 *et seq.*, and California Business and Professions Code §
22 17500 *et seq.*

23 116. Google violated the fraudulent prong of the UCL by explicitly representing in its
24 Privacy Policy and elsewhere that it would not make users' personal information and search queries
25 available to any third party. Google used those misrepresentations to induce users to use Google's
26 search engine service.

27 117. Google violated the unfair prong of the UCL by gaining control over and divulging to
28 third parties its users' search queries without consent and under false pretenses.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

COUNT VI

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

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

127. 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.”

128. 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.”

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

130. 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.

131. 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.

132. 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.

22
23
24
25
26
27
28

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.

1 135. Google appreciates or has knowledge of said benefit.

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

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

7 **PRAYER FOR RELIEF**

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

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

13 B. Declare that Google's actions, as described herein, violate the Electronic
14 Communications Privacy Act (18 U.S.C. § 2702 *et seq.*), the California Unfair Competition Law
15 (Cal. Bus. & Prof. Code § 17200, *et seq.*), the California False Advertising Law (Cal. Bus. & Prof.
16 Code § 17500, *et seq.*), Cal. Bus. & Prof. Code § 22575 *et seq.*, the Consumer Legal Remedies Act
17 (Cal. Bus. & Prof. Code § 1750 *et seq.*), Cal. Civ. Code §§ 1572-73, constitute violation of the
18 common law and unjust enrichment;

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

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

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


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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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: October 25, 2010

Respectfully submitted,
NASSIRI & JUNG LLP



Kassra P. Nassiri
Attorneys for Plaintiff


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: October 25, 2010

Respectfully submitted,
NASSIRI & JUNG LLP



Kassra P. Nassiri
Attorneys for Plaintiff