

1 KASSRA P. NASSIRI (215405)
(knassiri@nassiri-jung.com)
2 CHARLES H. JUNG (217909)
(cjung@nassiri-jung.com)
NASSIRI & JUNG LLP
3 47 Kearny Street, Suite 700
San Francisco, California 94108
4 Telephone: (415) 762-3100
Facsimile: (415) 534-3200
5

6 MICHAEL J. ASCHENBRENER (277114)
mja@aschenbrenerlaw.com
7 ASCHENBRENER LAW, P.C.
795 Folsom Street, First Floor
8 San Francisco, California 94107
Telephone: (415) 813-6245
9 Fax: (415) 813-6246

10 ATTORNEYS FOR PLAINTIFFS AND THE PUTATIVE CLASS

11 **UNITED STATES DISTRICT COURT**
12 **NORTHERN DISTRICT OF CALIFORNIA**
13 **SAN JOSE DIVISION**

14 PALOMA GAOS and ANTHONY) Case No. 5:10-CV-4809-EJD
15 ITALIANO, individually and on behalf of all)
16 others similarly situated,) **SECOND AMENDED COMPLAINT**
Plaintiff,)
17)
18 v.) CLASS ACTION
19) JURY TRIAL DEMANDED
GOOGLE INC., a Delaware corporation,)
20 Defendant.) Original Complaint filed: October 25, 2010
21)
22
23
24
25
26
27
28

1 Plaintiffs Paloma Gaos and Anthony Italiano bring this suit on behalf of themselves
2 and all others similarly situated, and make the following allegations on information and
3 belief, except as to allegations pertaining to Plaintiffs, which are based on their personal
4 knowledge:

5 INTRODUCTION

6 1. Plaintiffs bring this class action complaint against Google Inc. (“Google”) for
7 intentionally, systematically and repeatedly divulging its users’ search queries to third
8 parties. This practice adversely impacts billions of searches conducted by millions of
9 consumers.

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

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

23 4. In many instances, the information contained in disclosed search queries does
24 not directly identify the Google user. Through the reidentification (explained below) or
25 deanonymizing of data, however, the information contained in search queries can and, on
26 information and belief, are associated with the actual names of Google users. Computer
27
28

1 science academics and privacy experts are calling for the reexamination of privacy concerns
2 in light of the growing practice and power of reidentification.

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

9 6. Moreover, in October 2011, Google confirmed that it is, in effect, selling
10 individual user search queries to advertisers. In October 2011, Google started proactively
11 scrubbing user search queries from the information it passes on to third parties when some
12 users click on regular, organic search results, but would continue sending search queries to
13 third parties when all users click on paid listings. While this is, in a way, a small win for
14 privacy advocates, it also demonstrates just how valuable the search queries are to Google
15 and others: Google no longer gives away this precious data for free, but will do so when it
16 gets paid for it.

17 **PARTIES**

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

20 8. Plaintiff Anthony Italiano is a resident of Pasco County, Florida. Plaintiff has
21 at all material times been a registered Google Accounts user and a user of Google's search
22 engine services.

23 9. Defendant Google Inc. ("Google") is a Delaware corporation that maintains
24 its headquarters in Mountain View, Santa Clara County, California. Google conducts
25 business throughout California and the nation from California. Google makes and
26 implements all relevant decisions, including those at issue in this case, in California. Its
27 Terms of Service and Privacy Policy were decided on and implemented in California.
28

JURISDICTION AND VENUE

10. 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, and (c) in its Terms of Service, to which all users of Google Search, including Plaintiffs, must assent, Google consents to the personal jurisdiction of this Court:

The laws of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to these terms or the Services. All claims arising out of or relating to these terms or the Services will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts.

11. 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.

12. 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.

INTRADISTRICT ASSIGNMENT

13. Pursuant to Civil Local Rule 3-2(e), this case shall be assigned to the San Jose Division.

STATEMENT OF FACTS

A. Google's Search Business

1. Google's Dominance in Search

14. "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.

1 When using a search engine, users formulate a search query using keywords and phrases
2 reflecting the information sought by the user. The search engine then matches the search
3 query with websites matching the query and provides a list of those matching websites to the
4 user. The user clicks on the link in the resulting list and is redirected to the website
5 containing the sought-after information.

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

10 16. Google generates substantial profits from selling advertising. The revenue it
11 generates is derived from offering search technology and from the related sale of advertising
12 displayed on its site and on other sites across the web. On information and belief, over 99%
13 of Google's revenue is derived from its advertising programs, with total advertising revenues
14 estimated at \$28 billion in 2010 and \$36.5 billion in 2011. Google has implemented various
15 innovations in the online advertising market that helped make it one of the biggest
16 advertising platforms in the world.

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

24 18. Using technology from its wholly-owned subsidiary DoubleClick, Google can
25 also determine user interests and target advertisements so they are relevant to their context
26 and the user that is viewing them. Google's Analytics product allows website owners to track
27 where and how people use their website, allowing in-depth research to get users to go where
28

1 you want them to go.

2 19. Third-party search engine optimization (“SEO”) companies help businesses
3 design their websites so that users conducting internet search using search engines like
4 Google get search results containing their business at or near the top of the search results
5 page. SEOs accomplish this task by ensuring that a business’s relevant pages are designed to
6 work with Google’s search algorithms. Google has a symbiotic relationship with SEOs.
7 Google wants relevant results at the top of their search results page, and SEOs want their
8 customers’ relevant webpages to appear at the top of Google’s search results. To the extent
9 that SEOs are successful in getting their clients’ relevant pages to appear at or near the top of
10 Google’s search results page, users are more likely to return to Google next time they want to
11 search for information on the internet. And the more people use Google for search, the more
12 revenue Google derives from its advertising business.

13 2. Google’s Privacy Promises

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

19 21. Google has always recognized that user trust is paramount to its search
20 business success. To that end, Google adopted “Don’t be evil” as its motto, and Google states
21
22

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

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

1 that its Code of Conduct is one of the ways it puts that motto into practice.³ Google's Code of
 2 Conduct recognizes that it is "asking users to trust [it] with their personal information.
 3 Preserving that trust requires that each of us respect and protect the privacy of that
 4 information. Our security procedures strictly limit access to and use of users' personal
 5 information."⁴

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

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

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

26 ³ Google's Code of Conduct, <http://investor.google.com/corporate/code-of-conduct.html> (last
 27 visited April 26, 2012).

28 ⁴ *Id.*

⁵ Google's October 14, 2005 Privacy Policy,
http://www.google.com/intl/en/privacy_archive_2005.html (last visited April 26, 2012).

1
2 23. In October 2010, Google defined in its Privacy Center FAQ “Personal
3 information” as “information that [the user] provide[s] to us which personally identifies you,
4 such as your name, email address or billing information, or other data which can be
5 reasonably linked to such information by Google” and “Sensitive Information” as
6 “information we know to be related to confidential medical information, racial or ethnic
7 origins, political or religious beliefs or sexuality and tied to personal information. As of April
8 2012, Google no longer defines “Personal Information” at all in its Privacy Center FAQ.

9 24. Google also stated in its October 14, 2005 Privacy Policy that “We may share
10 with third parties certain pieces of *aggregated, non-personal information*, such as the number
11 of users who searched for a particular term, for example, or how many users clicked on a
12 particular advertisement. Such information does not identify you individually.”⁶ Google
13 defined “aggregated, non-personal information” as “information that is recorded about users
14 and *collected into groups* so that it no longer reflects or references an individually
15 identifiable user.”⁷

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

20 26. On March 1, 2012, Google implemented a new, singular privacy policy for all
21 Google products.⁸ While the new policy has broad implications for how Google shares user
22 data internally, Google makes the following representations regarding how it shares data with
23

24 ⁶ Google’s October 14, 2005 Privacy Policy, *supra*, n.5 (emphasis supplied).

25 ⁷ Google’s October 14, 2005 Privacy FAQs,
26 http://web.archive.org/web/20070113102317/www.google.com/intl/en/privacy_faq.html (last
27 visited October 24, 2010) (emphasis supplied).

28 ⁸ <http://www.google.com/intl/en/policies/privacy/> (last visited April 26, 2012).

third parties:⁹

Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances apply:

- **With your consent**

We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any [sensitive personal information](#).

- **With domain administrators**

If your Google Account is managed for you by a [domain administrator](#) (for example, for Google Apps users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

- view statistics regarding your account, like statistics regarding applications you install.
- change your account password.
- suspend or terminate your account access.
- access or retain information stored as part of your account.
- receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
- restrict your ability to delete or edit information or privacy settings.

Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

- **For legal reasons**

We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

⁹ *Id.*

- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share aggregated, non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

27. Google makes similar representations about the privacy of its users' search queries on its video "Privacy Channel" on YouTube. In October 2010, Google showcased a video on its Privacy Channel that starts with the statement "at Google, we make privacy a priority in everything we do."¹⁰ Google also stated in another privacy video from 2010 that "We don't sell user information to other companies."¹¹ In a 2011 video on its Privacy Channel called "What is a search log?," Google explains that it keeps logs of user search queries for a short period of time, but does not disclose that it shares those search logs with any third parties.¹²

28. In 2010, 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

¹⁰ Google's Privacy Principles, <http://www.youtube.com/watch?v=5fvL3mNt1g> (January 26, 2010) (last visited October 25, 2010) (not available as of April 26, 2012).

¹¹ Google's Privacy Principles, <http://googleblog.blogspot.com/2010/01/googles-privacyprinciples.html> at 1:44 (January 27, 2010, 7:00 p.m.) (last visited October 23, 2010) (not available as of April 26, 2012).

¹² http://www.youtube.com/watch?v=PIdfBUm0CPo&list=UUsB_OLJA28Nc-47BihG2_Ww&index=6&feature=plcp (October 18, 2011) (last visited April 26, 2012).

procedures, and stronger procedural protections relating to third party access to individuals' information."¹³ 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."¹⁴

3. Google Admits Search Queries Contain Sensitive, Personal Data

29. In 2006, the Department of Justice sought to compel Google to produce thousands of users' individual search queries.¹⁵ 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 who entered the text string into the search engine, or the computer from which the text string was entered."¹⁶

30. 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

¹³ Google's April 14, 2010 letter to Donald S. Clark, <http://www.scribd.com/doc/30196432/FTCRoundtable-Comments-Final> (last visited October 24, 2010).

¹⁴ *Id.*

¹⁵ *Gonzales v. Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW).

¹⁶ *Id.* at 682.

1 optimization issues at Google, stated as follows:¹⁷

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

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

- 20 • Google users trust that when they enter a search query into a Google search
- 21 box, not only will they receive back the most relevant results, but that Google
- 22 will keep private whatever information users communicate absent a
- 23 compelling reason.¹⁸
- 24 • The privacy and anonymity of the service are major factors in the attraction of
- 25 users – that is, users trust Google to do right by their personal information and
- 26 to provide them with the best search results. If users believe that the text of
- 27 their search queries into Google's search engine may become public
- 28 knowledge, it only logically follows that they will be less likely to use the
- service.¹⁹

25 ¹⁷ Declaration of Matt Cutts at 9, *Gonzales v. Google*, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW).

26 ¹⁸ Google's Opposition to the Government's Motion to Compel at 1, *supra*, n.12.

27 ¹⁹ *Id.* at 18.

- 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.”²⁰

32. In its order²¹ 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.

33. 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

²⁰ *Id.*

²¹ *Gonzales*, 234 F.R.D. at 687.

by 658,000 AOL users over a three-month period.²² That data included search queries revealing names, addresses, local landmarks, medical ailments, credit card numbers and social security numbers.²³

34. 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.”²⁴

35. 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 crosssession identifiers (cookies) included in the dataset.²⁵ 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.”²⁶

36. 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...”²⁷

²² Complaint at ¶ 16, *Doe I v. AOL LLC*, 2010 WL 2524494 (N.D. Cal. June 23, 2010) (No. C-06-5866-SBA).

²³ *Id.* at ¶ 18.

²⁴ 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>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

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

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

13 It's funny that we talk about the company being more transparent.
14 But there are many things inside our company that are important
15 that we don't share with everyone, starting with everyone's queries
16 and all the information that that implies. I've always worried that
17 the query stream was a fertile ground for governments to randomly
18 snoop on people [for example]. We had a case where we were only
19 a secondary party, where the government gave us a subpoena,
20 which was in our view, over-broad. And this over-broad subpoena
21 we fought in federal court – one of the great things about the
22 American system is that you can actually have a judge make an
23 impartial decision. And the judge ruled largely in our favor. So
24 that's an example of how strongly we take this point.²⁸

25 4. A Brief Primer on "Referrer Headers"

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

29 39. The HTTP Referrer function is a standard web browser function, provided by
30 standard web browsers since the HTTP 1.0 specification in May 1996.²⁹ When an internet

31 ²⁸ Conversation with Eric Schmidt hosted by Danny Sullivan,
32 <http://www.google.com/press/podium/ses2006.html> (last visited April 26, 2012).

33 ²⁹ <http://www.w3.org/Protocols/rfc1945/rfc1945>

1 user visits a web page using their computer or mobile device, every major web browser (e.g.,
 2 Internet Explorer, Firefox, Chrome, Safari) by default reports the last page that the user
 3 viewed before clicking on a link and visiting the current page — that is, the page that
 4 “referred” them to the current page. This information is transmitted in the HTTP Referrer
 5 Header.

6 40. The current version of the publicly-available HTTP specification, RFC
 7 2616,³⁰ provides for HTTP Referrer Headers in its provision 14.36.³¹ It is well known that if
 8 a site places confidential information, such as a username, in a URL, then the site risks
 9 releasing this information whenever a user clicks a link to leave the site. Indeed, the HTTP
 10 specification specifically flags this risk; in section 15.1.3, the HTTP specification advises
 11 developers of substantially the same problem: “Authors of services which use the HTTP
 12 protocol SHOULD NOT use GET based forms for the submission of sensitive data, because
 13 this will cause this data to be encoded in the REQUESTURI.”³²

14 41. While the HTTP Referrer function is a standard web browser function, Google
 15 ultimately determines whether to send referrer header information to third parties and
 16 exercises control over the content of the URL that is referred by this function to the owner of
 17 the destination web page.

18 5. Google Transmits Individual User Search Queries to Third Parties

19 42. Since the service’s launch, and continuing to this day, Google’s search engine
 20 has included its users’ search terms in the URL of the search results page. Thus, for example,
 21 a search for “abortion clinics in Indianapolis” would return a page with a URL similar to
 22 <http://www.google.com/search?q=abortion+clinics+in+Indianapolis>.

23 43. Because the search terms are included in the search results URL, when a
 24 Google user clicks on a link from Google’s search results page, the owner of the website that

25 ³⁰ <http://www.w3.org/Protocols/rfc2616/rfc2616.html>

26 ³¹ <http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.36>

27 ³² <http://www.w3.org/Protocols/rfc2616/rfc2616-sec15.html#sec15.1.3>

1 the user clicks on will receive from Google the user's search terms in the Referrer Header.

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

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

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

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

16 47. On September 6, 2010, a former FTC employee, Christopher Soghoian, filed a
17 complaint with the FTC accusing Google of not adequately protecting the privacy of
18 consumers' search queries. Much of the following information comes from Mr. Soghoian's
19 complaint.³³

20 48. Starting approximately in November 2008, Google began to test a new
21 method of delivering search results that uses advanced AJAX (Asynchronous JavaScript and
22 XML) technologies.³⁴ AJAX is one of the key pillars of the Web 2.0 experience.³⁵ This pilot

23
24 ³³ *In the Matter of Google, Inc.*, FTC Complaint, available at
<http://online.wsj.com/public/resources/documents/FTCcomplaint100710.pdf>.

25 ³⁴ Jesse James Garrett, *Ajax: A New Approach to Web Applications* (February 18, 2005),
26 <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").

27 ³⁵ Tim O'Reilly, *What Is Web 2.0 Design Patterns and Business Models for the Next*
28

1 was initially deployed in the Netherlands,³⁶ but in subsequent months, was observed by users
2 in other countries.

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

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

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

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

- 15 • “I’m seeing hundreds of these empty google referrers today and wondered
16 what was going on.”³⁷
- 17 • “This means organic searches from Google will now show up as just
18 <http://www.google.com/>, with no search parameters. In other words, no
19 analytics app can track these searches anymore. I started noticing lots of hits
20 from just ‘<http://www.google.com/>’ recently in our own search logs. I thought
21 maybe it was just a bug with Clicky. But then one of our users contacted me

22 *Generation of Software* (September 30, 2005), [http://oreilly.com/web2/archive/what-is-web-](http://oreilly.com/web2/archive/what-is-web-20.html)
23 20.html (“AJAX is also a key component of Web 2.0 applications such as Flickr, now part of
24 Yahoo!, 37signals’ applications basecamp and backpack, as well as other Google
25 applications such as Gmail and Orkut.”)

26 ³⁶ Ulco, “Google Search in AJAX?!” (November 19, 2008),
27 <http://www.ulco.nl/gibberish/googlesearch-in-ajax>.

28 ³⁷ Posting of sorabji.com to Clicky.blog, [http://getclicky.com/blog/150/googles-new-ajax-](http://getclicky.com/blog/150/googles-new-ajax-poweredsearch-results-breaks-search-keyword-tracking-for-everyone)
poweredsearch-results-breaks-search-keyword-tracking-for-everyone (February 03 2009,
1:05 p.m.).

about this article, and my jaw about broke from hitting the floor so hard.”³⁸

- “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.”³⁹

52. 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.⁴⁰

53. 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.⁴¹

³⁸ Clicky.blog, <http://getclicky.com/blog/150/googles-new-ajax-powered-search-results-breakssearch-keyword-tracking-for-everyone> (February 03, 2009, 9:50 a.m.).

³⁹ Posting of Michael VanDeMar to Smackdown!, What Will *Really* Break If Google Switches To AJAX...?, <http://smackdown.blogspot.com/2009/02/02/what-will-really-break-if-googleswitches-to-ajax/> (February 2, 2009, 11:26 a.m.).

⁴⁰ 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-termtracking-16431> (February 3, 2009, 5:41 p.m.) (emphasis supplied).

⁴¹ 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).

1
2 54. In March 2009, Google again began to test technology that unintentionally
3 caused the users' search terms to be stripped from the referrer header transmitted to web
4 sites. The following is an example of the format of the new URL that was being tested in
5 March 2009:

6 http://www.google.com/url?q=http://www.webmd.com&ei=in66ScnjBtKgtwfn0LTiDw&sa=X&oi=smap&resnum=1&ct=result&cd=1&usg=AFQjCNF9RdVC6vXBFOYvdialS_ZE_BMu8g

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

11 Occasionally you will see these Google redirects in the normal
12 [search engine results pages] as well, although usually not. The
13 thing is, I was seeing them on every search I performed. It struck
14 me as odd, until I suddenly realized that every search was being
15 done via AJAX.⁴²

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

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

23 **The solution to the referrer problem will be coming online in
24 the future. It uses a JavaScript-driven redirect that enables us
25 to pass the redirect URL as the referrer. This URL will contain
26 a 'q' param that matches the user's query.**⁴³

27 ⁴² Posting of Michael VanDeMar to Smackdown!, Google Re-initiates Testing of AJAX
28 SERP's With Faulty Proposed Fix,
29 <http://smackdown.blogspot.com/2009/03/13/google-re-initiate-testing-of-ajax-serps-with-faulty-proposed-fix/> (March 13, 2009, 11:14 a.m.).

⁴³ Posting of Matt Cutts to Smackdown!, supra, n.39,

57. 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:

<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.⁴⁴

58. 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.

<http://smackdown.blogsblogsblogs.com/2009/03/13/google-re-initiates-testing-of-ajax-serps-withfaulty-proposed-fix/> (March 17, 2009, 10:10 a.m.) (emphasis added).

⁴⁴ 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-togooglecom-search.html> (April 14, 2009, 2:50 p.m.).

1 59. The new redirection tool also leaks data to web site administrators that had
 2 never before been available to anyone but Google: The item number of the search result that
 3 was clicked non (e.g., the 3rd link or 5th link from the search results page).⁴⁵ The leakage of
 4 this additional information was confirmed by Matt Cutts, which he described as a benefit to
 5 web site administrators:

6 I think if you do experiments, you'll be able to confirm your
 7 speculation ... **I think this is awesome for webmasters--even**
 8 **more information than you could glean from the previous**
 9 **referrer string.**⁴⁶

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

13 [T]here is a change on the horizon and it's only a very small
 14 percentage of users right now, but I think that it probably will grow
 15 and it will grow over time where Google's referrer, that is
 16 whenever you do a Google search and you click on a result, you go
 17 to another website and your browser passes along a value called a
 18 referrer. That referrer 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**
 22 **got a lot of people frustrated**, but the google.com/search, **the new**
 23 **Google referrer string will have the query embedded in it.**

24 And there's a really interesting tidbit that not everybody knows,
 25 which is--it also has embedded in that referrer string a pretty good

26 ⁴⁵ 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 ⁴⁶ 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 added).

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."⁴⁷

61. 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:

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.⁴⁸

⁴⁷ 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).

⁴⁸ 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.).

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

2 Hey everybody, I asked folks who would know about this. It turns
3 out there was an issue a couple weeks ago where some code got
4 refactored, and the refactoring affected referrers for links opened in
5 a new tab or window. Right now the team is **expecting to have a
6 fix out in the next week** or so. Hope that helps.⁴⁹

7 63. On or about May 21, 2010, Google introduced an encrypted search service at
8 <https://www.google.com>.⁵⁰ By using the encrypted search service, Google would no longer
9 pass along search queries via Referrer Headers to unencrypted search links. On or about June
10 25, 2010, Google moved the encrypted search service to <https://encrypted.google.com>.

11 64. Later, on or about October 18, 2011, Google announced a change in policy for
12 how it handled search queries embedded in Referrer Headers.⁵¹ According to its new policy,
13 Google would proactively scrub out any and all search queries from all searches performed
14 by users who were logged in to any Google service, such as Gmail or Google Docs, before
15 sending the Referrer Headers to the sites in the results on which users would click. Thus,
16 when logged-in users would click on a search result link (whether the results link is
17 encrypted or unencrypted), Google would no longer pass on the search queries used to find
18 those results.

19 65. For users not logged in, Google would still transmit search queries via
20 Referrer Headers to the results sites on which users would click, unless those users entered
21 the search at <https://encrypted.google.com>.

22 66. Moreover, the new policy only applies to organic sites. For clicks on paid

23
24 ⁴⁹ Posting of Matt Cutts to Webmaster World, *supra*, n.45 (July 13, 2010, 9:46 p.m.)
(emphasis added).

25 ⁵⁰ <http://googleblog.blogspot.com/2010/05/search-more-securely-with-encrypted.html> (last
26 visited April 26, 2012).

27 ⁵¹ <http://googleblog.blogspot.com/2011/10/making-search-more-secure.html> (last visited
28 April 26, 2012).

links or advertisements, Google would still pass on the search queries.

67. If nothing else, Google's new policy regarding search queries demonstrates two things: 1) Google is fully capable of determining independently whether to transmit search queries to third parties—transmitting search queries embedded within Referrer Headers is not just how the Internet works; and, 2) Google is now effectively selling search queries to paying advertisers. Stated differently, part of what paying advertisers pay for when they buy AdWords are the search queries users enter.

7. The Science of Reidentification

68. "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 Anonymization" published in the UCLA Law Review in August of 2010.⁵²

69. 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

⁵² 57 UCLA L. REV. 1701 (2010).

easier to discover and reveal.⁵³

70. 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.⁵⁴

71. 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.⁵⁵

72. 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

⁵³ *Id.* at *7-8.

⁵⁴ *Id.* at *17.

⁵⁵ *Id.*

1 history has it been so easy to peer into the private diaries of so many people. Some
2 researchers call this the “age of self-revelation.”⁵⁶

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

5 The accretion problem is this: once an adversary has linked two
6 anonymized databases together, he can add the newly linked data
7 to his collection of outside information and use it to help unlock
8 other anonymized databases. Success breeds further success . . .
9 *once any piece of data has been linked to a person’s real identity,*
10 *any association between this data and a virtual identify breaks*
11 *the anonymity of the latter. This is why we should worry even*
12 *about reidentification events that seem to expose only non-*
13 *sensitive information, because they increase the linkability of*
14 *data, and thereby expose people to potential future harm.*⁵⁷

12 74. The accretive reidentification problem is exacerbated by the growing
13 prevalence of internet “data brokers.” The buying and selling of consumer data is a
14 multibillion-dollar, unregulated business that’s growing larger by the day.⁵⁸ Data is
15 increasingly bought, sold and resold by data brokers, which amplifies the accretion problem.
16 Advancements in computer science, data storage and processing power, and data accretion by
17 data brokers make it much more likely that an adversary could link at least one fact to any
18 individual and blackmail, discriminate against, harass, or steal the identity of that person.

19 75. On October 25, 2010, the Wall Street Journal reported that a highly-
20 sophisticated data broker, RapLeaf Inc. is accomplishing accretive reidentification of
21 “anonymous” data with astonishing success.⁵⁹ According to the report, RapLeaf has been
22 gathering data, including user names and email addresses, from numerous sources across the
23

24 ⁵⁶ *Id.* at *17-18.

25 ⁵⁷ *Id.* at *29 (emphasis added).

26 ⁵⁸ Rick Whiting, *Data Brokers Draw Increased Scrutiny* (July 10, 2006),
<http://www.informationweek.com/news/global-cio/showArticle.jhtml?articleID=190301136>.

27 ⁵⁹ Emily Steele, *A Web Pioneer Profiles Users by Name* (October 25, 2010), available at
<http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html>.

1 internet. Using accretive reidentification techniques, RapLeaf is able to cross-index
 2 “anonymous” data with email addresses and thereby associate real names with Web-
 3 browsing habits and highly-personal information scraped from social network sites such as
 4 Facebook. By 2009, RapLeaf had indexed more than 600 million unique email addresses, and
 5 was adding more at a rate of 35 million per month.

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

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

19 77. One type of anonymization practice is called “release-and-forget,” in which
 20 the data administrator will release records, and then forgets, meaning she makes no attempt
 21 to track what happens to the records after release.⁶⁰ To protect the privacy of the users in the
 22 released data, prior to releasing the data, the administrator will single out identifying
 23 information and either strip that information from the database, or modify it to make it more
 24
 25
 26

27 ⁶⁰ Ohm, supra, n.47 at *9-10.
 28

1 general and less specific to any individual.⁶¹ Many of the recent advances in the science of
2 reidentification target release-and-forget anonymization in particular.⁶²

3 78. Google's transmission of search queries is a type of piecemeal "release-and-
4 forget" anonymization.⁶³ Google transmits a single user search query each time a Google
5 user clicks on a link in Google's search results page. Over the course of just one day, on
6 information and belief, Google transmits millions of search queries to third parties. Google
7 will likely argue that search query information alone contains no personally-identifiable
8 information. Such an argument is practically equivalent to the data administrator who
9 "anonymizes" data before releasing it to the outside world. But, as repeatedly demonstrated,
10 easy reidentification of "anonymous" highlights the flaws in this thinking.

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

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

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

25 ⁶¹ *Id.* at *11-12.

26 ⁶² *Id.* at *10.

27 ⁶³ *Id.* at *9.

generally considered personal information.”⁶⁴ 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.⁶⁵

82. 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 engine provider ... can also be accomplished by other means, based on cookies or other distinguishing characteristics, such as individual IP addresses.”⁶⁶

83. 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

⁶⁴ 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>.

⁶⁵ Ohm, *supra*, n.47 at *41.

⁶⁶ 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.

1 and other information, and allow websites to recognize the user or computer visiting their
 2 site. In its response to Congressman Barton, Google wrote that “online ad-serving technology
 3 can be used by advertisers to serve and manage ads across the web ... the ad server sets a
 4 cookie on the user’s computer browser when the user views an ad served through the ad
 5 server. That cookie may be read in the future when the ad server serves other ads to the same
 6 browser.”⁶⁷ An ad serving company with any substantial market share would thus be able to
 7 readily link the search queries that Google provides to the IP addresses or cookies of internet
 8 users visiting the websites they serve.

9 **B. Google Accounts**

10 84. In addition to search, Google operates many services that require users to
 11 register for Google Accounts. Google Accounts grant access to services such as Gmail,
 12 Google Docs, and Google+, among others. As part of the registration process for a Google
 13 Account, each user must provide Google with an email address.

14 **FACTS RELATING TO PLAINTIFFS**

15 **A. Paloma Gaos**

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

21 86. During all time periods in which Google was transmitting user search queries
 22 to third parties, Plaintiff Gaos conducted numerous searches, including “vanity searches” for
 23 her actual name and the names of her family members, and clicked on links on her Google
 24 search results pages.

25 87. As a result, Google transmitted Plaintiff Gaos’s full search queries to third
 26

27 ⁶⁷ Letter from Davidson to Barton, *supra*, n.58 at 15.
 28

1 parties by sending the URLs containing her search queries to third party websites that
2 appeared in Plaintiff Gaos's Google search results page and which Plaintiff Gaos clicked on a
3 link.

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

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

10 **B. Anthony Italiano**

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

16 91. Plaintiff Italiano has also had a Google Account since at least January 2008.

17 92. During all time periods in which Google was transmitting user search queries
18 to third parties, including the time period from July 2010 to August 2011, Plaintiff Italiano
19 conducted numerous searches on Google's unencrypted search service, including:

- 20 a. His name + his home address;
- 21 b. His name + bankruptcy;
- 22 c. His name + foreclosure proceedings;
- 23 d. His name + short sale proceedings;
- 24 e. His name + Facebook; and,
- 25 f. His name + the name of his then soon-to-be ex-wife + forensic accounting.

26 93. These searches and the timeframe during which he conducted them are
27 particularly memorable to Plaintiff Italiano because it was during this time that he was going
28

1 through formal divorce proceedings. Moreover, many of his searches related directly or
 2 indirectly to his divorce proceedings—exactly the sort of personal, confidential searches that
 3 he did not want disclosed to third parties without his knowledge or consent, and exactly the
 4 sort of personal, confidential searches Google described to the federal government in the
 5 *Gonzales* matter.

6 94. As a result, Google transmitted Plaintiff Italiano’s full search queries to third
 7 parties by sending the URLs containing his search queries to third party websites that
 8 appeared in Plaintiff Italiano’s Google search results page and which Plaintiff Italiano
 9 clicked on a link.

10 95. In other words, when Plaintiff Italiano clicked on each link on his Google
 11 search results pages, the owner of the destination website that Plaintiff clicked on received
 12 from Google Plaintiff Italiano’s search terms through the Referral Header function.

13 96. As a result, Plaintiff Italiano has suffered actual harm in the form of Google’s
 14 unauthorized and unlawful dissemination of Plaintiff Italiano’s search queries, which
 15 sometimes contained sensitive personal information, to third parties.

16 CLASS ALLEGATIONS

17 97. Pursuant to Rules 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil
 18 Procedure, Plaintiffs Gaos and Italiano bring Count I (ECPA) on behalf of themselves as
 19 individuals and all other persons in the following similarly situated class:

20 *All persons in the United States with a Google Account who, at any*
 21 *time between October 25, 2006 and October 17, 2011 during*
 22 *which Google was transmitting search queries to search results*
 23 *links via referrer headers, submitted a search query at*
 24 *http://www.google.com and clicked on any link displayed by*
 25 *Google in its search results (the “ECPA Class”). Excluded from*
 26 *the Class are Google, its officers and directors, legal*
 27 *representatives, successors or assigns, any entity in which Google*
 28 *has or had a controlling interest, the judge to whom this case is*
assigned and the judge’s immediate family.

1 98. Pursuant to Rules 23(a) and 23(b)(3), Plaintiff Italiano also brings Counts II-
2 IV (state law claims) on behalf of himself individually and all other persons in the following
3 similarly situated class:

4 *All persons in the United States with a Google Account who, at any*
5 *time between October 25, 2006 and October 17, 2011 during*
6 *which Google was transmitting search queries to search results*
7 *links via referrer headers, submitted a search query at*
8 *http://www.google.com and clicked on any link displayed by*
9 *Google in its search results* (the “State Law Class”). Excluded
10 from the Class are Google, its officers and directors, legal
11 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.

12 99. Pursuant to Rules 23(a) and Rule 23(b)(2), Plaintiff Italiano also brings Count
13 III (the UCL) on behalf of himself individually and all other persons in the following
14 similarly situated class expressly seeking injunctive relief only:

15 *All persons in the United States who, at any time after October 25,*
16 *2006 and during which time Google was transmitting search*
17 *queries to search results links via referrer headers, submitted a*
18 *search query at http://www.google.com and clicked on any link*
19 *displayed by Google in its search results* (the “Injunctive Relief
20 Class”). Excluded from the Class are Google, its officers and
21 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.

22
23 100. The Classes are each composed of numerous people, whose joinder in this
24 action would be impracticable. The disposition of their claims through this class action will
25 benefit Class members, the parties and the courts. Upon information and belief, Google’s
26 search engine has been used by hundreds of millions of users during the relevant time period.

27 101. There is a well-defined community of interest in questions of law and fact
28

1 affecting the Classes. These questions of law and fact predominate over individual questions
 2 affecting individual Class members, including, but not limited to, the following:

- 3 a. whether and to what extent Google has disclosed its users' search queries to
- 4 third parties, and whether the disclosure is ongoing;
- 5 b. whether Google's conduct described herein violates Google's Privacy Policy
- 6 and representations to Plaintiffs and the Classes;
- 7 c. whether Google's conduct described herein violates the Electronic
- 8 Communications Privacy Act, 18 U.S.C. § 2702 et seq.;
- 9 d. whether Google's conduct described herein constitutes a breach of contract;
- 10 e. whether Google is unjustly enriched as a result of its conduct described
- 11 herein; and
- 12 f. whether Plaintiffs and members of the Classes are entitled to injunctive and
- 13 other equitable relief.

14 102. Google has engaged, and continues to engage, in a common course of conduct
 15 giving rise to the legal rights sought to be enforced by Plaintiffs and the Classes. Similar or
 16 identical statutory and common law violations, business practices and injuries are involved.
 17 Individual questions, if any, pale by comparison to the numerous common questions that
 18 dominate.

19 103. The injuries, actual and imminent, sustained by Plaintiffs and the Classes
 20 flow, in each instance, from a common nucleus of operative facts. In each case, Google
 21 caused or permitted unauthorized communications of private and personally-identifying
 22 information to be delivered to third parties without adequate or any notice, consent or
 23 opportunity to opt out.

24 104. Given the similar nature of the Classes members' claims and the absence of
 25 material differences in the statutes and common laws upon which the Classes members'
 26 claims are based, a nationwide class action will be easily managed by the Court and the
 27 parties.

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

106. Plaintiffs' claims are typical of those of the Classes as all members of the Classes are similarly affected by Google's uniform and actionable conduct as alleged herein.

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

108. Plaintiffs will fairly and adequately protect the interests of the Classes, and has retained counsel competent and experienced in class action litigation. Plaintiffs have no interests antagonistic to, or in conflict with, the Classes that Plaintiffs seek to represent.

109. Plaintiffs reserve the right to revise the above class definitions based on facts learned in discovery.

COUNT I

Violation of the ECPA

(on behalf of Plaintiffs individually and the ECPA Class)

110. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

111. 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 part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...” 18 U.S.C. § 2510(12).

112. 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

1 communication. The definition thus includes all aspects of the communication itself. No
 2 aspect, including the identity of the parties, the substance of the communication between
 3 them, or the fact of the communication itself, is excluded. The privacy of the communication
 4 to be protected is intended to be comprehensive.

5 113. Pursuant to the ECPA, “electronic storage” means any “temporary storage of a
 6 wire or electronic communication incidental to the electronic transmission thereof.” 18
 7 U.S.C. § 2510(17)(A).

8 114. Pursuant to the ECPA, Google operates an “electronic communications
 9 service” as defined in 18 U.S.C. § 2510(15). Pursuant to the Stored Communications Act of
 10 1986 (the “SCA”), Google also provides a “remote computing service” to the public. 18
 11 U.S.C. § 2711(2).

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

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

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

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

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

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

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

26 116. As alleged herein, by disclosing the private search queries of Plaintiffs and
 27 members of the ECPA Class without authorization, Google has knowingly divulged the
 28

1 contents of communications of Plaintiffs and members of the ECPA Class while those
2 communications were in electronic storage on its service, in violation of 18 U.S.C. §
3 2702(a)(1).

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

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

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

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

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

23 **COUNT II**

24 **Breach of Contract**

25 **(on behalf of Plaintiff Italiano and the State Law Class)**

26 122. Plaintiff Italiano incorporates by reference the foregoing allegations.

27 123. The provisions of Google's Terms of Service, which expressly incorporate its
28

1 Privacy Policy, constitute a valid and enforceable contract between Plaintiff and the Class on
2 the one hand, and Google on the other.

3 124. Under the Terms of Service and Privacy Policy, Plaintiff Italiano and the State
4 Law Class agreed to use Defendant's services and transmit sensitive personally-identifiable
5 information to Google in exchange for Google's promise that it would not share that personal
6 information with third parties without users' authorization.

7 125. Google materially breached the terms of its Terms of Service and Privacy
8 Policy through its unlawful conduct alleged herein, including the disclosure of Plaintiff
9 Italiano's and the State Law Class's private search queries to third parties.

10 126. As a result of Google's misconduct and breach of Google's Terms of Service
11 and Privacy Policy described herein, Plaintiff Italiano and the State Law Class suffered
12 injury. Plaintiff Italiano, on behalf of himself and the State Law Class, seeks damages from
13 Google in an amount to be determined at trial.

14 **COUNT III**

15 **Violation of Cal. Bus. & Prof. Code § 17200, Unfair Competition Law**

16 **(on behalf of Plaintiff Italiano individually, the State Law Class,**

17 **and the Injunctive Relief Class)**

18 127. Plaintiff Italiano incorporates by reference the foregoing allegations.

19 128. Cal. Bus. & Prof. Code § 17200 proscribes unfair business competition and
20 defines this to include any unfair, unlawful, or fraudulent business practice or act.

21 129. Google is headquartered in California and its misconduct originated in
22 California. Furthermore, Google's own Terms of Service state that the laws of the State of
23 California shall apply to all litigation concerning its services, including Google Search.
24 Therefore, Google has bound itself to the application of California law to its conduct.

25 130. Defendant's acts and practices as alleged herein constitute unlawful, unfair,
26 and/or fraudulent business practices in violation of California's Unfair Competition Law,
27 Cal. Bus. & Prof. Code §§ 17200, *et. seq.*

131. Defendant engaged in unlawful business practices by, among other things:

a. engaging in conduct, as alleged herein, that violates the ECPA.

132. Defendant engaged in unfair business practices by, among other things:

a. engaging in conduct where the utility of that conduct is outweighed by the gravity of the consequences to Plaintiff Italiano, the State Law Class, and the Injunctive Relief Class; and,

b. engaging in conduct that is reckless, unconscionable, or substantially injurious to Plaintiff Italiano, the State Law Class, and the Injunctive Relief Class.

133. Defendant utilized fraudulent business practices by engaging in conduct that was and is likely to deceive consumers acting reasonably under the circumstances.

Defendants' fraudulent business practices include but are not limited to:

a. failing to disclose that Defendant transmits user search queries to third parties;

b. touting the importance of trust and privacy while simultaneously transmitting sensitive personal data to third parties; and,

c. failing to disclose that Defendant does not need to transmit user search queries in order to facilitate searches.

134. As a direct and proximate result of Defendant's unlawful, unfair, and fraudulent acts, business practices, and conduct, Plaintiff Italiano, the State Law Class and the Injunctive Relief Class have suffered injury in fact and lost valuable property in the form of their private, sensitive search query data they entrusted to Google.

135. Plaintiff Italiano, on behalf of himself, the State Law Class, and the Injunctive Relief Class, seeks individual restitution, injunctive relief, and other relief allowed under § 17200, *et seq.*

COUNT IV

Unjust Enrichment (In the Alternative)

(on behalf of Plaintiff Italiano individually and the State Law Class)

136. Plaintiff Italiano incorporates by reference the foregoing allegations.

137. Plaintiff Italiano and members of the State Law Class have conferred a benefit upon Google. Google has received and retained valuable information belonging to Plaintiff Italiano and members of the State Law Class, 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.

138. Google appreciates or has knowledge of said benefit.

139. 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.

140. Plaintiff Italiano, on his own behalf and on behalf of the State Law 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, Plaintiffs, on behalf of themselves and the Classes, pray for the following relief:

A. Certify this case as a class action on behalf of the ECPA Class, State Law Class, and the Injunctive Relief Class as defined above, appoint Plaintiffs Gaos and Italiano as representatives of the ECPA Class and Plaintiff Italiano as representative of the State Law Class and the Injunctive Relief Class, and appoint their counsel as counsel for the ECPA Class, the State Law Class, and the Injunctive Relief Class, 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. Bus. & Prof. Code § 17200,

1 constitute Breach of Contract, and unjust enrichment;

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

5 D. Awarding damages, including statutory damages where applicable, to
6 Plaintiffs and the Classes, in an amount to be determined at trial;

7 E. Awarding all economic, monetary, actual, consequential, and compensatory
8 damages caused by Google's conduct, and if its conduct is proved willful, awarding Plaintiffs
9 and the Classes exemplary damages;

10 F. Awarding restitution against Google for all money to which Plaintiffs and the
11 Classes are entitled in equity;

12 G. Ordering Google to disgorge revenues and profits wrongfully obtained;

13 H. Awarding Plaintiffs and the Classes their reasonable litigation expenses and
14 attorneys' fees;

15 I. Awarding Plaintiffs and the Class interest, to the extent allowable; and,

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

17 **JURY TRIAL**

18 141. Plaintiffs demand a trial by jury for all issues so triable.

19
20 Dated: May 1, 2012

Respectfully submitted,
NASSIRI & JUNG LLP

21 s/ Kassra P. Nassiri _____
22 Kassra P. Nassiri
Attorneys for Plaintiffs and the Putative Class

23
24
25 Dated: May 1, 2012

Respectfully submitted,
ASCHENBRENER LAW, P.C.

26 s/ Michael Aschenbrener _____
27 Michael Aschenbrener
Attorneys for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

The undersigned certifies that, on May 1, 2012, he caused this document to be electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of filing to counsel of record for each party.

Dated: May 1, 2012

ASCHENBRENER LAW, P.C.

By: s/ Michael Aschenbrener
Michael Aschenbrener