Before the
Federal Trade Commission
Washington, DC 20580

In the Matter of	**)**
	)
Google, Inc.	**)**
and	**)**
DoubleClick, Inc.	**)**
	)

Complaint and Request for Injunction, Request for Investigation and for Other Relief

INTRODUCTION

1. This complaint concerns the impact on consumer privacy of Internet advertising practices and the specific issues that arise in the proposed acquisition of DoubleClick, Inc. by Google, Inc. As set forth in detail below, the increasing collection of personal information of Internet users by Internet advertisers poses far-reaching privacy concerns that the Commission should address. Neither Google nor DoubleClick have taken adequate steps to safeguard the personal data that is collected. Moreover, the proposed acquisition will create unique risks to privacy and will violate previously agreed standards for the conduct of online advertising.

PARTIES

2. The Electronic Privacy Information Center ("EPIC") is a public interest research organization incorporated in Washington, DC. EPIC's activities include the review of government and private sector policies and practices to determine their possible impact on the privacy interests of the American public. Among its other activities, EPIC first brought the Commission's attention to the privacy risks of online advertising.[1] EPIC also initiated the complaint to the FTC regarding Microsoft Passport in which the Commission subsequently required Microsoft to implement a comprehensive information security program for Passport and similar services.[2]

[1] In the Matter of DoubleClick, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Federal Trade Commission (Feb. 10, 2000), *available at* http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[2] In the Matter of Microsoft Corporation File No. 012 3240, Docket No. C-4069 (Aug. 2002), *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm. *See also*, Fed. Trade Comm'n, "Microsoft Settles FTC Charges Alleging False Security and Privacy Promises" (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), *available at* http://www.ftc.gov/opa/2002/08/microsoft.shtm.

3. The Center for Digital Democracy ("CDD") is a non-profit organization incorporated in the District of Columbia. CDD is committed to preserving the openness and diversity of the Internet in the broadband era. CDD and U.S. PIRG have recently filed with the Commission a Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices.[3]

4. The U.S. Public Interest Research Group ("U.S. PIRG"), incorporated in Washington, DC, serves as both the federal advocacy office for and the federation of non-profit, non-partisan state Public Interest Research Groups, with over one million members nationwide. U.S. PIRG is a strong supporter of fair, competitive marketplace practices, including compliance with the OECD Guidelines for the Protection of Privacy.

5. Google, Inc. ("Google") was incorporated in California in September 1998 and reincorporated in Delaware in August 2003. Google's principal offices are located at 1600 Amphitheatre Parkway, Mountain View, California 94043. At all times material to this complaint, Google's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

6. DoubleClick Inc. ("DoubleClick") was organized as a Delaware corporation on January 23, 1996. DoubleClick's international headquarters are located at 111 Eighth Avenue,10th Floor, New York, NY 10011. At all times material to this complaint, DoubleClick's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

THE IMPORTANCE OF PRIVACY PROTECTION

7. The right of privacy is a personal and fundamental right in the United States. The privacy of an individual is directly implicated by the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services and the rights of due process may be jeopardized by the misuse of personal information.

8. The excessive collection of personal data in the United States coupled with inadequate legal and technological protection have led to a dramatic increase in the crime of identity theft.[4]

9. The federal government has established policies for privacy and data collection on federal web sites that acknowledge particular privacy concerns "when uses of web technology

[3] *Available at* http://www.democraticmedia.org/PDFs/FTCadprivacy.pdf. *See also* Center for Digital Democracy, "Consumer Groups Call for FTC Investigation of Online Advertising and Consumer Tracking and Targeting Practices; Consumer Privacy Must Be Protected from Digital Commercial Shadowing - Privacy Violations Demand an Injunction Against Microsoft and Others," http://www.democraticmedia.org/issues/privacy/FTCprivacypr.html.
[4] Fed. Trade Comm'n, *Consumer Fraud and Identity Theft Compliant Data: January – December 2006* (Feb. 7, 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf (for the seventh year in a row, identity theft is the No. 1 concern of U.S. consumers).

can track the activities of users over time and across different web sites" and has discouraged the use of such techniques by federal agencies.

10. The Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognize that "the right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard."[5]

11. Privacy laws routinely require that information about consumers be deleted once it is no longer needed.[6]

12. Courts have recognized a privacy interest in the collection of information that concerns Internet use even where the information may not be personally identifiable.[7]

13. The Federal Trade Commission has a statutory obligation to investigate and prosecute violations of Section 5 of the Federal Trade Commission Act where the privacy interests of Internet users are at issue.

THE IMPACT OF INTERNET SEARCH ENGINES

14. Internet search engines, such as those offered by Google, Yahoo, and Microsoft, are the primary means by which individuals access content on the Internet.

15. Search terms entered into the main Google search engine alone may reveal a plethora of personal information such as an individual's medical issues, associations, religious beliefs, political preferences, sexual orientation, and investments monitored.

16. In 2005, more than 60 million American adults used search engines on a typical day.[8] The number is no doubt much higher today.

17. Search engine usage not only impacts online decisions of consumers, but also significant amounts of offline behavior.

---

[5] The OECD Privacy Guidelines of 1980 apply to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties." Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data, OECD Doc. 58 final (Sept. 23, 1980), art. 3(a), reprinted in M. ROTENBERG ED., THE PRIVACY LAW SOURCEBOOK 2004 395 (EPIC 20035. The OECD Privacy Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; there should be a policy of openness about the information's existence, nature, collection, maintenance and use; and individuals should have rights to access, amend, complete, or erase information as appropriate. *Id*.

[6] *See, e.g.*, Video Privacy Protection Act of 1988, 18 USC § 2710(e) ("A person subject to this section shall destroy personally identifiable information as soon as practicable . . . .); Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681x (concerning disposal of consumer records).

[7] *Gonzales v. Google,* 234 F.R.D. 674, 687 (N.D. Cal. 2006); *Northwestern Mem'l Hosp. v. Ashcroft*, 362 F.3d 923, 929 (7th Cir. 2004).

[8] Lee Rainie et al., Pew Internet & American Life Project, Search Engine Use November 2005 (2005), http://www.pewinternet.org/pdfs/PIP_SearchData_1105.pdf.

THE FEDERAL TRADE COMMISSION'S REVIEW OF THE PREVIOUS DOUBLECLICK MATTER

18. The Federal Trade Commission has previously investigated DoubleClick Inc. for violations of the Federal Trade Commission Act. On February 10, 2000, EPIC filed a complaint with the FTC concerning the information collection practices of DoubleClick.[9] EPIC alleged that DoubleClick was unlawfully tracking the online activities of Internet users and combining surfing records with detailed personal profiles contained in a national marketing database. EPIC asked the FTC to investigate the practices of the company, to destroy all records wrongfully obtained, to invoke civil penalties, and to enjoin the firm from violating the Federal Trade Commission Act.

19. On February 14, 2000, DoubleClick revealed in a document filed with the Securities and Exchange Commission that the FTC was investigating the company's privacy practices.[10] In addition to the ongoing FTC investigation, DoubleClick faced several class action lawsuits, legal action from the Michigan Attorney General's office, and an informal inquiry from the New York State Attorney General's office.[11]

20. On March 2, 2000, DoubleClick CEO Kevin O'Connor released a statement that said that the company made a "mistake by planning to merge names with anonymous user activity across Web sites in the absence of government and industry privacy standards."[12] The FTC investigation into the company's privacy practices continued.

21. On July 27, 2000, the Network Advertising Initiative ("NAI") made self-regulatory principles available to the public.[13] The NAI (a coalition of some companies in the Internet advertising industry), the FTC and Department of Commerce had been meeting since early 1999 discuss the industry's practices and the possibility of self-regulation.

22. On January 22, 2001, the FTC released a letter announcing that it had closed its investigation of DoubleClick.[14] The FTC letter listed the commitments DoubleClick had agreed to make:

> 1) DoubleClick has used clear GIFs (web bugs) to track users' progress within Web sites and collect information about the user. The company has agreed to disclose and explain its use of clear GIFs in its next privacy policy release.

---

[9] EPIC, In the Matter of DoubleClick, Complaint and Request for Injunction, Request for Investigation and for Other Relief, before the Fed. Trade Comm'n (Feb. 10, 2000), *available at* http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf.

[10] DoubleClick Inc., Registration Statement under Securities Act of 1933 (Form S-3/A) (Feb. 14, 2000), *available at* http://www.sec.gov/Archives/edgar/data/1049480/0000950117-00-000281-index.html.

[11] *Id*.

[12] Press Release, DoubleClick Inc., Statement From Kevin O'Connor, CEO of DoubleClick (Mar. 2, 2000), *available at* http://www.doubleclick.com/us/about_doubleclick/press_releases/default.asp?p=103.

[13] Fed. Trade Comm'n, Report on Online Profiling (July 27, 2000) ["NAI Privacy Principles"], *available at* http://www.ftc.gov/opa/2000/07/onlineprofiling.htm; information about the Network Advertising Initiative at http://www.networkadvertising.org.

[14] Joel Winston, Acting Associate Dir., Div. of Fin. Practices, Fed. Trade Comm'n, Letter to Christine Varney, Esq. (Jan. 22, 2001), *available at* http://www.ftc.gov/os/closings/staff/doubleclick.pdf.

2) Consumers who wish to stop DoubleClick from collecting information can do so by requesting an "opt out cookie." With certain browsers, however, when a consumer chooses the general option "Do not accept or send cookies," the DoubleClick opt out cookie is also deleted. DoubleClick has agreed to disclose in its next privacy policy that, if the user decides at a later date to accept cookies, the user will have to opt-out of DoubleClick again.

3) DoubleClick stated in the Privacy Policy on its Internet Address Finder ("IAF") Web site that it did not sell lists of names, addresses, or email addresses, even though it did so through an opt-in mail list managed by a marketing partner. DoubleClick agreed to revise the IAF Privacy Policy to state: "Internet Address Finder does not sell lists of names, addresses, or e-mail addresses, unless you specifically choose to sign up to receive special promotional offers or advertisements by e-mail, as described below."[15]

The letter also noted DoubleClick's "commitment to abide by [the NAI Privacy Principles]."

23. Under the NAI Privacy Principles, DoubleClick agreed to notify users, through a "clear and conspicuous" privacy policy, about online profiling activity.[16] If personally identifiable information was to be collected, DoubleClick represented that it would give users clear and conspicuous "robust" notice, appearing at the time and place of information collection.[17] DoubleClick further agreed that it would contractually require Web sites using DoubleClick technology to provide similar disclosures. DoubleClick also provided assurances that it would make reasonable efforts to enforce these contractual requirements.[18]

24. DoubleClick also agreed to give users reasonable access to personally identifiable information that DoubleClick retained for profiling.[19] Under the NAI terms, DoubleClick committed to making reasonable efforts to protect data that it collects for profiling from loss, misuse, alteration, or improper access.[20]

25. On May 23, 2001, the NAI created Web sites that enable Internet users to opt-out from online profiling from participating businesses.[21]

26. On December 31, 2001, DoubleClick ended its "intelligent targeting service," which allowed marketers to target ads based on a database of about 100 million profiles.

---

[15] *Id*. at 2.
[16] NAI Privacy Principles at Section IV (B)(1)(a), *supra* note 13.
[17] *Id*. at Section IV (C)(2).
[18] *Id*. at Section IV (A)(4).
[19] *Id*. at Section IV (C)(1)(f).
[20] *Id*. at Section IV (A)(3).
[21] Associated Press, *Ad Industry Creates Web Sites to Allow Consumers to Opt Out of Data Collection*, May 25, 2001.

STATEMENT OF FACTS

27. The acquisition of DoubleClick will permit Google to track both a person's Internet searches and a person's web site visits. This could impact the privacy interests of 233 million Internet users in North America, 314 million Internet users in Europe, and more than 1.1 billion Internet users around the world.[22]

28. Google has already expressed an intent to merge data from Google and DoubleClick to profile and target Internet users.[23]

29. Google has issued a vague statement regarding its plans to protect user privacy following the DoubleClick acquisition:

> "Google has a history of being an advocate for user privacy. We continue to develop technologies that improve privacy for internet users. With this acquisition, we will be able to more broadly deploy and improve privacy enhancing technologies for users. We are committed to transparency for end users, and to respecting the choices they make with regards to their privacy preferences."[24]

Google's Business Practices

30. Google operates the largest Internet search engine in the United States. In March 2007 alone, approximately 3.5 billion search queries were performed on Google websites.[25] Google's services include:

    a. *Google search*: any search term a user enters into Google;
    b. *Google Desktop*: an index of the user's computer files, e-mails, music, photos, and chat and web browser history;
    c. *Google Talk*: instant-message chats between users;
    d. *Google Maps*: address information requested, often including the user's home address for use in obtaining directions;
    e. *Google Mail (Gmail)*: a user's e-mail history, with default settings set to retain e-mails "forever";
    f. *Google Calendar*: a user's schedule as inputted by the user;
    g. *Google Orkut*: social networking tool storing personal information such as name, location, relationship status, etc.;
    h. *Google Reader*: which ATOM/RSS feeds a user reads;
    i. *Google Video/YouTube*: videos watched by user;

---

[22] Internet World Stats, "Internet Usage Statistics," (as of Mar. 19, 2007) http://www.internetworldstats.com/stats.htm.

[23] Joseph Menn, *Google plan raises privacy issue: The search giant wants to combine its data with that of DoubleClick after it buys the ad firm*, L.A. Times, Apr. 17, 2007, *available at* http://www.latimes.com/business/la-fi-privacy17apr17,1,5154383.story?coll=la-headlines-business.

[24] FAQ: Frequently asked questions, "Google acquires DoubleClick," *available at* http://216.239.57.110/blog_resources/DC_FAQ.pdf.

[25] Press Release, comScore, comScore Releases March U.S. Search Engine Rankings (Apr. 17, 2007), *available at* http://www.comscore.com/press/release.asp?press=1397)..

j. *Google Checkout*: credit card/payment information for use on other sites.

31. Google also dominates the search market in Europe, particularly outside the UK. In Germany. Google's market share approaches 90%. Google sites are also visited by a greater proportion of visitors in Europe (75%) than in the United States (60%).[26]

32. Google stores its users' search terms in connection with their Internet Protocol (IP) address, a unique string of numbers that identifies each individual computer connected to the Internet. When a user enters a search term into Google's search engine, Google's servers automatically log the user's web request, IP address, browser type, browser language, the date and time of the request and one or more cookies that may uniquely identify the user's browser.[27] As a user's web request includes the requested search term, Google's logs link a user's personally-identifiable IP address with their search terms.

33. Though Google tracks its users' search activity in connection with their IP address, Google does not currently use this data to engage in behavioral targeting.[28]

34. Google currently stores its users' search activity in connection with their IP address indefinitely. On March 14, 2007, Google announced that it would soon begin to "anonymize" the data linking search terms to a specific IP address after 18 to 24 months.[29] In 2006, the publication of search records of 658,000 Americans by AOL demonstrated that the storage of a number as opposed to personally identifiable information does not necessarily mean that search data cannot be linked back to an individual. Though the search logs released by AOL had been "anonymized," therefore only identifying the user by only a number, quick research by New York Times reporters matched some user numbers with the correct individuals.[30]

35. A January 2006 poll of 1,000 Google users found that 89% of respondents think their search terms are kept private, and 77% believed that Google searches do not reveal their personal identities.[31] These numbers indicate that Google's practices violate the public's expectation of privacy with respect to the collection and use of search history data.

36. The fact that Google collects its users' search terms in connection with their IP address is not disclosed on Google's "Privacy Policy Highlights" page[32] or on its full "Privacy Policy" page.[33] A user must click on four links from the Google homepage in order to obtain this information.

---

[26] "Google dominates the continent," *The European Search Advertising Landscape 2006* 4 (Nov. 2006).
[27] *See* Google Privacy Ctr.: Privacy Policy, http://www.google.com/intl/en/privacypolicy.html.
[28] *See* Miguel Helft, *Google Adds a Safeguard on Privacy for Searchers*, N.Y. Times, Mar. 15, 2007 (Google does not engage in behavioral targeting, unlike Microsoft and Yahoo).
[29] *See* Posting of Peter Fleischer and Nicole Wong to Google Blog, http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html (March 14, 2007, 15:00 EST).
[30] Michael Barbaro and Tom Zeller, *A Face Is Exposed For AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006.
[31] Linda Rosencrance, *Survey Finds Solid Opposition to Release of Google Data to Feds*, Computerworld, Jan. 24, 2006, http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,107993,00.html.
[32] *See* Google Privacy Ctr.: Privacy Policy Highlights, http://www.google.com/intl/en/privacy.html.
[33] *See* Google Privacy Ctr.: Privacy Policy, *supra* note 27.

On the Google homepage, a user must first click on "About Google." The user must then click on "Privacy Policy," which displays the "Google Privacy Policy Highlights" page. This page states:

> Google's servers automatically record information when you visit our website or use some of our products, including the URL, IP address, browser type and language, and the date and time of your request.[34]

The "Privacy Policy Highlights" page provides a link to full Google Privacy Policy. In its full policy, Google outlines the information it collects and how it uses it. Included in this list is log information, which Google describes as:

> When you use Google services, our servers automatically record information that your browser sends whenever you visit a website. These server logs may include information such as your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.[35]

If a user clicks on "server logs" from within the above description, he is brought to a FAQ entry for "What are server logs?" The answer explains to the user a typical log entry for a search of "cars." Google states that the log entry is as follows:

> 123.45.67.89 - 25/Mar/2003 10:15:32 - http://www.google.com/search?q=cars - Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

The log entry is then broken down into its parts. A description of the parts includes:

> (1) 123.45.67.89 is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
> [. . .]
> (2) http://www.google.com/search?q=cars is the requested URL, including the search query;[36]

37. Google does not comply with such well established government and industry privacy standards as the OECD Privacy Guidelines.

DoubleClick's Business Practices

38. DoubleClick is a leading provider of Internet-based advertising. The company places advertising messages on Web sites.

39. DoubleClick reaches an estimated 80 to 85 percent of the users of Internet. Its customers include Time Warner's AOL and Viacom's MTV Networks.

---

[34] Google Privacy Ctr.: Privacy Policy Highlights, *supra* note 32.
[35] Google Privacy Ctr.: Privacy Policy, *supra* note 27.
[36] Google Privacy Ctr.: Google Privacy FAQ, http://www.google.com/intl/en/privacy_faq.html#serverlogs

40. DoubleClick tracks the individual Internet users who receive ads served through DoubleClick. When a user is first "served" an ad, DoubleClick assigns the user a unique number and records that number in a "cookie" file stored on the user's computer. As that user subsequently visits other Web sites on which DoubleClick serves ads, he or she is identified and recorded as having viewed each ad. DoubleClick stores a user's history for two years.

41. Using the unique numbers contained in cookies, DoubleClick's "DART" (Dynamic, Advertising, Reporting, and Targeting) technology enables advertisers to target and deliver ads to Web users based on pre-selected criteria.

42. DoubleClick retains large volumes of consumer data. Its DART technology relies on consumer demographic information in order to execute behavioral targeting of advertisements. Behavioral targeting provides a far-reaching range of information about users, including web surfing, shopping cart behavior, and use of broadband video.

43. DoubleClick does not comply with such well established government and industry privacy standards as the OECD Privacy Guidelines.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

44. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits unfair or deceptive acts or practices in or affecting commerce.

Google's Activities Constitute Deceptive Trade Practices

45. Upon arriving at the Google homepage, a Google user is not informed of Google's data collection practices until he or she clicks through four links. Most users will not reach this page.

46. In truth and in fact, Google collects user search terms in connection with his or her IP address without adequate notice to the user. Therefore, Google's representations concerning its data retention practices were, and are, deceptive practices.

Google's Activities Constitute Unfair Trade Practices

47. Google's collection of information about its users, through the retention of users' search terms in connection with their IP address, is performed without the knowledge or consent of Google users. Self-regulatory principles set forth by the Network Advertising Initiative ("NAI") in July 2000 stated, "[c]onsumers will receive notice of network advertisers' profiling activities on host Web sites and have the ability to choose not to participate in profiling." As a result of Google's failure to detail its data retention policies until four levels down within its website, its users are unaware that their activities are being monitored. Furthermore, Google does not provide any "opt-out" option to its users who do not want Google to store their search terms.

48. Google's collection of information about its users without compliance with Fair Information Practices, such as the OECD Privacy Guidelines, is likely to cause

substantial injury to consumers, which is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition, and therefore is an unfair practice.

Consumer Injury

49. Google's and DoubleClick's conduct, as set forth above, has injured consumers throughout the United States by invading their privacy; storing information obtained through the retention of users' search terms in ways and for purposes other than those consented to or relied upon by such consumers; causing them to believe, falsely, that their online activities would remain anonymous; and undermining their ability to avail themselves of the privacy protections promised by online companies.

50. Absent injunctive relief by the Commission, Google is likely to continue to injure consumers and harm the public interest.

51. Absent injunctive relief by the Commission in this matter, Google will leave Internet users vulnerable to surveillance by law enforcement agents and intelligence officers, both in United States and in other countries, that could occur without any legal basis to permit the disclosure of personal information.

52. Absent injunctive relief by the Commission in this matter, other companies will be encouraged to collect large volumes of information from consumers in an unfair, disproportionate, and deceptive manner.

53. Absent injunctive relief by the Commission in this matter, the privacy interests of consumers engaging in online commerce and other Internet activities will be significantly diminished.

CONCLUSION

54. Google's proposed acquisition of DoubleClick will give one company access to more information about the Internet activities of consumers than any other company in the world. Moreover, Google will operate with virtually no legal obligation to ensure the privacy, security, and accuracy of the personal data that it collects. At this time, there is simply no consumer privacy issue more pressing for the Commission to consider than Google's plan to combine the search histories and web site visit records of Internet users.

REQUEST FOR RELIEF

55. Initiate an investigation of the proposed acquisition of DoubleClick by Google specifically with regard to the ability of Google to record, analyze, track, and profile the activities of Internet users with data that is both personally identifiable and data that is not personally identifiable.

56. Order DoubleClick to remove user identified cookies and other persistent pseudonymic identifier from all corporate records, databases, and data sets under the control of DoubleClick prior to the transfer to Google, unless DoubleClick obtains explicit

affirmative consent, following an opportunity for the individual to whom the data concerns to inspect, delete and modify the data.

57. Order Google to present a public plan for how it plans to comply with such well established government and industry privacy standards as the OECD Privacy Guidelines.

58. Order Google to provide for reasonable access to all personally identifiable data maintained by the company to the person to whom the data pertains.

59. Order Google to establish a meaningful data destruction policy and require that Google destroy all cookies and other persistent identifiers resulting from Internet searches that are or could be personally identifiable once the user terminates the session with Google.

60. Pending an adequate resolution of the issues identified in this Complaint, as well as other matters that may be brought to the Commission's attention, the Commission should use its authority to review mergers to halt Google's proposed acquisition of DoubleClick.

Respectfully submitted,

Marc Rotenberg	Melissa Ngo	Caitriona Fitzgerald
Executive Director	Staff Counsel	IPIOP Law Clerk

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW Suite 200
Washington, DC 20009
202- 483-1140 (tel)
202-483-1248 (fax)

April 20, 2007