Request for Participation and Comment from the Electronic Privacy Information Center (EPIC)

Andrew Shen
Electronic Privacy Information Center (EPIC)
Tel: (202) 544-9240
Fax: (202) 547-5482
Email: shen@epic.org

Online Profiling Project - Request to Participate, P994809 / Docket No. 990811219-9219-01

Pursuant to the notice published by the National Telecommunications and Information Administration of the United States Department of Commerce and the Federal Trade Commission, Andrew Shen, on behalf of the Electronic Privacy Information Center (EPIC), formally requests participation as a panelist in Session III : The Role of Self Regulation in the Public Workshop on Online Profiling to take place on November 8, 1999.

EPIC is a public interest research center located in Washington, D.C. that has extensive expertise in privacy, particularly in federal regulation as it pertains to online communication.

EPIC reflects the public interest particularly well in this proceeding as it receives no financial support from any organization that would be directly affected by regulation of online profiling. Furthermore, while it is for the agency to determine the appropriate number of parties to participate in the workshop, it is our view that public concern about privacy matters must be given top priority in the upcoming public workshop.

Jason Catlett of Junkbusters and Ed Mierzwinski of United States Public Interest Research Group (US PIRG) are designated as parties who share group interests with Andrew Shen and EPIC.

Online Profiling Project - Comment, P994809 / Docket No. 990811219-9219-01

Comment follows below. All papers and surveys cited in the comment are publicly available at the footnoted URLs.

1. What types of companies are engaged in online profiling or in the development of online profiling technologies?

Virtually all e-commerce companies, whether selling products like Amazon.com, serving as a portal like Yahoo!, or advertising like DoubleClick attempt to create profiles on their customers.

Below is an excerpt from an article on e-commerce done by The Economist[1]. In the article, Jeff Bezos, the CEO of Amazon.com, is asked about the special nature of e-commerce and how it differs from traditional ways of transacting business.

> Getting to know all about you
>
> Despite the expense, all this feedback from customers has its rewards. Amazon now has a vast database of customers' preferences and buying patterns, tied to their e-mail and postal addresses. Publishers would kill for this stuff: they know practically nothing about their readers, and have no way of contacting them directly. That relationship has traditionally been monopolised by the bookshops, and even they rarely keep track of what individual customers like. Amazon offers publishers a more immediate link. "Ultimately, we're an information broker," says Mr. Bezos. "On the left side we have lots of products, on the right side we have lots of customers. We're in the middle making the connections. The consequence is that we have two sets of customers: consumers looking for books and publishers looking for consumers. Readers find books or books find readers."
>
> This is a generic model that could work in plenty of industries: anywhere with enough different products—and consumer tastes—to call for a big catalogue and a lot of advice. When Mr. Bezos started Amazon, he knew nothing about the book trade; he simply understood the power of electronic commerce. As a former financial analyst, he picked books because existing margins and distribution patterns seemed most favourable to an online business. In future, Amazon may expand into music and videos. Once you understand the model, the applications seem almost limitless.

[1] http://www.economist.com/editorial/freeforall/14-9-97/ec3.html

The business model that the author refers to is that of finding out as much as possible from the consumers -- the so-called creation of an online profile. Much of this is driven by the desire to target individuals likely to purchase items or respond to certain types of advertising. As almost all companies attempt to take advantage of targeting, almost all are actively creating online profiles.

2. What are the relevant business models?

Targeting specific individuals or groups to sell products or services is not a new phenomenon. Businesses and advertisers have long been trying to reach specific market segments through which they seek out the people most likely to purchase items. However, the Internet provides an unprecedented way to do so. Online profiling creates the ability to target or specialize advertising for services for individuals based on a new level of detailed analysis typically without the consumer's knowledge or consent.

For example, here are the statements posted by DoubleClick.net, one of the largest advertisers on the web, on the effectiveness and special features of online advertising.

From DoubleClick -

> Effectiveness Influencers[2]
>
> DoubleClick believes that there are many factors that influence the effectiveness of online advertising. Here, we have listed four which we feel are most influential to success. Whenever possible, we have attempted to develop products or services that help marketers react to these factors and leverage the true power of the Internet as a marketing medium.
>
> . . . .
>
> Targeting
> On the Internet your ability to target consumers leads to great efficiencies. You not only have the ability to reach only specific target audiences (avoiding waste), but also to learn more about your consumers so that you can target them more efficiently in the future. It is this process, the building of a one-to-one relationship which can truly make your effort a success.
>
> Research Findings: Banner Effectiveness Tips[3]

[2] http://www.doubleclick.net/learning_center/research_findings/influencers.htm
[3] http://www.doubleclick.net/learning_center/research_findings/effectiveness.htm

> Lesson 1: Target, Target, Target
> By utilizing the Web's ability to target, you can increase the effectiveness and efficiency of your online advertising efforts. You can deliver your message to specific industries, include or exclude specific geographic regions or cities, target by user interest and even control frequency. Through targeting, you can be sure that you are reaching your target audience, and only your target audience. Taking advantage of the Web's ability to deliver highly targeted audiences will help you generate leads and sales and create the one-to-one relationships which will extend and build your brand.

Before the Internet and other computer technology, it was impossible to gather so much information about consumers in such a secretive way and specialize the advertising offered to those individuals. But the advent of the World Wide Web has made it possible to collect and utilize information at the unprecedented level of the individual consumer.

3. What types of information are currently being collected by online profiling companies from or about Web site visitors?

Consumer profiling normally occurs through analysis of clickstream data, that is, information about which parts of the website are being clicked on or viewed by individuals surfing the web. Through such data, companies attempt to build a profile of consumer behavior, i.e. of what kinds of advertisements are most attractive, of what customers seek to buy online, etc. While this provides on the one hand the ability to create databases of new aggregate data about customers, clickstream data becomes more valuable as individual online profiles are associated with real individuals.

The association of online profiles with individuals is important as it allows businesses to target the people who they think are most likely to purchase certain products or services. Unlike normal consumer environments, the behavior of a person online is constantly being monitored and recorded so as to make possible the targeting of specific audiences. But, since the buyer and seller never face each other as in the offline world, identification is no longer based on visual recognition or casual familiarity. Instead, technologies have been developed which allow companies to uniquely identify people who surf the web and closely monitor their behavior.

4. What technologies do online profiling companies use to collect information about consumers? Please describe how these technologies function.

The creation of online profiles is not simply a matter of recording what a person sees on single, isolated visits to a website. An online profile is a continuing collection of online behavior that occurs despite disconnecting and then reconnecting later onto the Internet. An online profile provides a detailed history of personal behavior that was not possible in the offline world.

There are two ways that an online profiles of individuals are created. The first is through the use of Internet Protocol (IP) addresses, which is often recorded by websites. The second are cookies, special files that are stored on a Internet user's computer and are transmitted to websites. IP addresses provide a way for companies to track individual users online. Cookies allow for the unique identification of individuals over multiple visits to a particular site.

IP addresses:

Every computer connected to the Internet possesses an IP address. They provide a way for computers to find each other through the Internet. While we commonly search or identify websites by name such as http://www.epic.org, this is just a domain name or nickname to tell the computer to find the computer with the IP address 204.91.138.50. (You can just type in 204.91.138.50 into the browser window and you will arrive at the website for the Electronic Privacy Information Center just as if you had typed in http://www.epic.org.) Every computer connected to the Internet must have an IP address at all times.

All web servers record the IP addresses of computers that are looking at their website on logs. As soon as you enter http://www.epic.org, the server (or the computer that contains all the files for the website) records the IP address of the computer. Also, when you click on links to other parts of the website, that is also displayed on the logs. In this way, websites can keep track of what parts of the website are being looked at or what links are particularly interesting.

IP addresses are assigned to all computers connected to the Internet. These IP addresses are normally assigned by blocks. For example, Company A may possess IP addresses between 201.11.142.1 through 201.11.142.300. Different companies possess different blocks of IP addresses and the employees of company A can be identified as such by the logs maintained by the web server. In a real-world example, any person maintaining a website knows that someone from the Federal Trade Commission (FTC) is looking at their website if an IP address beginning with "164.62"[4] appears on their logs. However, it is impossible to discover which FTC employee is looking at the website without knowledge of which IP addresses were internally assigned to which computers. In a company or work environment, the anonymity of most people is protected by the number of people who also work in that company.

In the same vein, many people who have Internet access from home may not necessarily reveal their identity since many big Internet service providers (ISPs) such as America Online utilize dynamic IP addresses where different IP addresses are assigned to individuals every time they connect to the Internet. Someone who may have been using

[4] You can look up IP addresses at the following website at no charge. http://www.arin.net/whois/index.html

one IP address in one instance will be assigned a completely different one the next time they connect to the Internet.

However, the advent of broadband, "always on", access such as Digital Subscriber Line (DSL) or cable modems can not take advantage of the strong anonymity afforded by dynamic IP addresses since they do not connect then disconnect to the Internet. As broadband access grows in popularity, more and more individual home users will be associated with a single IP address. But, even in the realm of broadband access, a given IP address will not reveal an individual's identity. An IP address can only be tracked back to the ISP, not to the individual. The only entities that can correspond IP addresses to "offline" or real-world identities are the ISPs.

Cookies:

Utilizing IP addresses, cookies are a way of identifying unique Internet users over time. Cookies are files placed on your computer by the server containing a given website. Each cookie is assigned an individual number. The next time you connect to the website, the cookie is sent from your computer to the website when you connect. In that way, the website "knows" that the computer has visited the website before. One potential use of cookies is to keep track of the number of unique visitors to a website rather than the aggregate amount of visits or hits it may receive. Many sites also use cookies to customize websites. For example, Yahoo! offers a feature where individuals can create a customized page called "My Yahoo!"

Cookies exist for the purpose of allowing customizable pages and other conveniences -- like not having to log-in every time when connecting to a web-page -- but they also exist

for the purpose of collecting information about the user. Cookies do not contain personal information but the unique identification it provides allows for the potential association of clickstream data with a real individual.

5. Do these technologies currently enable creation of anonymous profiles?

As mentioned in the response to question 4, cookies and IP addresses do allow for the creation of anonymous profiles. However, many websites also ask for personal information and this data can later be correlated with a real identity.

Sharing personal information is often encouraged by web-sites. For example, at the very bottom of the registration for a customizable service called My Yahoo! there is a link to their privacy policy[5]. The first section of the privacy policy states that:

> Some personal information is gathered when you register. During registration, Yahoo! asks for your name, email address, birth date, gender, zip code, occupation, industry and personal interests. The more information you volunteer (and the more accurate it is), the better we are able to customize your experience. Once you register you are no longer anonymous to Yahoo! - you are given a Yahoo! ID and are able to take full advantage of Yahoo!'s many offerings.

After scrolling down the full My Yahoo! Privacy Policy, there are also links to resources on what privacy risks may be present, but there is a clear indication that Yahoo! pushes Internet users to provide as much personally identifiable information as possible.

Other companies that specialize in online advertising also collect personal information. For example, the Privacy Policy for online advertising giant DoubleClick states that "in the course of delivering an ad to you, DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address."[6] However, at odds with that policy, DoubleClick does admit to asking for personal information on a purely voluntary basis.

---

[5] http://docs.yahoo.com/info/privacy/
[6] http://www.doubleclick.net/privacy_policy/

More interesting is that on a different part of the website describing the effectiveness of past DoubleClick advertising campaigns, the company boasts of its ability to build a database of names, mailing addresses and email addresses for Bristol-Meyers. On the case study, the stated objective was to "build database of potential customers with lower cost per lead than traditional media."[7] To that end, DoubleClick claimed tripling the originally stated goal of registered names.

Anonymous profiles can be created through cookies and IP addresses, but companies often show an unwillingness to preserve that anonymity. Therefore, anyone who purchases any services or products over the Internet should be aware that their anonymity is at risk.

One can preserve anonymity by using various available technologies such as anonymizer.com[8]. Anonymizer.com is a subscription service that provides anonymous Web surfing and email service. The anonymity is provided through the use of proxy servers, which serves as an intermediary between an user and a website. Instead of directly connecting an individual to a website, the user operates through the proxy server, i.e. on the website logs, the IP address of the anonymizer proxy servers appears rather than that of the user. In this way, the behavior can not be uniquely identified with an individual since all the clickstream data corresponds to anonymizer servers and consequently anyone that is using that service. Other techniques to protect privacy are available at the EPIC web page -- Online Guide to Practical Privacy Tools[9].

[7] http://www.doubleclick.net/learning_center/case_studies/excedrin.htm
[8] http://www.anonymizer.com/3.0/index.shtml
[9] http://www.epic.org/privacy/tools.html

6. Do these technologies currently enable the creation of consumer profiles that identify individual consumers? Do the profiles include information originally collected anonymously but later linked to an individual? Are online profiling companies currently creating such profiles?

Technologies exist to create online profiles but many websites possess personal information that is often voluntarily given by consumers. When buying a book on Amazon.com, you must provide your name and address. Online profiles are not necessarily limited to clickstream data.

For example, the Amazon.com Privacy Policy[10] states that:

> When you order, we need to know your name, e-mail address, mailing address, credit card number, and expiration date. This allows us to process and fulfill your order and to notify you of your order status.

While not in itself harmful, providing personally identifiable information is fairly common through normal Internet transactions. Personal information is also joined to other forms of data about your behavior online. Amazon.com's Privacy Policy also mentions that:

> We personalize your shopping experience by using your purchases to shape our recommendations about the books, CDs, and other merchandise that might be of interest to you. We also monitor customer traffic patterns and site usage to help us develop the design and layout of the store.

However, Amazon does not disclose to customers exactly what information is collected, nor does it give customers access to this information. In this respect, Amazon violates one of the main principles of Fair Information Practices.

[10] http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html/ref=gw_m_ln_nh_pp/002-7876636-5573867

7. Are there technologies in development that will enable the creation of consumer profiles that identify individual consumers? If so, please describe.

Even if one does not purchase any items that require revealing personal information, other techniques exist to correlate online profiles with real individuals. Data mining, which utilizes artificial intelligence (AI) algorithms, can associate online profiles with real individuals. Individual consumers may not be named, but their behavior can be monitored, recorded and analyzed on a person by person basis. While a company may never know their name, companies can still exert control over consumers at the level of the individual.

Many products are taking advantage of the new marketing opportunities and technologies offered by online advertising. One such product is Ultramatch™[11], which has run analyses on users of Infoseek, a popular search engine and portal for the Internet. Their approach to learning about their market is similar to other products newly available to analyze Internet use.

Ultramatch™[12] begins by assigning every user a "behavioral fingerprint" that provides unique identification.

> The analogy to real fingerprints is quite accurate. A real fingerprint is an anonymous yet unique data point. We all leave fingerprints on everything we touch every day. The fingerprint by itself is innocuous – it does not disclose identity, tastes, attitudes, or incomes. Like a real fingerprint, a "behavioral fingerprint" is a unique trace left by each person that allows everyone to have his or her own unique and anonymous identity.

[11] http://info.infoseek.com/doc/ultramatch/Introduction.html
[12] http://info.infoseek.com/doc/ultramatch/Introduction.html

The "behavioral fingerprint" probably operates using a cookie, which provides unique identification and can also keep track of information of interest to businesses like clickstream data. However, despite the analogy between real and "behavioral" fingerprints, "behavioral fingerprints" are different in that they do simultaneously provide unique identification and historical behavior. While real fingerprints can be tied to a name and other personal information, all the information is located in different locations. "Behavioral fingerprints" allow access to information and identification at once.

8. How is the information collected by online profiling companies used?

In the words of the Ultramatch™ promotional material, "Ultramatch technology allows us to understand the reach and frequency of individual behavior groups at micro-behavioral level." Due to the increase in technology and collection of personal data, it is easier to gain insight into the behavior of smaller and smaller market segments. While it is difficult to design marketing for a large group of people, by focusing on smaller and smaller groups of individuals, companies can more closely monitor the behavior of their customers. Before the Internet and online profiles, companies would have to rely on surveys or other sorts of mass data collection. Online profiling provides an unprecedented way of learning about online behavior at a detailed level.

At issue is the fact that in those earlier times, individuals would have known that they were releasing information to companies. However, currently, many types of data collection and profiling proceed without a customer's knowledge or control.

9. Is the information collected by online profiling companies being merged with other databases? If so, what kinds of information are included in such databases? How is the merged information being used?

While IP addresses and cookies present potential ways to correspond online customer profiles with offline identities, mergers between online advertisers and offline companies present a much larger and starkly invasive manner in which a person's identity will become common knowledge on the Internet.

On June 14, DoubleClick Inc. announced a merger with the Abacus Direct Corporation. DoubleClick is an online advertiser that uses cookies to track customer behavior online and create customer profiles. Abacus Direct is an offline company that collects information about consumers' purchasing habits through a database that tracks catalog subscriptions and purchases. Through this database, Abacus knows your credit card numbers, personal address, telephone number and information about your household income, family makeup and other habits. The merger of these companies puts a lot of information, including both personal and demographic data, in the hands of advertisers. In just one month -- December of 1998 -- 45.8% of all online users in the United States, reaching 48 million people, received a cookie from DoubleClick. Abacus possesses more than 88 million five-year buying profiles. The merging of these two databases of information creates the ability to not only obtain personally identifiable information, but a way in which to know the online behavior of real individuals.

The application of this information to the online world reveals the entirely different nature of online advertisement. Online advertisers attempt to target their advertising as much as possible and that involves the use of customer profiling. Huge mergers, such as

the one between DoubleClick and Abacus, have resulted in a pervasive new business practice -- that of targeting individuals on the basis of previous buying behavior. There are two important facts to note of this phenomenon.

The first is that DoubleClick and Abacus never entered a relationship with the people about which they have information. For example, I may enter into a relationship with Amazon.com, my shopping for and purchasing book from them, that may result in my giving Amazon.com personal information such as my name and my address and general information about the topics in which I am interested. DoubleClick and Abacus on the other hand obtain information about people by monitoring their behavior online. Online advertisers have no direct relationship with customers.

The second notable fact about online advertising is there is no offline equivalent for the approach that these online advertisers take. The only imaginable offline parallel was if someone was secretly following you around as you shopped around a mall and taking notes on what caught your interest. We would certainly find that an objectionable practice on the part of businesses and on government through inaction, but the online version of this monitoring is taking place -- but just without us noticing.

10. What are the costs and benefits, to both industry and consumers, of online profiling? Given the fluidity of electronic commerce models and the absence of hard data, it is difficult to assess the precise costs and benefits for online profiling. It is clear, however, that there are some significant risks in online profiling.

Reliance on online profiling could result in marketing items completely on the basis of profiles, which are essentially based on past consumer behavior. In this way, it restricts the ability of people to receive notices about items, which they have not previously expressed, interest. Also, online profiles may cause individuals to lose the ability to compare similar products from different companies. Instead of finding out about the best products, consumers may be forced to purchase products from companies that have created the most complete online profile, and thus the best idea of whom might want to purchase such a product.

These possibilities and an instinctive customer discomfort with the collection of information can only have negative effects on online business. The future of electronic commerce not only relies on the practicalities of implementing new ways of conducting business but also the ability of customers to become comfortable with these new processes. The collection of information pertaining to individuals and their behavior play a significant role in undermining the trust of consumers in electronic commerce. The lack of legally enforceable protections on customer information can not result in anything less than the continuing distrust of consumers in a new industry.

11. What are consumers' perceptions about online profiling? Please provide the results of any studies or surveys addressing this question.

In a paper entitled "Building Consumer Trust in Online Environments: The Case for Information Privacy"[13], (produced by the Project 2000 Research Program on Marketing in Computer Mediated Environments at the Owen School Graduate School of Management, Vanderbilt University) the authors examine some reasons why individuals who begin an online transaction never finish them.

They found the major reasons for consumer hesitancy are worries about security and information privacy. Security fears arise from the possibility that a computer hacker may be able to steal valuable information such as credit card numbers. Information privacy is a concern due to the perceived lack of ability to control their personal information, i.e. that this information may be sold or distributed to third parties.

The paper relies heavily on the GVU 7th WWW User Survey conducted in 1997 and which sampled a population of 14,014 self-selected respondents. Here are some of the results of that survey:

87% of Web users think they should have "complete control" over demographic information captured by websites
71% believe there should be new laws to protect their privacy online
63% of those who do not provide personal information to websites reportedly do so because out of a lack of trust
94% of Web users have declined to provide personal information at least once
40% have fabricated false demographic data when requested by a website
81% of Web users do not want websites to resell personal information

In the words of the authors,

[13] http://ecommerce.vanderbilt.edu/papers/CACM.privacy98/CACM.privacy98.htm

> . . . commercial Web sites are their own worst enemies. Contrary to the conventional wisdom, the enabling conditions for giving up information are not product discounts, access to the site, or value-added services. Indeed, fully two-thirds to three-quarters of all Web users are decidedly uninterested in selling their personal data to Web sites for monetary incentives or access privileges. In other words, *consumers do not view their personal data in the context of an economic exchange of information*, as many commercial Web providers believe. [emphasis theirs]

These survey results not only demonstrate the concern that most Web users have about the demographic information obtained by websites but also their control over that information. Indeed, many websites would be disappointed to find that the information that they attempt to collect is often false. Continued attempts to profile customers and their behavior have created a growing distrust of websites and consequently harm the future growth of electronic commerce.

12. What are the beneficial uses of the information collected by online profiling companies?

see 10.

13. Are consumers' privacy interests implicated by the collection, compilation, sale and use of information collected by online profiling companies? If so, please describe.

Online profiling has potentially huge adverse consequences for privacy. Online profiling in its detailed description of online behavior can contain valuable personal information. Histories of consumer behavior can shed light on interests, hobbies or goals. They may also reveal medical conditions, sexual preferences, and political or religious beliefs.

Furthermore, the acquisition of online profiles threatens consumer control over this information. Many people are not aware to the extent to which this information is being collected and to which it may distributed. Consumers should have the right to control their own information and any collection, sale or use of that information.

Online profiling has become practice despite these concerns due the lack of enforceable legal safeguards on privacy. As exhibited by the results of the GVU survey, consumers are overwhelmingly against the unregulated collection of personal data. Nonetheless, people are forced to interact with companies that continue to develop online profiles because all companies online practice such behavior. Given a situation where consumers are hesitant about using the Internet due to their concerns about privacy and not using online companies at all -- many consumers are doing what the report from Project 2000 describes, completing transactions less often than they would if they were assured that their privacy were legally protected.

14. Do online profiling companies disclose the ultimate uses of the information they collect? If so, what is the nature of such disclosures? Where possible, please provide examples of such disclosures.

Online profiling companies rarely disclose the actual use of personal information. Typically, web sites provide a 'privacy policy' that is vague, legalistic, and provides little useful information[14]. As the following excerpts from the Yahoo! privacy policy demonstrate, the ability of the individual to control their information is eroded by companies that choose to share information with third parties with which individuals have no intention of conducting business. The ultimate use and distribution of the information quite possibly may never be known.

For example, the privacy policy states, "Yahoo! may disclose your personal information to business partners or sponsors, but this is specifically described to you prior to data collection or prior to transferring the data."[15] This type of policy undercuts any expectations that consumers might have about the ability to control their information. Being notified about when your information is being transferred is not comforting when you may not want that information transferred at all.

---

[14] Often, but not always, websites will have "Privacy Policies" that let users know what information is being collected and how it may be used. The Georgetown Internet Privacy Policy Survey (http://www.msb.edu/faculty/culnanm/GIPPS/gipps1.PDF), conducted in June 1999, investigates the presence of privacy policies and the information contained within those policies. The survey looked at a sample of 361 of the 7500 most popular websites.
The survey found that only one third of the sites did not any notice of any kind about what they do with users' information. Of those that posted any sort of policy, the survey discovered that only 13.6% of them (32 out of the total of 361 websites) mentioned all the minimum five elements that concern information privacy: notice, choice, access, security, and contact information.
However the lack of Privacy Policies, did not keep many websites from collecting information. Almost 93% of sites collected personal information (defined as email address, mailing address, or name). Almost 57% sought demographic information such as gender or geographic area. The majority of websites, 56.2% collected both types of information. Only a very small minority of 6.6% of websites chose not to collect any type of information.

[15] http://docs.yahoo.com/info/privacy/

At the end of this section of the policy, after denoting no less than five other types of entities to which Yahoo! may disclose personally identifiable information, Yahoo! also creates a dispensation to reveal information to other entities "for administrative and other purposes that we deem necessary to maintain, service, and improve our products and services." This is a vague and indiscernible statement about when personally identifiable information can be used. When there are no legal protections for information, the user will continue to remain in the dark about the ultimate use of their personal information.

15. Do online profiling companies provide effective mechanisms for a consumer to remove his or her information from their databases or otherwise control the use of such information?

No. Consumers are typically unaware of organizations that are creating these profiles and there is also no effective means to limit profiling techniques. The absence of meaningful legal protections under a self-regulatory regime provides no reassurance that the consumer can remove their own information from databases or exercise any other types of control.

16. Do online profiling companies provide consumers an opportunity to choose whether and how their information will be collected and used? If so, please describe the choices that consumers are given and how consumers can exercise these choices.

Online profiling companies do provide an opportunity for choice, but the opportunity often remains unknown to the consumer. Many companies offer the option to opt-out of databases. An opt-out policy lets consumers send an email or another sort of notification to the company that will remove the customer and their information from the database. Opt-out places the entire burden of protecting information on the consumer and the individual rather than the business. The ability to opt-out is often not displayed clearly and prominently on websites. Due to the obscurity of opt-out policies, they are not effective in providing meaningful control over personal information. When a consumer has to perform research and decipher privacy policies to avail themselves of their own rights not to be included in these databases, they do not have effective control over their information. For that reason, opt-in policies, where a consumer has to explicitly express their desire to be included on databases, should be the de facto standard.

17. What is current industry practice, with respect to information already collected from individuals, when there is a later change in the company's policies? What is the current industry practice, with respect to information already collected from individuals, when there is a material change in the corporate structure or business contracts governing such information, such as through a merger, joint venture, or sale of customer lists? Do online profiling companies provide notice and choice with respect to how already-collected information is handled under changed circumstances?

Even considering the less than encouraging ratio of companies that collect information compared to those who post no policy whatsoever, it is important to remember that there is no legal guarantees that any websites will follow the guidelines set out in privacy policies. It is quite possible that a company will simply not follow what they claim to be practicing or may simply change their privacy policy after a time. In either case, companies still have the information that individuals have given them. For example, the privacy policy for My Yahoo! states simply at the top of the page that, "please read the following policy to understand how your personal information will be treated as you make full use of our many offerings. This policy may change from time to time so please check back periodically."[16]

[16] http://docs.yahoo.com/info/privacy/

18. What, if any, legal or other practical issues would be implicated in the creation of effective self-regulatory programs to govern the sorts of changed circumstances described in Question 16?

Effective protection and control of personal information can not take place without legal enforceability of privacy policies. In the situation that exists now, where consumers have no guarantee of finding out the ultimate use of their information (see question 14), no expectation of easy and explicit ways to remove their information (see question 15), no clear choices in terms of information collection (see question 16), and no recourse if a policy or practice suddenly changes (see question 17) -- the current policy self-regulation clearly gives no meaningful protection of personal information. Self-regulation gave rise to online profiling techniques that are now beyond the control of users. Action is needed to provide a satisfactorily safe online environment for consumers.

19. Do online profiling companies provide consumers the opportunity to see what information has been collected from or about them and the ability to correct errors? If so, please describe.

Even companies with privacy policies do not disclose the actual content of the profile that is created by the company. Typically, firms will describe the general nature of the information collection (e.g., name, address, etc.), but will never actually display the profile with the complete listing of data elements.

20. What procedures have online profiling companies instituted to maintain the security of the information they collect?

Privacy policies, if they exist, sometimes provide information on the security procedures of online profiling companies. But a good security policy says little about how the information might be routinely disclosed to others.

21. What self-regulatory efforts have online profiling companies undertaken to address concerns raised by their collection, compilation, sale, and use of consumer information? How do these efforts address the fair information practice of notice, choice, access, security, and enforcement? What are the costs and benefits, to both consumers and businesses, of such self-regulatory efforts?

In response to customer concerns, some online companies have attempted to create various coalitions and programs as a form of "self-regulation" that hopes to take the place of legal guarantees of privacy protection.

TRUSTe is one "non-profit" agency that seeks to promote self-regulation through trustmarks. TRUSTe will allow companies to display the TRUSTe trustmark only if companies have agreed to their privacy principles and consumer resolution process. A short statement of their principles is displayed on their FAQ[17]:

> A displayed trustmark signifies to online users that the Web site will openly share, at a minimum, what personal information is being gathered, how it will be used, with whom it will be shared, and whether the user has an *option to control its dissemination.* [emphasis added]

It should alarm consumers that the principles that TRUSTe upholds do not even presume that users should have control over the use of their information.

Also startling is that, as reported in the June 18, 1999 issue of Privacy Times[18], a Federal portal called www.students.gov had to remove the TRUSTe seal from its website because the requirements of the 1974 Privacy Act -- which set limits on what personal information the Federal government could collect -- were not met by TRUSTe.

[17] http://www.truste.org/about/about_faqs.html
[18] http://www.privacytimes.com

22. Are there any efforts currently underway or planned to educate consumers and businesses about online profiling? If so, please describe.

Organizations such as EPIC serve as a resource for both consumers and businesses about the possible adverse results of online profiling. There are also many other organizations that provide such information.[19]

EPIC also supports the effort of the Federal Trade Commission and the National Telecommunications and Information Administration of the U.S. Department of Commerce in organizing the Online Profiling Workshop. Such events play an important role in educating the public and providing a forum for continued discussion of these issues.

[19] For a list of these organizations, please see http://www.epic.org/privacy/privacy_resources_faq.html#Privacy_Organizations.