Prepared Statement of
The Federal Trade Commission
"Online Profiling: Benefits and Concerns"

Before the

Committee on Commerce, Science, and Transportation
United States Senate

Washington, D.C.

June 13, 2000

Mr. Chairman and Members of the Committee, I am Jodie Bernstein, Director of the Bureau of Consumer Protection of the Federal Trade Commission.[(1)] I appreciate this opportunity to discuss the Commission's report on profiling issued today.[(2)] The report describes the nature of online profiling, consumer privacy concerns about these practices, and the Commission's efforts to date to address these concerns. The Commission is not making any recommendations at this time.

As it has in other areas, the Commission has encouraged effective industry self-regulation, and the network advertising industry has responded with drafts of self-regulatory principles for our consideration. As discussed further in this testimony, there are real challenges to creating an effective self-regulatory regime for this complex and dynamic industry, and this process is not yet complete. The Commission will supplement this report with specific recommendations to Congress after it has an opportunity to fully consider the self-regulatory proposals and how they interrelate with the Commission's previous views and recommendations in the online privacy area.

I. Introduction and Background

A. FTC Law Enforcement Authority

The FTC's mission is to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive acts or practices and to increase consumer choice by promoting vigorous competition. As you know, the Commission's responsibilities are far-reaching. The Commission's primary legislative mandate is to enforce the Federal Trade Commission Act ("FTCA"), which prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[(3)] With the exception of certain industries and activities, the FTCA provides the Commission with broad investigative and law enforcement authority over entities engaged in or whose business affects commerce.[(4)] Commerce on the Internet falls within the scope of this statutory mandate.

B. Privacy Concerns in the Online Marketplace

Since its inception in the mid-1990's, the online consumer marketplace has grown at an exponential rate. Recent figures suggest that as many as 90 million Americans now use the Internet on a regular basis.[(5)] Of these, 69%, or over 60 million people, shopped online in the third quarter of 1999.[(6)] In addition, the Census Bureau estimates that retail e-commerce sales were $5.2 billion for the fourth quarter of 1999, and increased to $5.3 billion for the first quarter of 2000.[(7)]

At the same time, technology has enhanced the capacity of online companies to collect, store, transfer, and analyze vast amounts of data from and about the consumers who visit their Web sites. This increase in the collection and use of data, along with the myriad subsequent uses of this information that interactive technology makes possible, has raised public awareness and consumer concerns about online privacy.[(8)] Recent survey data demonstrate that 92% of consumers are concerned (67% are "very concerned") about the misuse of their personal information online.[(9)] The level of consumer unease is also indicated by a recent study in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential.[(10)] To ensure consumer confidence in this new marketplace and its continued growth, consumer concerns about privacy must be addressed.[(11)]

C. The Commission's Approach to Online Privacy - Initiatives Since 1995

Since 1995, the Commission has been at the forefront of the public debate concerning online privacy.[(12)] The Commission has held public workshops; examined Web site information practices and disclosures regarding the collection, use, and transfer of personal information; and commented on self-regulatory efforts and technological developments intended to enhance consumer privacy. The Commission's goals have been to understand this new marketplace and its information practices, and to assess the costs and benefits to businesses and consumers.[(13)]

In June 1998 the Commission issued *Privacy Online: A Report to Congress* ("1998 Report"), an examination of the information practices of commercial sites on the World Wide Web and of industry's efforts to implement self-regulatory programs to protect consumers' online privacy.[(14)] The Commission described the widely-accepted fair information practice principles of *Notice*, *Choice*, *Access* and *Security*. The Commission also identified *Enforcement* - the use of a reliable mechanism to provide sanctions for noncompliance - as a critical component of any governmental or self-regulatory program to protect privacy online.[(15)] In addition, the 1998 Report presented the results of the Commission's first online privacy survey of commercial Web sites. While almost all Web sites (92% of the comprehensive random sample) were collecting great amounts of personal information from consumers, few (14%) disclosed anything at all about their information practices.[(16)]

Based on survey data showing that the vast majority of sites directed at children also collected personal information, the Commission recommended that Congress enact legislation setting forth standards for the online collection of personal information from children.[(17)] The Commission deferred its recommendations with respect to the collection

of personal information from online consumers generally. In subsequent Congressional testimony, the Commission referenced promising self-regulatory efforts suggesting that industry should be given more time to address online privacy issues. The Commission urged the online industry to expand these efforts by adopting effective, widespread self-regulation based upon the long-standing fair information practice principles of Notice, Choice, Access, and Security, and by putting enforcement mechanisms in place to assure adherence to these principles.[(19)] In a 1999 report to Congress, *Self-Regulation and Privacy Online*, a majority of the Commission again recommended that self-regulation be given more time.[(20)]

On May 22, 2000, the Commission issued its third report to Congress examining the state of online privacy and the efficacy of industry self-regulation. *Privacy Online: Fair Information Practices in the Electronic Marketplace* ("2000 Report") presented the results of the Commission's 2000 Online Privacy Survey, which reviewed the nature and substance of U.S. commercial Web sites' privacy disclosures, and assessed the effectiveness of self-regulation. In that Report, a majority of the Commission concluded that legislation is necessary to ensure further implementation of fair information practices online and recommended a framework for such legislation.[(21)]

II. Online Profiling

On November 8, 1999, the Commission and the United States Department of Commerce jointly sponsored a Public Workshop on Online Profiling.[(22)] As a result of the Workshop and public comment, the Commission learned a great deal about what online profiling is, how it can benefit both businesses and consumers, and the privacy concerns that it raises.

A. What is Online Profiling?

More than half of all online advertising is in the form of "banner ads" displayed on Web pages - small graphic advertisements that appear in boxes above or to the side of the primary site content.[(23)] Often, these ads are not selected and delivered by the Web site visited by a consumer, but by a network advertising company that manages and provides advertising for numerous unrelated Web sites.

In general, these network advertising companies do not merely supply banner ads; they also gather data about the consumers who view their ads. This is accomplished primarily by the use of "cookies"[(26)] which track the individual's actions on the Web.[(27)] The information gathered by network advertisers is often, but not always, anonymous, that is, the profiles are frequently linked to the identification number of the advertising network's cookie on the consumer's computer rather than the name of a specific person. In some circumstances, however, the profiles derived from tracking consumers' activities on the Web are linked or merged with personally identifiable information.[(28)]

Once collected, consumer data is analyzed and can be combined with demographic and "psychographic"[(29)] data from third-party sources, data on the consumer's offline purchases, or information collected directly from consumers through surveys and

registration forms. This enhanced data allows the advertising networks to make a variety of inferences about each consumer's interests and preferences. The result is a detailed profile that attempts to predict the individual consumer's tastes, needs, and purchasing habits and enables the advertising companies' computers to make split-second decisions about how to deliver ads directly targeted to the consumer's specific interests.

The profiles created by the advertising networks can be extremely detailed. A cookie placed by a network advertising company can track a consumer on any Web site served by that company, thereby allowing data collection across disparate and unrelated sites on the Web. Also, because the cookies used by ad networks are generally persistent, their tracking occurs over an extended period of time, resuming each time the individual logs on to the Internet. When this "clickstream" information is combined with third-party data, these profiles can include hundreds of distinct data fields.[(30)]

Although network advertisers and their profiling activities are nearly ubiquitous,[(31)] they are most often invisible to consumers. All that consumers see are the Web sites they visit; banner ads appear as a seamless, integral part of the Web page on which they appear and cookies are placed without any notice to consumers.[(32)] Unless the Web sites visited by consumers provide notice of the ad network's presence and data collection, consumers may be totally unaware that their activities online are being monitored.[(33)]

B. Profiling Benefits and Privacy Concerns

Network advertisers' use of cookies [(34)] and other technologies to create targeted marketing programs can benefit both consumers and businesses. As noted by commenters at the Public Workshop, targeted advertising allows customers to receive offers and information about goods and services in which they are actually interested.[(35)] Businesses clearly benefit as well from the ability to target advertising because they avoid wasting advertising dollars marketing themselves to consumers who have no interest in their products.[(36)] Additionally, a number of commenters stated that targeted advertising helps to subsidize free content on the Internet.[(37)]

Despite the benefits of targeted advertising, there is widespread concern about current profiling practices. The most consistent and significant concern expressed about profiling is that it is conducted without consumers' knowledge.[(38)] The presence and identity of a network advertiser on a particular site, the placement of a cookie on the consumer's computer, the tracking of the consumer's movements, and the targeting of ads are simply invisible in most cases.

The second most persistent concern expressed by commenters was the extensive and sustained scope of the monitoring that occurs. Unbeknownst to most consumers, advertising networks monitor individuals across a multitude of seemingly unrelated Web sites and over an indefinite period of time. The result is a profile far more comprehensive than any individual Web site could gather. Although much of the information that goes into a profile is fairly innocuous when viewed in isolation, the cumulation over time of vast numbers of seemingly minor details about an individual produces a portrait that is

quite comprehensive and, to many, inherently intrusive.[(39)]

For many of those who expressed concerns about profiling, the privacy implications of profiling are not ameliorated in cases where the profile contains no personally identifiable information.[(40)] First, commenters feared that companies could unilaterally change their operating procedures and begin associating personally identifiable information with non-personally identifiable data previously collected.[(41)] Second, these commenters objected to the use of profiles--regardless of whether they contain personally identifiable information--to make decisions about the information individuals see and the offers they receive. Commenters expressed concern that companies could use profiles to determine the prices and terms upon which goods and services, including important services like life insurance, are offered to individuals. [(43)]

C. Online Profiling and Self Regulation: the NAI Effort

The November 8th workshop provided an opportunity for consumer advocates, government, and industry members not only to educate the public about the practice of online profiling, but to explore self-regulation as a means of addressing the privacy concerns raised by this practice. In the Spring of 1999, in anticipation of the Workshop, network advertising companies were invited to meet with FTC and Department of Commerce staff to discuss their business practices and the possibility of self-regulation. As a result, industry members announced at the Workshop the formation of the Network Advertising Initiative (NAI), an organization comprised of the leading Internet Network Advertisers - 24/7 Media, AdForce, AdKnowledge, Avenue A, Burst! Media, DoubleClick, Engage, and MatchLogic - to develop a framework for self-regulation of the online profiling industry.

In announcing their intention to implement a self-regulatory scheme, the NAI companies acknowledged that they face unique challenges as a result of their indirect and invisible relationship with consumers as they surf the Internet. The companies also discussed the fundamental question of how fair information practices, including choice, should be applied to the collection and use of data that is unique to a consumer but is not necessarily personally identifiable, such as clickstream data generated by the user's browsing activities and tied only to a cookie identification number.[(44)]

Following the workshop, the NAI companies submitted working drafts of self-regulatory principles for consideration by FTC and Department of Commerce staff. Although efforts have been made to reach a consensus on basic standards for applying fair information practices to the business model used by the network advertisers, this process is not yet complete. The Commission will supplement this report with specific recommendations to Congress after it has an opportunity to fully consider the self-regulatory proposals and how they interrelate with the Commission's previous views and recommendations in the online privacy area.

III. Conclusion

The Commission is committed to the goal of ensuring privacy online for consumers and will continue working to address the unique issues presented by online profiling. I would be pleased to answer any questions you may have.

---

1. The Commission vote to issue this testimony was 5-0, with Commissioner Swindle concurring in part and dissenting in part. Commissioner Swindle's separate statement is attached to the testimony.

2. My oral testimony and responses to questions you may have reflect my own views and are not necessarily the views of the Commission or any individual Commissioner.

3. 15 U.S.C. § 45(a).

4. The Commission also has responsibility under 45 additional statutes governing specific industries and practices. These include, for example, the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq.*, which mandates disclosures of credit terms, and the Fair Credit Billing Act, 15 U.S.C. §§ 1666 *et seq.*, which provides for the correction of billing errors on credit accounts. The Commission also enforces over 30 rules governing specific industries and practices, *e.g.*, the Used Car Rule, 16 C.F.R. Part 455, which requires used car dealers to disclose warranty terms via a window sticker; the Franchise Rule, 16 C.F.R. Part 436, which requires the provision of information to prospective franchisees; the Telemarketing Sales Rule, 16 C.F.R. Part 310, which defines and prohibits deceptive telemarketing practices and other abusive telemarketing practices; and the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312.

In addition, on May 12, 2000, the Commission issued a final rule implementing the privacy provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.* The rule requires a wide range of financial institutions to provide notice to their customers about their privacy policies and practices. The rule also describes the conditions under which those financial institutions may disclose personal financial information about consumers to nonaffiliated third parties, and provides a method by which consumers can prevent financial institutions from sharing their personal financial information with nonaffiliated third parties by opting out of that disclosure, subject to certain exceptions. The rule is available on the Commission's Web site at <http://www.ftc.gov/os/2000/05/index.htm#12. *See Privacy of Consumer Financial Information*, to be codified at 16 C.F.R. pt. 313.

The Commission does not, however, have criminal law enforcement authority. Further, under the FTCA, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance, are wholly or partially exempt from Commission jurisdiction. *See* Section 5(a)(2) and (6)a of the FTC Act, 15 U.S.C. § 45(a)(2) and 46(a). *See also* The McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

5. The Intelliquest Technology Panel, *Panel News*, available at <http://www.techpanel.com/news/index.asp> [hereinafter "Technology Panel"] (90 million adult online users as of third-quarter 1999). Other sources place the number in the 70-75 million user range. *See* Cyber Dialogue, *Internet Users*, available at <http://www.cyberdialogue.com/resource/data/ic/index.html> (69 million users); Cyberstats, *Internet Access and Usage, Percent of Adults 18+*, available at <http://www.mediamark.com/cfdocs/MRI/cs_f99a.cfm> (75 million users).

6. Technology Panel. This represents an increase of over 15 million online shoppers in one year. *See id.*

7. United States Department of Commerce News, *Retail E-commerce Sales Are $5.3 Billion In First Quarter 2000, Census Bureau Reports* (May 31, 2000), available at <http://www.census.gov/mrts/www/current.html>.

8. Survey data is an important component in the Commission's evaluation of consumer concerns, as is actual consumer behavior. Nonetheless, the Commission recognizes that the interpretation of survey results is complex and must be undertaken with care.

9. Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want*, Privacy and American Business at 11 (Nov. 1999) [hereinafter "Westin/PAB 1999"]. *See also IBM Multi-National Consumer Privacy Survey* at 72 (Oct. 1999), prepared by Louis Harris & Associates Inc. [hereinafter "IBM Privacy Survey"] (72% of Internet users very concerned and 20% somewhat concerned about threats to personal privacy when using the Internet); Forrester Research, Inc., *Online Consumers Fearful of Privacy Violations* (Oct. 1999), available at <http://www.forrester.com/ER/Press/Release/0,1769,177,FF.html> (two-thirds of American and Canadian online shoppers feel insecure about exchanging personal information over the Internet).

10. *Survey Shows Few Trust Promises on Online Privacy*, Apr. 17, 2000, available at <http://www.nyt.com> (citing recent Odyssey survey).

11. The Commission, of course, recognizes that other consumer concerns also may hinder the development of e-commerce. As a result, the agency has pursued other initiatives such as combating online fraud through law enforcement efforts. *See FTC Staff Report: The FTC's First Five Years Protecting Consumers Online* (Dec. 1999). The Commission, with the Department of Commerce, recently held a public workshop and soliciting comment on the potential issues associated with the use of alternative dispute resolution for online consumer transactions. *See* Initial Notice Requesting Public Comment and Announcing Public Workshop, 65 Fed. Reg. 7,831 (Feb. 16, 2000); Notice Announcing Dates and Location of Workshop and Extending Deadline for Public Comments, 65 Fed. Reg. 18,032 (Apr. 6, 2000). The workshop was held on June 6 and 7, 2000. Information about the workshop, including the federal register notices and public comments received, is available at <http://www.ftc.gov/bcp/altdisresolution/index.htm>.

12. The Commission's review of privacy has mainly focused on online issues because the Commission believes privacy is a critical component in the development of electronic commerce. However, the FTC Act and most other statutes enforced by the Commission apply equally in the offline and online worlds. As described *infra*, n.11, the agency has examined privacy issues affecting both arenas, such as those implicated by the Individual Reference Services Group, and in the areas of financial and medical privacy. It also has pursued law enforcement, where appropriate, to address offline privacy concerns. *See FTC v. Rapp*, No. 99-WM-783 (D. Colo. filed Apr. 21, 1999); *In re Trans Union*, Docket No. 9255 (Feb. 10, 2000), *appeal docketed*, No. 00-1141 (D.C. Cir. Apr. 4, 2000). These activities - as well as recent concerns about the merging of online and offline databases, the blurring of distinctions between online and offline merchants, and the fact that a vast amount of personal identifying information is collected and used offline - make clear that significant attention to offline privacy issues is warranted.

13. The Commission held its first public workshop on privacy in April 1995. In a series of hearings held in October and November 1995, the Commission examined the implications of globalization and technological innovation for competition and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices regarding the collection, use, and transfer of consumers' personal information; self-regulatory efforts and technological developments to enhance consumer privacy; consumer and business education efforts; the role of government in protecting online information privacy; and special issues raised by the online collection and use of information from and about children. The Commission held a second workshop in June 1997 to explore issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

The Commission and its staff have also issued reports describing various privacy concerns in the electronic marketplace. *See, e.g.*, *FTC Staff Report: The FTC's First Five Years Protecting Consumers Online* (Dec. 1999); *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997); *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec.

1996); *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996). Recently, at the request of the Department of Health and Human Services ("HHS"), the Commission submitted comments on HHS' proposed Standards for Privacy of Individually Identifiable Health Information (required by the Health Insurance Portability and Accountability Act of 1996). The Commission strongly supported HHS' proposed "individual authorization" or "opt-in" approach to health providers' ancillary use of personally identifiable health information for purposes other than those for which the information was collected. The Commission also offered HHS suggestions it may wish to consider to improve disclosure requirements in two proposed forms that would be required by the regulations. The Commission's comments are available at <http://www.ftc.gov/be/v000001.htm>.

The Commission also has brought law enforcement actions to protect privacy online pursuant to its general mandate to fight unfair and deceptive practices. *See FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000) (consent decree) (settling charges that an online auction site obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited e-mail messages to those consumers seeking their business); *Liberty Financial Companies, Inc.*, FTC Dkt. No. C-3891 (Aug. 12, 1999) (consent order) (challenging the allegedly false representations by the operator of a "Young Investors" Web site that information collected from children in an online survey would be maintained anonymously); *GeoCities*, FTC Dkt. No. C-3849 (Feb. 12, 1999) (consent order) (settling charges that Web site misrepresented the purposes for which it was collecting personal identifying information from children and adults).

14. The Report is available on the Commission's Web site at http://www.ftc.gov/reports/privacy3/index.htm.

15. 1998 Report at 11-14.

16. *Id.* at 23, 27.

17. *Id.* at 42-43. In October 1998, Congress enacted the Children's Online Privacy Protection Act of 1998 ("COPPA"), which authorized the Commission to issue regulations implementing the Act's privacy protections for children under the age of 13.[(18)]

18. 15 U.S.C. § § 6501 *et seq.* §§ '

19. *See* Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web" before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Committee on Commerce, U.S. House of Representatives (July 21, 1998), available at <http://www.ftc.gov/os/1998/9807/privac98.htm>.

20. *Self-Regulation and Privacy Online* (July 1999) at 12-14 (available at <http://www.ftc.gov/os/1999/9907/index.htm#13>).

21. The 2000 Report is available at <http://www.ftc.gov/os/2000/05/index.htm#22>. The Commission's vote to issue the report was 3-2, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part.

22. A transcript of the Workshop is available at <http://www.ftc.gov/bcp/profiling/index.htm> and will be cited as "Tr. [page], [speaker]." Public comments received in connection with the Workshop can be viewed on the Federal Trade Commission's Web site at <http://www.ftc.gov/ bcp/profiling/comments/index.html> and will be cited as "Comments of [organization or name] at [page]."

23. In 1999, 56% of all online advertising revenue was attributable to banner advertising. Online

advertising has grown exponentially in tandem with the World Wide Web: online advertising revenues in the U.S. grew from $301 million in 1996[(24)]

24. *See* Federal Trade Commission, Privacy Online: A Report to Congress (1998) at 3. The Report is available on the Commission's Web site at <http://www.ftc.gov/reports/ privacy3/index.htm>. [(25)]

25. *See* Jupiter Communications, Inc., Online Advertising Through 2003 (1999) (summary available at <http://www.jupitercommunications.com>).

26. A cookie is a small text file placed on a consumer's computer by a Web server that transmits information back to the server that placed it. As a rule, a cookie can be read only by the server that placed it.

27. In addition to cookies, which are largely invisible to consumers, other hidden methods of monitoring consumers' activities on the Web may also be used. One such method is through the use of "Web bugs," also known as "clear GIFs" or "1-by-1 GIFs." Web bugs are tiny graphic image files embedded in a Web page, generally the same color as the background on which they are displayed. They are one pixel in height by one pixel in length - the smallest image capable of being displayed on a monitor - and are invisible to the naked eye. The Web bug sends back to its home server (which can belong to the host site, a network advertiser or some other third party): the IP (Internet Protocol) address of the computer that downloaded the page on which the bug appears; the URL (Uniform Resource Locator) of the page on which the Web bug appears; the URL of the Web bug image; the time the page containing the Web bug was viewed; the type of browser that fetched the Web bug; and the identification number of any cookie on the consumer's computer previously placed by that server. Web bugs can be detected only by looking at the source code of a Web page and searching in the code for 1-by-1 IMG tags that load images from a server different than the rest of the Web page. At least one expert claims that, in addition to disclosing who visits the particular Web page or reads the particular email in which the bug has been placed, in some circumstances, Web bugs can also be used to place a cookie on a computer or to synchronize a particular email address with a cookie identification number, making an otherwise anonymous profile personally identifiable. *See generally* Comments of Richard M. Smith; *see also Big Browser is Watching You!*, Consumer Reports, May 2000, at 46; USA Today, *A new wrinkle in surfing the Net: Dot-coms' mighty dot-size bugs track your every move*, Mar. 21, 2000 (available at <http://www.usatoday.com/life/cyber/tech/cth582.htm>).

28. Personally identifiable data is data that can be linked to specific individuals and includes, but is not limited to such information as name, postal address, phone number, e-mail address, social security number, and driver's license number. The linkage of personally identifiable information with non-personally identifiable information generally occurs in one of two ways when consumers identify themselves to a Web site on which the network advertiser places banner ads. First, the Web site to whom personal information is provided may, in turn, provide that information to the network advertiser. Second, depending upon how the personal information is retrieved and processed by the Web site, the personally identifying information may be incorporated into a URL string that is automatically transmitted to the network advertiser through its cookie. In addition, network advertising companies can and do link personally identifiable information to non-personally identifiable information at their own Web sites by asking consumers to provide personal information (for example, to enter a sweepstakes) and then linking that information to the cookie previously placed on the consumer's computer; the linkage of personally identifying information to a cookie makes all of the data collected through that cookie personally identifiable.

29. Psychographic data links objective demographic characteristics like age and gender with more abstract characteristics related to ideas, opinions and interests. Data mining specialists analyze demographic, media, survey, purchasing and psychographic data to determine the exact groups that are most likely to buy specific products and services. *See* Comments of the Center for Democracy and Technology (CDT) at 5 n.5. Psychographic profiling is also referred to in the industry as "behavioral profiling."

30. For example, the Web site for Engage states repeatedly that its profiles contain 800 "interest categories." *See, e.g.*, <http://www.engage.com/ press/releases/2qfiscal.htm>.

31. DoubleClick has approximately 100 million consumer profiles, *see* Heather Green, *Privacy: Outrage on the Web*, Business Week, Feb 14, 2000, at 38; Engage has 52 million consumer profiles, *see* <http://www.engage.com/press/releases/2qfiscal.htm>; and 24/7 Media has 60 million profiles, *see* <http://www.247media.com/connect/adv_pub.html>.

32. Most Internet browsers can be configured to notify users that a cookie is being sent to their computer and to give users the option of rejecting the cookie. The browsers' default setting, however, is to permit placement of cookies without any notification.

33. Not all profiles are constructed by network advertising companies. Some Web sites create profiles of their own customers based on their interactions. Other companies create profiles as part of a service - for example, offering discounts on products of interest to consumers or providing references to useful Web sites on the same topic as those already visited by the consumer. *See, e.g.*, Megan Barnett, *The Profilers: Invisible Friends*, The Industry Standard, Mar. 13, 2000, at 220; Ben Hammer, *Bargain Hunting*, The Industry Standard, Mar. 13, 2000, at 232. These profiles are generally created by companies that have a known, consensual relationship with the consumer and are not addressed in this report. This report uses the term "profiling" to refer only to the activities of third-party network advertising companies.

34. Cookies are used for many purposes other than profiling by third-party advertisers, many of which significantly benefit consumers. For example, Web sites often ask for user names and passwords when purchases are made or before certain kinds of content are provided. Cookies can store these names and passwords so that consumers do not need to sign in each time they visit the site. In addition, many sites allow consumers to set items aside in an electronic shopping cart while they decide whether or not to purchase them; cookies allow a Web site to remember what is in a consumer's shopping cart from prior visits. Cookies also can be used by Web sites to offer personalized home pages or other customized content with local news and weather, favorite stock quotes, and other material of interest to individual consumers. Individual online merchants can use cookies to track consumers' purchases in order to offer recommendations about new products or sales that may be of interest to their established customers. Finally, by enabling businesses to monitor traffic on their Web sites, cookies allow businesses to constantly revise the design and layout of their sites to make them more interesting and efficient. The privacy issues raised by these uses of cookies are beyond the scope of this report.

35. *See, e.g.*, Comments of the Magazine Publishers of America (MPA) at 1; Comments of the Direct Marketing Association (DMA) at 2; Comments of the Association of National Advertisers (ANA) at 2; Tr. 30, Smith; Tr. 120, Jaffe.

36. *See, e.g.*, Comments of the Association of National Advertisers (ANA) at 2.

37. *See, e.g.*, Comments of the Magazine Publishers of America (MPA) at 1; Comments of Solveig Singleton at 3-4; Tr. 20, Jaye; Tr. 124, Aronson.

38. *See, e.g.*, Comments of the Center for Democracy and Technology (CDT) at 2, 16; Reply Comments of the Electronic Information Privacy Center (EPIC) at 1; Comments of TRUSTe at 2; Tr. 113, Mulligan.

39. *See, e.g.*, Comments of the Center for Democracy and Technology (CDT) at 2; Reply Comments of Electronic Information Privacy Center (EPIC) at 1-2.

40. *See, e.g.*, Comments of the Center for Democracy and Technology (CDT) at 2-3; Tr. 112, Steele; Tr. 128, Smith.

41. *See* Comments of the Center for Democracy and Technology (CDT) at 2-3; Comments of Christopher K. Ridder (Nov. 30, 1999) at 6 (listing examples of sites whose privacy policies explicitly reserve the right of the site to change privacy policies without notice to the consumer); Tr. 158, Mulligan. These commenters also felt that the comprehensive nature of the profiles and the technology used to create them make it reasonably easy to associate previously anonymous profiles with particular individuals.[(42)]

42. *See, e.g.*, Rebuttal Comments of the Electronic Frontier Foundation (EFF) at 2; Tr. 40-1, Catlett; Tr. 54, Smith; Tr. 62, Weitzner.

43. *See* Comments of the Center for Democracy and Technology (CDT) at 3; Comments of the Electronic Frontier Foundation (EFF) Session II at 2; Rebuttal Comments of the Electronic Frontier Foundation (EFF) at 4; Tr. 81, Feena; Tr. 114, Hill; Tr. 146-7, Steele; *see also* John Simons, *The Coming Privacy Divide*, The Standard, Feb. 21, 2000, <http://www. thestandard.com/article/display/1,1153,10880,00.html>. For example, products might be offered at higher prices to consumers whose profiles indicate that they are wealthy, or insurance might be offered at higher prices to consumers whose profiles indicate possible health risks. This practice, known as "web-lining," raises many of the same concerns that "redlining" and "reverse redlining" do in offline financial markets. *See, e.g.*, Rebuttal Comments of the Electronic Frontier Foundation (EFF) at 4 (expressing concern about "electronic redlining"); Tr. 81, Feena (describing technology's potential use for "red-lining" [sic]); Tr. 146-7, Steele (describing risk of "electronic redlining and price discrimination").

44. Tr. 186, Jaye; Tr. 192-193, Zinman.