ONLINE PROFILING: A REPORT TO CONGRESS

JUNE 2000

FEDERAL TRADE COMMISSION*

Robert Pitofsky	Chairman
Sheila F. Anthony	Commissioner
Mozelle W. Thompson	Commissioner
Orson Swindle	Commissioner
Thomas B. Leary	Commissioner

BUREAU OF CONSUMER PROTECTION

Division of Financial Practices

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

TABLE OF CONTENTS

I. INTRODUCTION

On November 8, 1999, the Federal Trade Commission (hereinafter "FTC" or "Commission") and the United States Department of Commerce jointly sponsored a Public Workshop on Online Profiling.[1] The goals of the Workshop were to educate government officials and the public about online profiling and its implications for consumer privacy, and to examine efforts of the profiling industry to implement fair information practices.[2] The Commission also sought public comment on any issues of fact, law or policy that might inform its consideration of the practice of online profiling.[3]

In keeping with its longstanding support of industry self-regulation, the Commission has encouraged the network advertising industry in its efforts to craft an industry-wide program. The industry has responded with working drafts of self-regulatory principles for our consideration. In examining the practice of online profiling, as well as our work in online privacy, we nonetheless recognize there are real challenges to creating an effective self-regulatory regime for this complex and dynamic industry, and this process is not yet complete.

This report describes the current practice of online profiling by the network advertisers[4] and

---

[1] 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]."

[2] *See FTC and Commerce Dept. to Hold Public Workshop on Online Profiling*, <http://www.ftc.gov/opa/1999/9909/profiling.htm>.

[3] *See* 64 Fed. Reg. 50813, 50814 (1999) (also available at <http://www.ftc.gov/os/1999/9909/ FRN990915.htm>).

[4] Not all profiles are constructed by network advertising companies (also known as online profilers). 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

the benefits and concerns it presents for consumers. It also discusses the ongoing effort of the industry to develop self-regulatory principles. The Commission expects to 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.

II. WHAT IS ONLINE PROFILING?

A. Overview

Over the past few years, 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[5] to $4.62 billion in 1999,[6] and were projected to reach $11.5 billion by 2003.[7] A large portion of that 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.[8] Currently, tens of billions of

---

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, direct relationship with the consumer, unlike third-party network advertising companies, and are beyond the scope of this report.

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

[6] *See* Internet Advertising Bureau, *Internet Advertising Revenues Soar to $4.6 billion in 1999* (available at <http://www.iab.net/news/content/revenues.html>).

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

[8] In 1999, 56% of all online advertising revenue was attributable to banner advertising. *See* Internet Advertising Bureau, *Internet Advertising Revenues Soar to $4.6 billion in 1999* (available at <http://www.iab.net/news/content/revenues.html>).

banner ads are delivered to consumers each month as they surf the World Wide Web.[9] 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. DoubleClick, Engage, and 24/7 Media, three of the largest Internet advertising networks, all estimate that over half of all online consumers have seen an ad that they delivered.[10]

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"[11] and "Web bugs" which track the individual's actions on the Web.[12] Among the types of

---

[9] DoubleClick, the largest network advertising company, estimates that it serves an average of 1.5 billion ads each day, for an average of approximately 45 billion ads per month. The next largest network advertisers, Engage and 24/7 Media, serve approximately 8.6 billion ads/month and 3.3 billion ads/month respectively. *See DoubleClick DART Now Serving on Average 1.5 Billion Ads Per Day*, <http://www.doubleclick.com/company_info/press_kit/pr.00.22.24.htm>; *Engage Reports Strong Growth in Key Metrics for Fiscal 2000 Second Quarter*, <http://www.engage.com/press/releases/2qfiscal.htm>; *24/7 Media, Inc.*, <http://www.247media.com/ index2.html>.

[10] *See, e.g.*, <http://www.doubleclick.com/company_info>; <http://www.engage.com/press/releases/2qfiscal.htm>; <http://www.247media.com/advertise/index.html>.

[11] A cookie is a small text file placed on a consumer's computer hard drive by a Web server. The cookie transmits information back to the server that placed it and, in general, can be read only by that server. For more information on cookies, *see, e.g.*, <http://www.cookiecentral.com>.

[12] "Web bugs" are 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 which 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*

information that can be collected by network advertisers are: information on the Web sites and pages within those sites visited by consumers; the time and duration of the visits; query terms entered into search engines; purchases; "click-through" responses to advertisements;[13] and the Web page a consumer came from before landing on the site monitored by the particular ad network (the referring page). All of this information is gathered even if the consumer never clicks on a single ad.

The information gathered by network advertisers is often, but not always, anonymous, *i.e.*, 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. This data is generally referred to as non-personally identifiable information ("non-PII"). In some circumstances, however, the profiles derived from tracking consumers' activities on the Web are linked or merged with personally identifiable information ("PII").[14] This generally occurs in one of two ways when consumers identify themselves to a Web site on which the network advertiser places banner ads.[15] 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

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>).

[13] When a consumer requests additional information about a product or service by clicking on a banner ad, she has "clicked through" the advertisement.

[14] 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.

[15] A previously anonymous profile can also be linked to personally identifiable information in other ways. For example, a network advertising company could operate its own Web site at which consumers are asked to provide personal information. When consumers do so, their personal information could be linked to the identification number of the cookie placed on their computer by that company, thereby making all of the data collected through that cookie personally identifiable.

Web site, the personally identifying information may be incorporated into a URL string[16] that is automatically transmitted to the network advertiser through its cookie.[17]

Once collected, consumer data can be analyzed and combined with demographic and "psychographic"[18] 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

---

[16] "URL" stands for Uniform Resource Locator.

[17] This kind of data transmission occurs when Web sites use the "GET" (as opposed to "POST") method of processing data. *See, e.g.*, Janlori Goldman, Zoe Hudson, and Richard M. Smith, California HealthCare Foundation, *Privacy: Report on the Privacy Policies and Practices of Health Web Sites* (Jan. 2000). It is not presently clear how personally identifiable information sent to network advertisers in a URL string as the result of "GET" technology is recognized, stored, or utilized.

[18] 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."

fields.[19]

Although network advertisers and their profiling activities are nearly ubiquitous,[20] 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.[21] 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.

B. An Illustration of How Network Profiling Works

Online consumer Joe Smith goes to a Web site that sells sporting goods. He clicks on the page for golf bags. While there, he sees a banner ad, which he ignores as it does not interest him. The ad was placed by USAad Network. He then goes to a travel site and enters a search on "Hawaii." USAad Network also serves ads on this site, and Joe sees an ad for rental cars there. Joe then visits an online bookstore and browses through books about the world's best golf courses. USAad Network serves ads there, as well. A week later, Joe visits his favorite online news site, and notices an ad for golf vacation packages in Hawaii. Delighted, he clicks on the ad, which was served by the USAad Network. Later, Joe begins to wonder whether it was a coincidence that this particular ad appeared and, if not, how it happened.

---

[19] 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>.

[20] 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>.

[21] 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.

At Joe's first stop on the Web, the sporting goods site, his browser will automatically send certain information to the site that the site needs in order to communicate with Joe's computer: his browser type[22] and operating system;[23] the language(s) accepted by the browser; and the computer's Internet address. The server hosting the sporting goods site answers by transmitting the HTTP[24] header and HTML[25] source code for the site's home page, which allows Joe's computer to display the page.

Embedded in the HTML code that Joe's browser receives from the sporting goods site is an invisible link to the USAad Network site which delivers ads in the banner space on the sporting goods Web site. Joe's browser is automatically triggered to send an HTTP request to USAad which reveals the following information: his browser type and operating system; the language(s) accepted by the browser; the address of the referring Web page (in this case, the home page of the sporting goods site); and the identification number and information stored in any USAad cookies already on Joe's computer. Based on this information, USAad will place an ad in the pre-set banner space on the sporting goods site's home page. The ad will appear as an integral part of the page. If an USAad cookie is not already present on Joe's computer, USAad will place a cookie with a unique identifier on Joe's hard drive. Unless he has set his browser to notify him before accepting cookies, Joe has no way to know that a cookie is being placed on his computer.[26] When Joe clicks on the page for golf bags, the URL address of that page, which discloses its content, is also transmitted to USAad by its cookie.

---

[22] For example, Netscape's Navigator or Microsoft's Internet Explorer.

[23] For example, Windows.

[24] Hypertext Transfer Protocol (the protocol for communication between Web browsers and Web servers).

[25] Hypertext Markup Language (the code/language in which most Web content is created).

[26] Because many sites require users to accept cookies in order to view their content, or make multiple attempts to place cookies before displaying content, the notification process may unacceptably frustrate consumers' ability to surf the Web efficiently.

When Joe leaves the sporting goods site and goes to the travel site, also serviced by USAad, a similar process occurs. The HTML source code for the travel site will contain an invisible link to USAad that requests delivery of an ad as part of the travel site's page. Because the request reveals that the referring site is travel related, USAad sends an advertisement for rental cars. USAad will also know the identification number of its cookie on Joe's machine. As Joe moves around the travel site, USAad checks his cookie and modifies the profile associated with it, adding elements based on Joe's activities. When Joe enters a search for "Hawaii," his search term is transmitted to USAad through the URL used by the travel site to locate the information Joe wants and the search term is associated with the other data collected by the cookie on Joe's machine. USAad will also record what advertisements it has shown Joe and whether he has clicked on them.

This process is repeated when Joe goes to the online bookstore. Because USAad serves banner ads on this site as well, it will recognize Joe by his cookie identification number. USAad can track what books Joe looks at, even though he does not buy anything. The fact that Joe browsed for books about golf courses around the world is added to his profile.

Based on Joe's activities, USAad infers that Joe is a golfer, that he is interested in traveling to Hawaii someday, and that he might be interested in a golf vacation. Thus, a week later, when Joe goes to his favorite online news site, also served by USAad, the cookie on his computer is recognized and he is presented with an ad for golf vacation packages in Hawaii. The ad grabs his attention and appeals to his interests, so he clicks on it.

III. PROFILING BENEFITS AND PRIVACY CONCERNS

A. Benefits

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.[27]

Network advertisers' use of cookies and other technologies to create targeted marketing programs also benefits 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.[28] Targeted advertising can also improve a consumer's Web experience simply by ensuring that she is not repeatedly bombarded by the same ads.[29] 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.[30]

Additionally, a number of commenters stated that targeted advertising helps to subsidize free content on the Internet. By making advertising more effective, profiling allows Web sites to charge

---

[27] The privacy issues raised by these uses of cookies are beyond the scope of this report. Data reflecting the use of cookies are reported in the FTC's recent report *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000) [hereinafter "2000 Report"], available at <http://www.ftc.gov/ reports/privacy2000/privacy2000.pdf> The Commission's vote to issue the 2000 Report was 3-2, with Commissioner Swindle dissenting and Commissioner Leary concurring in part and dissenting in part.

[28] *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.

[29] *See, e.g.*, Comments of the Magazine Publishers of America (MPA) at 1.

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

more for advertising. This advertising revenue helps to subsidize their operations, making it possible to offer free content rather than charging fees for access.[31]

Finally, one commenter suggested that profiles can also be used to create new products and services. First, entrepreneurs could use consumer profiles to identify and assess the demand for particular products or services. Second, targeted advertising could help small companies to more effectively break into the market by advertising only to consumers who have an interest in their products or services.[32]

In sum, targeted advertising can provide numerous benefits to both business and consumers.

B. Concerns

Despite the benefits of targeted advertising, there is widespread concern about current profiling practices.[33] Many commenters at the Workshop objected to network advertisers' hidden monitoring of consumers and collection of extensive personal data without consumers' knowledge or consent; they also noted that network advertisers offer consumers few, if any, choices about the use and dissemination of their individual information obtained in this manner. As one of the commenters put it, current profiling practices "undermine[] individuals' expectations of privacy by fundamentally changing the Web experience from one where consumers can browse and seek out information anonymously, to one where an individual's every move is recorded."[34]

The most consistent and significant concern expressed about profiling is that it is conducted

---

[31] *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.

[32] *See* Comments of Solveig Singleton at 4-5.

[33] 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.

[34] *See* Comments of the Center for Democracy and Technology (CDT) at 3.

without consumers' knowledge.[35] 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. This is true because, as a practical matter, there are only two ways for consumers to find out about profiling at a particular site before it occurs.[36] The first is for Web sites that use the services of network advertisers to disclose that fact in their privacy policies. Unfortunately, this does not typically occur. As the Commission's recent privacy survey discovered, although 57% of a random sample of the busiest Web sites allowed third parties to place cookies, only 22% of those sites mentioned third-party cookies or data collection in their privacy policies; of the top 100 sites on the Web, 78% allowed third-party cookie placement, but only 51% of those sites disclosed that fact.[37] The second way for consumers to detect profiling is to configure their browsers to notify them before accepting cookies.[38] One recent survey indicates, however, that only 40% of computer users have even heard of cookies and, of those, only

---

[35] *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.

[36] It is possible for consumers to learn about profiling after the fact by examining the cookie files on their hard drive; the text of a cookie will disclose the server that placed the cookie. Consumers can also delete the cookie files stored on their computers. Deletion will not erase any information stored by a network advertising company, but it will prevent future Web activity from being associated with past activity through the identification number of the deleted cookie.

[37] For purposes of the FTC's survey, third parties were defined as any domain other than the one survey participants were currently visiting, but the majority of the third-party cookies were in fact from network advertising companies that engage in profiling. The full results of the FTC study, as well as a description of its methodology, were released in the Commission's 2000 Report.

[38] Even for consumers who are aware of cookies, it is often difficult to discern how to change a browser's settings in order to receive notification of cookies. For example, in Netscape Navigator, a user must click on the "Edit" menu and select "Preferences" from the dropdown menu; select "Advanced" under the listing of categories; and click on a check-off box to activate the notification feature. In Internet Explorer 5.0, the user must click on the "Tools" menu and select "Internet Options" from the dropdown menu; click on the tab for "Security" options; click on "Custom Level"; then scroll down to the choices for cookies and select "Prompt."

75% have a basic understanding of what they are.[39]

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.[40]

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.[41] First, these commenters 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] This means that anyone who obtains access to ostensibly anonymous data – either by purchasing the data or hacking into it – might be able to mine the data and link it to identifiable individuals. Second, commenters feared that companies could unilaterally change their operating procedures and begin associating personally identifiable information with non-personally

---

[39] *See* BUSINESS WEEK ONLINE, BUSINESS WEEK/HARRIS POLL: A GROWING THREAT, *www.businessweek.com/2000/00_12/b3673010.htm* (March 20, 2000) [hereinafter "Business Week/Harris Poll"].

[40] *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. One commenter also worried that the existence of detailed personal profiles may facilitate an increase in identity theft. *See* Rebuttal Comments of the Electronic Frontier Foundation (EFF) at 4.

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

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

identifiable data previously collected.[43] Third, commenters noted that, regardless of whether they contain personally identifiable information, profiles are used to make decisions about the information individuals see and the offers they receive. These 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 (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).[44] This practice, known as "weblining," raises many of the same concerns that "redlining" and "reverse redlining" do in offline financial markets.[45]

Another concern expressed by commenters is that, as consumers begin to learn more about companies' monitoring activities, fear of online monitoring will discourage valuable uses of the Internet that are fostered by its perceived anonymity. As one commenter noted:

> The anonymity that the Internet affords individuals has made it an incredible resource for those seeking out information. Particularly where the information sought is on controversial topics such as sex, sexuality, or health issues such as HIV, depression, and abortion; [sic] the ability to access information without risking identification has

---

[43] *See* Comments of the Center for Democracy and Technology (CDT) at 2-3; 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.

[44] *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>.

[45] *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"); *see also* Marcia Stepanek, *Weblining: Companies are using your personal data to limit your choices – and force you to pay more for products*, BUSINESS WEEK ONLINE, Apr. 3, 2000, <http://www.businessweek.com/2000/00_14/b3675027.htm>. "Redlining" and "reverse redlining" are, respectively, the practice of some financial institutions to not extend credit or to offer less favorable credit terms to prospecitve borrowers in predominantly minority areas.

been critical.[46]

Indeed, in support of this point, this commenter cites studies that it believes suggest that, in both the online and offline world, the perceived anonymity of computer research facilitates access to these kinds of sensitive information.[47] By chilling use of the Internet for such inquiries, several commenters asserted, profiling may ultimately prevent access to important kinds of information.[48]

Finally, some commenters expressed the opinion that targeted advertising is inherently unfair and deceptive. They argued that targeted advertising is manipulative and preys on consumers' weaknesses to create consumer demand that otherwise would not exist, and that, as a result, targeted advertising undermines consumers' autonomy.[49]

Recent consumer surveys indicate that consumers are troubled by the monitoring of their online activities. First, as a general matter, surveys consistently show that Americans are worried about online privacy. Ninety-two percent say they are concerned about threats to their personal privacy when they use the Internet and seventy-two percent say they are very concerned.[50] Eighty percent of Americans believe that consumers have lost all control over how personal information is collected and used by companies.[51]

In particular, surveys show that consumers are not comfortable with profiling. A *Business*

---

[46] Comments of the Center for Democracy and Technology (CDT) at 19; *see also* Rebuttal Comments of the Electronic Frontier Foundation (EFF) at 4-5; Reply Comments of the Electronic Information Privacy Center (EPIC) at 2.

[47] *See* Comments of the Center for Democracy and Technology (CDT) at 19.

[48] *See* Comments of the Center for Democracy and Technology (CDT) at 19; Rebuttal Comments of the Electronic Frontier Foundation (EFF) at 4-5; Reply Comments of the Electronic Information Privacy Center (EPIC) at 2.

[49] *See, e.g.*, Comments of Robert Ellis Smith; Tr. 56-7, Catlett; Tr. 122, 148, Chester; Tr. 129-30, Smith.

[50] *See* LOUIS HARRIS & ASSOC., IBM MULTI-NATIONAL CONSUMER PRIVACY SURVEY (1999) [hereinafter "IBM Privacy Survey"], at 81.

[51] *See* IBM Privacy Survey, at 76.

Week survey conducted in March of this year found that 89% of consumers are not comfortable having their browsing habits and shopping patterns merged into a profile that is linked to their real name and identity.[52] If that profile also includes additional personal information such as income, driver's license, credit data and medical status, 95% of consumers express discomfort.[53] Consistent with the comments received in connection with the Public Workshop, consumers are also opposed to profiling even when data are not personally identifiable: sixty-three percent of consumers say they are not comfortable having their online movements tracked even if the data is not linked to their name or real-world identity.[54] An overwhelming 91% of consumers say that they are not comfortable with Web sites sharing information so that they can be tracked across multiple Web sites.[55]

Many consumers indicate that their concerns about the collection of personal information for online profiling would be diminished if they were given clear notice of what data would be collected about them and what it would be used for, and were given a choice to opt-out of data collection or of particular uses of their personal data. A recent survey by Privacy & American Business explained to Internet users that, in order to offer consumers personalized advertising, companies would need information about the consumer.[56] Internet users were then asked about their willingness to provide that information by: (1) describing their interests; (2) allowing the use of information on their Web site visits; (3) allowing the use of information on their Internet purchases; (4) allowing the use of information on their offline purchases; and (5) allowing the combination of online and offline purchasing information. When told that the company providing tailored ads would spell out how they would use the consumer's information and the consumer would be given a chance to opt-out of any

---

[52] Business Week/Harris Poll.

[53] Business Week/Harris Poll.

[54] Business Week/Harris Poll.

[55] Business Week/Harris Poll.

[56] *See* ALAN F. WESTIN, PRIVACY AND AMERICAN BUSINESS, PERSONALIZED MARKETING AND PRIVACY ON THE INTERNET: WHAT CONSUMERS WANT (1999) [hereinafter "Westin/PAB 1999"] at 8-9.

uses that he did not approve, a majority of consumers indicated willingness to provide personal information. With notice and choice, 68% were willing to describe their interests; 58% were willing to allow site visit data to be used; 51% were willing to allow use of online purchasing information; 53% were willing to allow use of offline purchasing data; and 52% were willing to allow the use of combined online and offline purchasing information.[57]

Although this survey indicates that, with appropriate notice and choice, many consumers would be willing to allow companies to use their personal information in order to deliver advertising targeted to the consumer's individual needs and interests, the statistics also demonstrate that many consumers are not willing to allow this kind of profiling regardless of whether notice and choice are given. A substantial minority of Internet users – between 32% and 49% – indicated that they would not be willing to participate in personalization programs even if they were told what would be done with their information and were given the choice to opt-out of uses that they did not approve.[58]

Internet users are also overwhelmingly opposed to the wholesale dissemination of their personal information. Ninety-two percent say that they are not comfortable with Web sites sharing their personal information with other organizations and 93% are uncomfortable with their information being sold.[59] Eighty-eight percent of consumers say they would like a Web site to ask their permission every time it wants to share their personal information with others.[60]

Ultimately, consumers' privacy concerns are businesses' concerns; the electronic marketplace will not reach its full potential unless consumers become more comfortable browsing and purchasing online. That comfort is unlikely to come unless consumers are confident (1) that they are notified at

---

[57] Westin/PAB 1999 at 8-9.

[58] Westin/PAB 1999 at 11. Consumers also want access to and control over their personal information. Eighty-three percent of Internet users say that it is important that companies engaged in tailored advertising programs allow participants to see their individual profiles and remove items that they do not want included; seventy percent felt that this was absolutely vital or very important. *Id*.

[59] Business Week/Harris Poll.

[60] Business Week/Harris Poll.

the time and place information is collected who is collecting information about them, what information is being collected, and how it will be used and (2) that they can choose whether their personal information is gathered, how it is used, and to whom it is disseminated.[61]

IV. THE FTC'S ROLE IN ADDRESSING ONLINE PRIVACY ISSUES AND SELF-REGULATION

A. Legal 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. 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.[62] 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.[63] Commerce on the Internet falls within the

[61] There may be complicated issues regarding the consequences of choice, such as the extent to which consumers may exchange use of their data for benefits.

[62] *See* 15 U.S.C. § 45(a).

[63] 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.

scope of this statutory mandate.

B. Online Privacy

As noted in Section III.B., the online collection and use of consumers' information, including the tracking of individual browsing habits, raise significant concerns for many consumers. These concerns are not new; since 1997, surveys have consistently demonstrated consumer unease with data collection practices in the online marketplace.[64] The Commission has responded to these concerns with a series of workshops and reports focusing on a variety of privacy issues, including the collection of personal information from children, self-regulatory efforts and technological developments to enhance consumer privacy, consumer and business education efforts, and the role of government in protecting online privacy.[65] The Commission's longstanding goal has been to understand this new

---

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).

[64] *See* 1998 Report at 3.

[65] The Commission held its first public workshop on online 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 issues and consumer protection issues, including privacy concerns. At a public workshop held in June 1996, the Commission examined Web site practices in 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

marketplace and its information practices and to assess its cost and beneficial effects. It has also used its law enforcement authority to challenge Web sites with deceptive privacy policy statements.[66]

In its 1998 report, *Privacy Online: A Report to Congress*, the Commission summarized widely-accepted principles regarding the collection, use, and dissemination of personal information.[67] These fair information practice principles, which predate the online medium, have been recognized and developed by government agencies in the United States, Canada, and Europe since 1973, when the United States Department of Health, Education, and Welfare released its seminal report on privacy protections in the age of data collection, *Records, Computers, and the Rights of Citizens*.[68]

---

issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

These efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. Further, the Commission and its staff have issued reports describing various privacy concerns in the electronic marketplace. *See, e.g.*, *Individual Reference Services: A Federal Trade Commission Report to Congress* (1997); FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (1996) ["1996 Staff Report"]; FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (1996); 1998 Report; Federal Trade Commission, *Self-Regulation and Online Privacy: A Report to Congress* (1999) [hereinafter "1999 Report"].

[66] *See ReverseAuction.com, Inc.*, Civil Action No. 000032 (D.D.C.) (Final Order, January 10, 2000) (available at <http://www.ftc.gov/ opa/2000/01/reverse4.htm>); *Liberty Financial Cos.*, Docket No.C-3891 (Final Order, Aug. 12, 1999) (available at <http://www.ftc.gov/opa/1999/9905/younginvestor.htm>); *GeoCities*, Docket No. C-3849 (Final Order, Feb. 5, 1999) (available at <http://www.ftc.gov/os/1999/9902/9823015d%26o.htm>).

[67] 1998 Report at 7-14. *See also* 1996 Staff Report at 8-12, available at <http://www.ftc.gov/reports/privacy/privacy1.htm> (summarizing participants' testimony on fair information practices).

[68] 1998 Report at 7-11. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The U.S. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977); Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980); U.S. Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, Privacy and the National Information Infrastructure: *Principles for Providing and Using Personal Information* (1995); U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995); *The European Union Directive on the*

The 1998 Report identified the core principles of privacy protection common to the government reports, guidelines, and model codes that had emerged as of that time:

> **(1) Notice** – data collectors must disclose their information practices before collecting personal information from consumers;[69]
>
> **(2) Choice** – consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;[70]
>
> **(3) Access** – consumers should be able to view and contest the accuracy and completeness of data collected about them;[71] and
>
> **(4) Security** – data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.[72]

It also identified Enforcement – the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices – as a critical ingredient in any governmental or self-regulatory program to ensure privacy online.[73]

The 1998 Report assessed the information practices of commercial Web sites and the existing self-regulatory efforts in light of these fair information practice principles and concluded that an effective self-regulatory system had not yet taken hold.[74] The Commission deferred judgment on the

---

Protection of Personal Data (1995); and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996).

[69] 1998 Report at 7-8; *see also* 1999 Report at 3-4; 2000 Report at 4.

[70] 1998 Report at 8-9; *see also* 1999 Report at 3-4; 2000 Report at 4.

[71] 1998 Report at 9; *see also* 1999 Report at 3-4; 2000 Report at 4.

[72] 1998 Report at 10; *see also* 1999 Report at 3-4; 2000 Report at 4.

[73] 1998 Report at 10-11; *see also* 1999 Report at 3-4; 2000 Report at 4.

[74] *See* 1998 REPORT at 41. In addition, the Commission recommended that Congress adopt legislation setting forth standards for the online collection of personal information from children; and

need for legislation to protect the online privacy of consumers generally, and instead urged industry to focus on the development of broad-based and effective self-regulatory programs.[75] One year later, the Commission issued a second report, *Self-Regulation and Online Privacy: A Report to Congress* ("1999 Report").[76] In the 1999 Report, a majority of the Commission again recommended that self-regulation be given more time, but called for further industry efforts to implement the fair information practices.[77] The Commission also outlined plans for future Commission actions to encourage greater implementation of online privacy protections, including the public workshop on online profiling.[78] In its 2000 Report, a majority of the Commission concluded that, despite its significant work in developing self-regulatory initiatives, industry efforts alone have been insufficient. Thus, the majority recommended that Congress enact legislation to ensure consumer privacy online.[79]

C. Online Profiling and Self Regulation: the NAI Effort

---

indeed, just four months after the 1998 Report was issued, Congress enacted the Children's Online Privacy Protection Act of 1998 ("COPPA"). On October 21, 1999, the Commission issued the Children's Online Privacy Protection Rule, which implements the Act's fair information practices standards for commercial Web sites directed to children under 13, or who knowingly collect personal information from children under 13. The Rule became effective on April 21, 2000.

[75] *See* 1998 Report at 41-42.

[76] *See* 1999 Report.

[77] The 1999 Report was issued by a vote of 3-1, with Commissioner Anthony concurring in part and dissenting in part.

[78] *See* 1999 Report at 13-14. Other actions contemplated by the Commission included the establishment of an advisory committee of industry representatives and privacy and consumer advocates to develop strategies to implement the fair information practices of access and security and to assess the costs and benefits of those strategies. The Advisory Committee on Online Access and Security was established in December 1999 and its final report was released as an appendix to the Commission's 2000 Report.

[79] *See* supra at n.27; 2000 Report at 34-38. The 2000 Report did not discuss and its legislative proposal does not address the unique issues raised by online profiling.

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.[80]

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.

IV. 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.

---

[80] Tr. 186, Jaye; Tr. 192-193, Zinman.