S. HRG. 106–1117

ONLINE PROFILING AND PRIVACY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JUNE 13, 2000

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

82–146 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JOHN McCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
SLADE GORTON, Washington
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
JOHN ASHCROFT, Missouri
BILL FRIST, Tennessee
SPENCER ABRAHAM, Michigan
SAM BROWNBACK, Kansas

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
RICHARD H. BRYAN, Nevada
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
MAX CLELAND, Georgia

MARK BUSE, *Republican Staff Director*
MARTHA P. ALLBRIGHT, *Republican General Counsel*
KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*

CONTENTS

	Page
Hearing held on June 13, 2000	1
Statement of Senator Bryan	5
Statement of Senator Burns	2
Statement of Senator Cleland	40
Prepared statement	43
Statement of Senator Hollings	3
Prepared statement	4
Statement of Senator Kerry	44
Statement of Senator McCain	1
Prepared statement	2
Statement of Senator Wyden	5

WITNESSES

Bernstein, Jodie, Director, Bureau of Consumer Protection, Federal Trade Commission, (Accompanied by David Medine, Associate Director for Financial Practices, Bureau of Consumer Protection, Federal Trade Commission and Dawne Holz, Federal Trade Commission)	6
Prepared statement of Jodie Bernstein	9
Polonetsky, Jules, Chief Privacy Officer, Doubleclick	47
Prepared statement	49
Jaye, Daniel, Chief Technology Officer, Engage Technologies	50
Prepared statement	52
Rotenberg, Marc, Director, Electronic Privacy Information Center	55
Prepared statement	57
Smith, Richard, Internet Consultant	71
Prepared statement	73

APPENDIX

Markowitz, Steve, Chairman and CEO, MyPoints.com, Inc., prepared statement	97
Smith, Richard, Internet Consultant, additional testimony	98

ONLINE PROFILING AND PRIVACY

TUESDAY, JUNE 13, 2000

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m. in room SR–253, Russell Senate Office Building, Hon. John McCain, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

The CHAIRMAN. Good morning. This morning the Committee will hear testimony on online profiling done by Internet network advertisers and how it impacts consumers' privacy. I welcome and thank all the witnesses we will hear from today. Your testimony will help the Committee gain a better understanding of the issues involved and the appropriate action the Committee should take.

As has been said so often, the Internet continues to transform our lives and our economy. Each day more and more Americans access the web to shop, read the news, find a job, or for a variety of other reasons. The Internet continues to offer great opportunities to consumers, but it also raises concerns about individual privacy.

Online profiling, and specifically profiling done by network advertisers, raises serious privacy concerns among many consumers. Through the use of cookies and other technologies, network advertisers have the ability to collect and store a great deal of information about individual consumers. They can track the websites we visit, the pages we view on websites, the time and duration of our visits, terms entered into search engines, purchases, responses to advertisements, and the page we visited before coming to a site.

All of this information can be collected without clicking on an advertisement. In fact, often this information is collected without the consumer's knowledge or consent. The FTC noted in its May report on online privacy that just 22 percent of websites that allow the placement of third party cookies provide notice to customers. Recently, *USA Today* noted in a May 1st article that, even when consumers are aware of this practice, it can be extremely difficult to opt out of the collection of this data.

While online profiling raises serious privacy concerns, some consumers desire this service and benefit by receiving targeted advertisements that appeal to them. What we need to find is the delicate balance between benefiting consumers and invading their privacy, and I am hopeful that today's witnesses will help us eventually find that balance. I look forward to the testimony presented today.

Senator Burns, thank you for being here.

[The prepared statement of Senator McCain follows:]

PREPARED STATEMENT OF HON. JOHN MCCAIN,
U.S. SENATOR FROM ARIZONA

This morning, the Committee will hear testimony on online profiling done by Internet network advertisers and how it impacts consumers' privacy. I welcome and thank all of the witnesses we will hear from today. Your testimony will help the Committee gain a better understanding of the issues involved and the appropriate action the Committee should take.

As has been said so often, the Internet continues to transform our lives and our economy. Each day more and more Americans access the web to shop, read the news, find a job or for a variety of other reasons. The Internet continues to offer great opportunities to consumers, but it also raises concerns about individual privacy.

Online profiling and specifically profiling done by network advertisers raises serious privacy concerns among many consumers. Through the use of cookies and other technologies, network advertisers have the ability to collect and store a great deal of information about individual consumers. They can track the websites we visit; the pages we view in websites; the time and duration of our visits; terms entered into search engines; purchases; responses to advertisements and the page we visited before coming to a site. All of this information can be collected without clicking on an advertisement.

In fact, often this information is collected without the consumer's knowledge or consent. The FTC noted in its May report on online privacy that just 22% of websites that allow the placement of third party cookies provide notice to consumers. Recently, *USA Today* noted in a May 1st article that, even when consumers are aware of this practice, it can be extremely difficult to opt out of the collection of this data.

While online profiling raises serious privacy concerns, some consumers desire this service and benefit by receiving targeted advertisements that appeal to them. What we must find is the delicate balance between benefiting consumers and invading their privacy. I am hopeful that today's witnesses will help us eventually find that balance.

I look forward to your testimony and to working with all of you to address this vital issue.

STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. Thank you, Mr. Chairman, and I thank you for holding this hearing. It's very timely, too, because it does concern something of vital importance to today's digital era, so to speak, the protection of online privacy.

While the Internet is growing at an amazing rate and it offers educational and commercial opportunities to millions of Americans, new information technologies have allowed the collection of personal information on an unprecedented scale. Many times this information is collected without the knowledge of consumers. Online profiling poses particular concerns, especially when these profiles are merged with offline information to create massive individualized databases on consumers.

Given the continuing erosion of Americans' privacy, I am more convinced than ever that legislation is necessary to protect and empower consumers in the online world. Privacy is not a partisan issue, but a deeply held American principle.

I would like to thank Senator Wyden for his hard work on this and many other related issues, including spamming and encryption, when we start dealing with the Internet. Over year ago, Senator Wyden and I introduced the Online Privacy Protection

Act, which was based on our shared view that, while self-regulation should be encouraged, we also need to provide strong enforcement mechanisms to punish bad actors. In short, the approach should be trust but verify.

I have grown increasingly frustrated with the industry's continuing stance that no legislation is necessary, even in the face of overwhelming public concern. Just last week, during his address to the Internet Caucus, Bill Gates claimed that the Burns–Wyden bill goes too far and that the time is still not right for privacy legislation. Unfortunately, his view is nearly unanimous among the technology industry.

Senator Wyden has been engaging in the discussions with industry for well over a year and we continue to hear nothing more than how self-regulation is working. The need for privacy legislation has increased over the last year, not decreased. I want to reiterate my commitment to moving strong privacy legislation to protect consumers whether industry agrees or not.

I commend the Federal Trade Commission for recognizing the industry has failed to produce progress and finally calling for legislation itself. The Commission's recent report to Congress revealed the extent of the stunning lack of consumer privacy on the Internet. Even among the 100 most popular websites, only 42 percent have implemented fair information practices to ensure consumer privacy. Among a broader random sample of all commercial websites, the number drops dramatically to 20 percent compliance.

Several industry representatives have argued that the increase in privacy policies being posted by websites reveals that no privacy legislation is necessary. While the majority of commercial websites now post privacy policies, the difference between posting a privacy policy and actually providing real privacy to users can be huge. While I applaud the increase in posting of those privacy policies, many of them are overly complex and they are technical. I never cease to be amazed when you click one and then 20 pages of legalese comes up. I have never been hinged with the title "lawyer," so I don't even try to work my way through the thing. I find it interesting that the Commission itself had to use teams of lawyers to decipher the privacy policies of many websites in the preparation of its report.

So, Mr. Chairman, I want to thank you for holding this hearing. Also, I remain open to working with Senator Wyden and the rest of my colleagues on this Committee. I am more committed than ever that we should move a privacy bill forward. And I thank the Chairman.

The CHAIRMAN. Senator Hollings.

STATEMENT OF HON. ERNEST F. HOLLINGS, U.S. SENATOR FROM SOUTH CAROLINA

Senator HOLLINGS. I thank you, Mr. Chairman. I will file my statement for the record. Thank you.

[The prepared statement of Senator Hollings follows:]

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

I want to thank Chairman McCain for holding this hearing, the third this Committee has conducted in this Congress on the important issue of Internet privacy. Today we examine the troubling privacy implications raised by the practice of "online profiling." While many commercial entities collect data about individuals on the Internet, the practice of profiling, particularly as it is conducted by network advertisers, threatens individual privacy in a manner that raises serious concerns, and warrants special consideration by this Committee.

On the Internet, individuals knowingly initiate relationships with Internet service providers or commercial websites. For example, they join AOL or subscribe to *The New York Times* online, or visit the search portal Yahoo. Third party network advertisers, however, collect and use individuals' personal information but almost never possess a direct relationship with those individuals. Instead, these advertisers reach through the site and collect information about individuals—most likely without notice or consent—by placing "cookies" on users' computers that then track their every move on the Internet. The advertisers then examine the contents of these "cookies" so as to collect and analyze the results of this surreptitious monitoring.

For the most part, Internet users are completely unaware that this surveillance is occurring. And yet this surveillance allows the advertisers to collect and compile incredibly detailed profiles of individual's tastes, preferences, and research habits as observed throughout the Internet. To make matters worse, these same companies may use the actual information they have collected to develop so called "psycographic" profiles that reflect the companies' inferences and conclusions about the individual's interests, habits, associations, and traits. Such a profile by its very nature includes predictive information about an individual that the individual has not, in fact, personally provided, and which may not be an accurate characterization of that individual at all. And all this is going on without any real informed notice or consent on the part of the individual who is being monitored.

If I purchased a pair of shoes, and a computer chip in the sole monitored every place I walked, and then others collected used that information to target me with "personalized" advertisements, I would be outraged. If a phone company tape recorded my conversations and then used my statements to market products to me I would be irate. And yet such obviously unacceptable practices in the traditional marketplace are appropriate analogies to the activities practiced by network advertisers on the Internet. The fact that individuals often use the Internet in the quiet seclusion of their homes only exacerbates the sense of trespass occasioned by these activities.

Of course, not all sharing of information is bad. Some people probably desire targeted, personalized advertisements. The magic of the Internet makes that possible to a degree we never before experienced. However, the use of individuals' personal information to purportedly improve their Internet experience is only appropriate if the individual has been informed, and has made a conscious decision to consent to that practice. As we will learn today, that is not currently the case in the marketplace.

Moreover, there are no sensible limits in place to ensure that individuals' personal information is, in fact, only used for relatively benign purposes, such as commercial advertisements. As *The New York Times* reported on February 2, 2000, 19 out of the top 21 health sites on the Internet had privacy policies but had unwittingly shared users' personal information with third parties through "cookies" that had been placed on the sites by network advertisers. Simply put, we need federal legislation to ensure that these violations do not occur.

Some network advertisers do not collect personal information and instead target their marketing only to computers or Internet protocol addresses about which they have developed an anonymous profile. Although this practice demonstrates that these entities can function without collecting personal information, we must examine this activity, as well, to determine any possible risk it poses to individuals on the Internet.

Again, I thank the Chairman for calling this hearing and look forward to the testimony of the witnesses.

The CHAIRMAN. Thank you, sir.

Senator Wyden.

STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON

Senator WYDEN. Mr. Chairman, I will be very brief. First let me say that I share Senator Burns' view that it is time to move on with a bipartisan bill to address these privacy issues. He and I have worked for more than a year with a variety of groups, business and others, toward that effort.

I happen to think Senator Hollings and Senator Rockefeller have made an excellent contribution, have constructive ideas. Senator Kerry has ideas on this matter. The clock is ticking down on this session, and I think we ought to go forward with a bipartisan privacy bill.

Now, today's session it seems to me is particularly important. Most of what we have looked at is personal data that a consumer provides to websites he or she visits—such as name, address, and personal information supplied in order to purchase a product or register for a service online. The practice that we are looking at today is different in that it frequently involves the collection and compilation of information by third parties, companies whose websites the consumer has never visited, but who are nonetheless constructing profiles of the consumer's Internet habits.

I am of the view that online profiling does raise difficult and troublesome issues. The mere fact that consumers often are not aware of the profiling is troubling enough, but even more serious is the prospect that a company might try to merge online profile data with personally identifiable data, producing detailed sets of information about specific individuals. We have already seen that represented in the debate about DoubleClick.

Finally, Mr. Chairman, it seems to me that there is a role for self-regulation. All of the bills try to give a wide berth for self-regulation, and I believe that programs like TRUSTe have made a difference. But I continue to believe that, absent legislation, meaningful enforcement, and air-tight coverage, we will continue to vitiate a lot of the constructive work that is being done by the privacy sector. That is why I think we ought to go forward with bipartisan legislation.

Mr. Chairman, I look forward particularly to working with you and Senator Hollings as the leadership of this Committee to get it done, and I yield back.

The CHAIRMAN. Senator Bryan.

STATEMENT OF HON. RICHARD H. BRYAN,
U.S. SENATOR FROM NEVADA

Senator BRYAN. Mr. President, let me commend you for holding this important hearing. Undeniably, the Internet and e-commerce provide enormous opportunities for Americans. I think on balance it has been an extraordinary and remarkable development. But there is also a dark side to it and that is the loss of privacy.

I think most Americans, if they were thinking about this in the context of their local shopping center or their local mall, that somebody was following them around taking notes as to which store they went into, how long they were there, which items they looked at, and then at the end of that shopping session all of this was

compiled and this information was sold to a third-party marketer. People would be absolutely offended and outraged.

In a real sense, that is what is happening today in the world of cyberspace. Now, I know, Mr. Chairman, some of our colleagues take the position that this industry is so sacrosanct that it is sacrilegious to even suggest that there be some type of regulatory review. It seems to me, as my colleague Senator Wyden pointed out, there is opportunity for some self-regulation involved. But, in my sense, the time is now for us to appropriately take a look at what kind of basic protections we can provide for American consumers. I think the hearing that you have convened is extraordinarily important, and I am delighted to be here and hope to work in a bipartisan fashion with our colleagues to develop an appropriate response.

The CHAIRMAN. I thank you, Senator Bryan.

Before we turn to our witness, Senator Wyden, I believe that our first witness will comment that there are some negotiations going on now between her organization, the Department of Commerce, and some of the online advertisers as to some agreement that may be made on self-regulation. I hope our witness will illuminate us on that aspect of this issue.

Welcome, Ms. Bernstein. You are our first witness. For the record, Ms. Jodie Bernstein is the Director of the Bureau of Consumer Protection of the Federal Trade Commission. Welcome.

STATEMENT OF JODIE BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, (ACCOMPANIED BY DAVID MEDINE, ASSOCIATE DIRECTOR FOR FINANCIAL PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, AND DAWNE HOLZ, FEDERAL TRADE COMMISSION)

Ms. BERNSTEIN. Thank you, Mr. Chairman and members of the Committee. With me this morning is David Medine, who works closely with me on Internet privacy issues particularly, and Dawne Holz, who is our guru of information technology, who is at her desk over there.

We very much appreciate the opportunity to discuss the Commission's report on online profiling. The report describes the nature of profiling, consumer privacy concerns about these practices, and the Commission's efforts so far to address the concerns. As the Commission has in other areas, the Commission, along with the Department of Commerce, as you indicated, Mr. Chairman, we have encouraged effective industry self-regulation, and the network advertising industry has cooperatively responded with working drafts of principles for our consideration.

All parties agree that there are real challenges to creating an effective self-regulatory program, including how network advertisers disclose practices to consumers and how consumers should exercise choice. As a result, there has been a serious effort by this industry group to craft a program. After the Commission has had an opportunity to consider the final proposal, it will make a recommendation to Congress.

With the remarkable growth of e-commerce has come increased consumer awareness as well as increased consumer concern about

the online collection and use of personal data. One of the areas that has generated most public concern and about which, as several of you have mentioned, there is relatively little public knowledge or understanding is online profiling by network advertising companies.

In my testimony, I thought the most useful thing to do would be to try to illustrate how profiling works. So, if I may, I would like to show you an example of profiling. First, we will see what the consumer sees as he surfs the web. Then I would like to take you behind the scenes and explain what the consumer does not see.

Our online consumer, Joe Smith, logs onto the Internet and goes first to Webdragonsports. That is a site we made up that sells sporting goods. He is looking for a new golf bag and so he clicks on the link for golf and then he browses for golf bags. Then Joe says, I am going to go to TraveltheUS. He and his wife are considering taking a vacation, so he decides to go to search for information—about where? Let us go to Arizona, he says.

A week later Joe visits his favorite online news site, which is also SenateCommerceNews. He immediately notices an ad for a golf vacation package in Arizona. Well, he is delighted. He clicks on the ad.

Only later, Joe begins to wonder, how did that ad come to appear on my computer? Now let us look at what is going on behind the scenes and what Joe does not see. Joe's first stop was the wagon—I keep saying "wagon"—Webdragonsports site. Hidden in the computer code was an invisible link to USAads. Now, USAads is what we talked about before. It is a network advertising company—we also made it up—that delivers ads in the banner space on the Webdragonsite.

Joe's computer automatically sent a message to USAads asking for an ad. It also sent information about Joe's computer, as well as the fact that he was at Webdragonsports. USAads immediately placed a file, known to all of us as a cookie, with a unique ID number on Joe's hard drive, unknown to Joe.

Meanwhile, back at USAads a profile associated with that cookie was also created showing Joe's interest in sports. Now, it does not take a lot of studies to know—and they do know this—that an interest in sports is often related to an interest in sports cars. Therefore, USAads quickly sends Joe an add for Motorworks sports cars. When Joe clicked on the golf page, this information was transferred, transmitted to USAads and his profile was immediately updated to reflect an interest in golf.

When Joe went to TraveltheUS, a similar process occurred. An invisible link to USAads produced yet another ad. Because they knew the site was travel-related, USAads sent an ad for rental cars. When Joe entered a search for Arizona, his search term was transmitted again to USAads. As a result, travel and Arizona were added to the profile associated with the cookie on Joe's computer.

When Joe then went to his favorite online news site, that was also served by USAads. The cookie on his computer was read and he was presented with an ad targeted to his profile, a golf vacation package in Arizona.

Now, some consumers would be delighted to receive an ad targeted to their specific interest. Others, however, would be troubled

by having been tracked through prior website browsing without their knowledge.

Now let us suppose it occurred to Joe, and it did occur to him, that somebody had some information about him, that maybe he got the golfing vacation in Tucson ad because of a cookie placed on his computer. One way for Joe to see at least a small part of the process, the placement of the cookie on his machine, is for him to set the browser to notify him before accepting cookies. Now, you decide whether or not this is an easy thing for Joe or anyone to do.

There is a capability to do it. Let's look and see how easy it is. What would Joe do to change the cookie settings on his browser? Now, nothing up there says "cookies," but maybe he would say, try the edit menu, and that would be a good one to try. Then maybe he'd decide to try "Preferences." Now what? Would the smart choice be "Smart browsing," that category under "Navigator"? No.

Maybe Joe needs a lifeline here. Maybe he will try to even poll the Committee members who might help him out. Try clicking on "Advance," and then someone would say, "Is that your final answer?" Now you would see a checkbox that says "Warn me before accepting cookies." Well, that sounds right. That sounds intuitive almost.

So let us see what Joe, what he accomplished after he clicked on "Warn me before accepting cookies." What does the notification or warning from the browser look like? This is what it tells you. It tells you that someone named "USAads" wants to put a cookie on your computer with a particular ID number on it and the cookie will stay there until the year 2010.

With the way computers, personal computers, change, it'll probably outlast any number of computers that you have. But the cookie will be there twice as long. Notice, however, that this warning from your browser does not tell you who USAads is or what their cookie does. In other words, you have to choose to accept or reject this cookie without knowing very much at all.

You know, if it is that hard to deal with one cookie, we wanted to see what it would be like and how many cookies were likely to come up soon that you would have to deal with. Here is a sample cookie file that we constructed. We did it by deleting all the cookies from an FTC computer and we had a law clerk spend about 15 minutes only surfing some of the popular sites, the most popular sites on the web.

In just 15 minutes, 124 cookies were deposited on the computer, some of which are shown. The highlighted cookies were placed by third party advertising networks, in other words "profilers."

One other interesting thing to note is that the message—I really like this—that appears at the top of this file says "This is a generated file. Do not edit." That reminds me of the label that you all have seen, and I have too, on the mattress that says "Under penalty of law, do not remove this label." Well, the reason for this—the suggestion is that the user cannot selectively edit the cookie file to keep really helpful cookies and get rid of the unwanted cookies.

That is not true. The user can edit cookie files, but you might end up as confused as we were as we tried to work through the cookie files.

Let me conclude, and I do thank the Committee for allowing us this amount of time. As the Commission's report details, targeted advertising can provide benefits to both consumers and business. Nonetheless, current profiling practices raise a number of serious concerns. The most serious concern, which I hope this presentation illustrated, is that profiling is largely invisible to consumers.

Another concern is, because network advertisers can monitor consumers across numerous unrelated websites over time, the profiles they create can be extremely detailed and many would say extremely intrusive.

The Commission looks forward to working with the Committee to address the many privacy issues raised by online profiling and would be pleased to answer your questions. Thank you again, Mr. Chairman, for the opportunity to present the Commission's report.

[The prepared statement of Ms. Bernstein follows:]

PREPARED STATEMENT OF JODIE BERNSTEIN, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION (ACCOMPANIED BY DAVID MEDINE, ASSOCIATE DIRECTOR FOR FINANCIAL PRACTICES, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, AND DAWNE HOLZ, FEDERAL TRADE COMMISSION)

The Federal Trade Commission on "Online Profiling: Benefits and Concerns"

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

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

I. Introduction and Background

A. FTC Law Enforcement Authority

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

B. Privacy Concerns in the Online Marketplace

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

At the same time, technology has enhanced the capacity of online companies to collect, store, transfer, and analyze vast amounts of data from and about the consumers who visit their Web sites. This increase in the collection and use of data,

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

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

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

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

Based on survey data showing that the vast majority of sites directed at children also collected personal information, the Commission recommended that Congress enact legislation setting forth standards for the online collection of personal information from children.[17] The Commission deferred its recommendations with respect to the collection of personal information from online consumers generally. In subsequent Congressional testimony, the Commission referenced promising self-regulatory efforts suggesting that industry should be given more time to address online privacy issues. The Commission urged the online industry to expand these efforts by adopting effective, widespread self-regulation based upon the long-standing fair information practice principles of Notice, Choice, Access, and Security, and by putting enforcement mechanisms in place to assure adherence to these principles.[18] In a 1999 report to Congress, *Self-Regulation and Privacy Online,* a majority of the Commission again recommended that self-regulation be given more time.[19]

On May 22, 2000, the Commission issued its third report to Congress examining the state of online privacy and the efficacy of industry self-regulation. *Privacy Online: Fair Information Practices in the Electronic Marketplace* ("2000 Report") presented the results of the Commission's 2000 Online Privacy Survey, which reviewed the nature and substance of U.S. commercial Web sites' privacy disclosures, and assessed the effectiveness of self-regulation. In that Report, a majority of the Commission concluded that legislation is necessary to ensure further implementation of fair information practices online and recommended a framework for such legislation.[20]

II. Online Profiling

On November 8, 1999, the Commission and the United States Department of Commerce jointly sponsored a Public Workshop on Online Profiling.[21] As a result of the Workshop and public comment, the Commission learned a great deal about what online profiling is, how it can benefit both businesses and consumers, and the privacy concerns that it raises.

A. What is Online Profiling?

More than half of all online advertising is in the form of "banner ads" displayed on Web pages—small graphic advertisements that appear in boxes above or to the side of the primary site content.[22] Often, these ads are not selected and delivered by the Web site visited by a consumer, but by a network advertising company that manages and provides advertising for numerous unrelated Web sites.

In general, these network advertising companies do not merely supply banner ads; they also gather data about the consumers who view their ads. This is accomplished primarily by the use of "cookies"[23] which track the individual's actions on the Web.[24] The information gathered by network advertisers is often, but not always,

anonymous, that is, the profiles are frequently linked to the identification number of the advertising network's cookie on the consumer's computer rather than the name of a specific person. In some circumstances, however, the profiles derived from tracking consumers' activities on the Web are linked or merged with personally identifiable information.[25]

Once collected, consumer data is analyzed and can be combined with demographic and "psychographic"[26] data from third-party sources, data on the consumer's offline purchases, or information collected directly from consumers through surveys and registration forms. This enhanced data allows the advertising networks to make a variety of inferences about each consumer's interests and preferences. The result is a detailed profile that attempts to predict the individual consumer's tastes, needs, and purchasing habits and enables the advertising companies' computers to make split-second decisions about how to deliver ads directly targeted to the consumer's specific interests.

The profiles created by the advertising networks can be extremely detailed. A cookie placed by a network advertising company can track a consumer on any Web site served by that company, thereby allowing data collection across disparate and unrelated sites on the Web. Also, because the cookies used by ad networks are generally persistent, their tracking occurs over an extended period of time, resuming each time the individual logs on to the Internet. When this "clickstream" information is combined with third-party data, these profiles can include hundreds of distinct data fields.[27]

Although network advertisers and their profiling activities are nearly ubiquitous,[28] 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.[29] 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.[30]

B. Profiling Benefits and Privacy Concerns

Network advertisers' use of cookies[31] and other technologies to create targeted marketing programs can benefit both consumers and businesses. As noted by commenters at the Public Workshop, targeted advertising allows customers to receive offers and information about goods and services in which they are actually interested.[32] 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.[33] Additionally, a number of commenters stated that targeted advertising helps to subsidize free content on the Internet.[34]

Despite the benefits of targeted advertising, there is widespread concern about current profiling practices. The most consistent and significant concern expressed about profiling is that it is conducted without consumers' knowledge.[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.

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.[36]

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.[37] First, commenters feared that companies could unilaterally change their operating procedures and begin associating personally identifiable information with non-personally identifiable data previously collected.[38] Second, these commenters objected to the use of profiles—regardless of whether they contain personally identifiable information—to make decisions about the information individuals see and the offers they receive. Commenters expressed concern that companies could use profiles to determine the prices and terms upon which goods and services, including important services like life insurance, are offered to individuals.[39]

C. Online Profiling and Self Regulation: the NAI Effort

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

In announcing their intention to implement a self-regulatory scheme, the NAI companies acknowledged that they face unique challenges as a result of their indirect and invisible relationship with consumers as they surf the Internet. The companies also discussed the fundamental question of how fair information practices, including choice, should be applied to the collection and use of data that is unique to a consumer but is not necessarily personally identifiable, such as clickstream data generated by the user's browsing activities and tied only to a cookie identification number.[40]

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

III. Conclusion

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

Endnotes

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

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

3. 15 U.S.C. § 45(a).

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

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

The Commission does not, however, have criminal law enforcement authority. Further, under the FTCA, certain entities, such as banks, savings and loan associations, and common carriers, as well as the business of insurance, are wholly or par-

tially exempt from Commission jurisdiction. *See* Section 5(a)(2) and (6)a of the FTC Act, 15 U.S.C. § 45(a)(2) and 46(a). *See also* The McCarran-Ferguson Act, 15 U.S.C. § 1012(b).

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

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

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

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

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

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

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

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

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

issues raised by individual reference services, as well as issues relating to unsolicited commercial e-mail, online privacy generally, and children's online privacy.

The Commission and its staff have also issued reports describing various privacy concerns in the electronic marketplace. *See, e.g.*, *FTC Staff Report: The FTC's First Five Years Protecting Consumers Online* (Dec. 1999); *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 1997); *FTC Staff Report: Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996); *FTC Staff Report: Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace* (May 1996). Recently, at the request of the Department of Health and Human Services ("HHS"), the Commission submitted comments on HHS' proposed Standards for Privacy of Individually Identifiable Health Information (required by the Health Insurance Portability and Accountability Act of 1996). The Commission strongly supported HHS' proposed "individual authorization" or "opt-in" approach to health providers' ancillary use of personally identifiable health information for purposes other than those for which the information was collected. The Commission also offered HHS suggestions it may wish to consider to improve disclosure requirements in two proposed forms that would be required by the regulations. The Commission's comments are available at <http://www.ftc.gov/be/v000001.htm>.

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

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

15. 1998 Report at 11–14.

16. *Id.* at 23, 27.

17. *Id.* at 42–43. In October 1998, Congress enacted the Children's Online Privacy Protection Act of 1998 ("COPPA"), which authorized the Commission to issue regulations implementing the Act's privacy protections for children under the age of 13. 15 U.S.C. §§ 6501 *et seq*. In October 1999, as required by COPPA, the Commission issued its Children's Online Privacy Protection Rule, which became effective last month. 16 C.F.R. Part 312.

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

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

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

21. 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]."

22. In 1999, 56% of all online advertising revenue was attributable to banner advertising. Online advertising has grown exponentially in tandem with the World Wide Web: online advertising revenues in the U.S. grew from $301 million in 1996 to $4.62 billion in 1999. *See Press Release: Internet Advertising Revenues Soar to $4.6 billion in 1999* (available at <http://www.iab.net/news/content/revenues.html>). Advertising revenues are projected to reach $11.5 billion by 2003. *See* Jupiter Communications, Inc., *Online Advertising Through 2003* (July 1999) (summary available at <http://www.jupitercommunications.com>).

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

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

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

26. 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."

27. 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>.

28. 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>.

29. 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.

30. Not all profiles are constructed by network advertising companies. Some Web sites create profiles of their own customers based on their interactions. Other companies create profiles as part of a service—for example, offering discounts on products of interest to consumers or providing references to useful Web sites on the same topic as those already visited by the consumer. *See, e.g.*, Megan Barnett, *The Profilers: Invisible Friends*, The Industry Standard, Mar. 13, 2000, at 220; Ben Hammer, *Bargain Hunting*, The Industry Standard, Mar. 13, 2000, at 232. These profiles are generally created by companies that have a known, consensual relation-

ship with the consumer and are not addressed in this report. This report uses the term "profiling" to refer only to the activities of third-party network advertising companies.

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

32. *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.

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

34. *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.

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. *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.

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

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

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

40. Tr. 186, Jaye; Tr. 192–193, Zinman.

Statement of Commissioner Orson Swindle Concurring in Part and Dissenting in Part to Prepared Statement of the Federal Trade Commission on "Online Profiling: Benefits and Concerns"

I concur in the issuance of the Prepared Statement of the Federal Trade Commission on "Online Profiling: Benefits and Concerns" before the Committee on Commerce, Science, and Transportation, United States Senate (June 13, 2000) ("Commission Statement"), but I dissent from how certain consumer opinion surveys are used in the Commission Statement.

First, consumer opinion surveys like the ones used in the Commission Statement often are not reliable predictors of consumer behavior. For several reasons, and as the Commission Statement acknowledges in footnote 8, survey results should be ex-

amined with scrupulous care. Surveys are one-time snapshots of consumer opinion, are easily biased by design, and must be examined for methodological integrity.

Ideally, consumer opinion surveys should complement, but not be a substitute for, empirical evidence of consumer behavior relating to privacy. They should not serve as the substantive basis for policy.[1]

Second, when the Commission reports to or testifies before Congress, it owes the Congress a certain degree of thoroughness. A statistic included in a Commission report likely will be given credibility beyond what might attach to the use of that same number in a brief news story or an advertisement. Because of the added degree of credibility attached to a Commission report, the Commission should not uncritically repeat estimates, projections, or other statistics unless it knows how the numbers were derived, including the assumptions on which they may have been based. This requires going directly to the source of a number. If that standard of analysis cannot be met, then the Commission either should not use the number or should explicitly qualify its use of the number by the uncertainties attached to it.

For example, both the Online Profiling Report and this testimony contain an estimate of future advertising revenue drawn from an overview of a July 1999 report by a management consulting firm. (*see* "Online Profiling: A Report to Congress" at 2, n.7; Commission Statement at n.22). The Commission has no basis for assessing what assumptions went into that projection, nor does the Report or the testimony highlight that the July 1999 date of the projection alone likely means it is less accurate in light of the tremendous growth in online commerce since then. In my dissent from the Commission's 2000 Privacy Report, I criticized the Commission's use of a lost sales projection by the same management consulting firm based on the repetition of that projection in a news article and the information available from an online overview of the study. An examination of the full study revealed that the lost sales projection was based on assumptions that completely invalidated the Privacy Report's reliance on that lost sales projection. *See* 2000 Privacy Report, Dissenting Statement of Commissioner Orson Swindle at 13–14.

Another example of relying on numbers without assessing their validity is the testimony's reference to an Odyssey study in which 92% of respondents from online households stated that they do not trust online companies to keep their personal information confidential. (Commission Statement at 5–6 n.10). This figure comes from the same Odyssey Study cited by the majority in the Privacy Report and appears to be subject to the same flaws that I discussed in my dissent from the Privacy Report. Unfortunately, the Odyssey Study does not reveal the specific questions used to derive the 92% that either agree or strongly agree with the proposition repeated in the Commission Statement. If the Odyssey Study uses the same methodology as for other questions, it likely biases the responses to "agree" categories by not allowing a choice to "somewhat disagree." (*See* 2000 Privacy Report, Dissenting Statement of Commissioner Orson Swindle at 11.)

I respectfully ask that Congress keep these limitations in the data in mind as it considers the Commission's Online Profiling Report and the Commission Statement.

Online Profiling: A Report to Congress
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

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

[1] A portion of my dissent from the Commission's 2000 Privacy Report addressed the Commission's dubious reliance on consumer opinion surveys. *See* Dissenting Statement of Commissioner Orson Swindle, Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress" (May 22, 2000) at 12–16.

* 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.

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 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 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 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 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 splitsecond 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 gen-

erally persistent, their tracking occurs over an extended period of time, resuming each time the individual logs on to the Internet. When this "clickstream" information is combined with third-party data, these profiles can include hundreds of distinct data fields.[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.

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 preset 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.

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 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 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 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 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 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 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 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 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 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 marketplace and its information practices and to assess its cost and beneficial effects. It has also used its law en-

forcement 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] 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 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

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.

Endnotes

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 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>).

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 par-

ticular Web page or reads the particular e-mail 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 e-mail address with a cookie identification number, making an otherwise anonymous profile personally identifiable. *See generally* Comments of Richard M. Smith; *see also Big Browser is Watching You!,* Consumer Reports, May 2000, at 46; *USA Today, A new wrinkle in surfing the Net: Dot-coms' mighty dotsize 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.

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."

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.

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.

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.

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.

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."

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.

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 "redlining" [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.

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.

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.

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.

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. 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 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 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 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.

80. Tr. 186, Jaye; Tr. 192–193, Zinman.

Statement of Commissioner Orson Swindle Concurring in Part and Dissenting in Part in Online Profiling: A Report to Congress

File No. P994809

I concur in the issuance of "Online Profiling: A Report to Congress," but I dissent from the use of consumer opinion surveys in the Report.

Consumer opinion surveys like the ones used in the Report are often not reliable predictors of consumer behavior. For several reasons, and as this Report acknowledges in footnote 33, survey results should be examined with scrupulous care. Sur-

veys are one-time snapshots of consumer opinion, are easily biased by design, and must be examined for methodological integrity.

Ideally, consumer opinion surveys should complement, but not be a substitute for, empirical evidence of consumer behavior relating to privacy. Consumer opinion surveys should not serve as a substantive basis for policy decisions.

The CHAIRMAN. Thank you very much and thank you for a very interesting, illuminating presentation.

I would like to talk for a minute about these discussions you are having with the online advertisers. Is not a fundamental question here opt-in or opt-out?

Ms. BERNSTEIN. That would be a fundamental question and it could be—or there are those who would say that, depending on what the purpose is, it could be—one or the other, and it might depend on the type of information that is being collected.

The CHAIRMAN. Would that not get a little complicated pretty quick?

Ms. BERNSTEIN. It could get very complicated. We hope not, because obviously it needs to be simple in order to be useful to consumers.

The CHAIRMAN. Well, we conduct these hearings on the basis—on the premise—that there is no such thing as a dumb question, Okay?

It seems to me that the decision made by the consumer as to whether they want out of one of those files is one thing. It is an entirely different scenario if these people have to come to me and say, we would like for you to give your positive, affirmative permission to use your information or track your habits.

So is this not a fundamental question here?

Ms. BERNSTEIN. Yes, it is.

The CHAIRMAN. Mr. Medine, you want to comment?

Mr. MEDINE. Well, these discussions are trying to address this issue, but of course the discussions are under way, and obviously the Committee's views on what the proper balance is in this area would be extremely helpful in informing us as the discussions go forward as to whether consumers should be asked if they want to participate in this process or should simply be told of their ability to not participate in this process.

The CHAIRMAN. Well, do you have a view on that, Ms. Bernstein?

Ms. BERNSTEIN. The Commission has not taken a position on that yet, as you know, Mr. Chairman. And in view of the fact that we are still engaged in trying to do two things—one is to see if we can complete an effective self-regulatory program—I think we would be, as David said, we could be of the view that in order for a cookie to be placed in the first instance an affirmative consent by a consumer would be useful. Principally, one wants to put the consumer in the position of being in control of how his information is used.

The CHAIRMAN. Well, it just seems to me that the advertisers would argue strenuously for an opt-out option.

Ms. BERNSTEIN. They have and I am sure that they would continue to.

The CHAIRMAN. What we just saw is relatively innocuous. I believe that—I hope that every American would know of a golfing vacation package in Tucson.

[Laughter.]

Senator BRYAN. And want to go there.

The CHAIRMAN. Bypassing Nevada on the way.

[Laughter.]

Senator BRYAN. And stopping there on the way back.

Senator WYDEN. But still finding their way to the Oregon coast.

Ms. BERNSTEIN. We will try to accommodate every Senator on this Committee.

The CHAIRMAN. Let us hear from you or Mr. Medine about the less attractive aspects of this. Your presentation is excellent, but, frankly, if that was the only problem we have here, I do not think we would be having these hearings. Let us talk about the really invasive, intrusive aspects of this kind of procedure.

Ms. BERNSTEIN. I will be happy to do that. One of the things that is clear from the presentation that we decided to use as an illustration is that so far the information is not personal. It is only connected to the consumer's computer. That is, it does not say John McCain asked for this information, but rather it is connected to John McCain's computer.

That information, however, is capable of being combined with personal information about that person.

The CHAIRMAN. For example?

Ms. BERNSTEIN. By use of another database or combining it with prior information, or sometimes the website itself.

The CHAIRMAN. For example, what kind of personal information? How much money I have in a bank account, or my credit rating?

Ms. BERNSTEIN. Well, it could be your name, your address, perhaps your telephone number. From that information, sometimes more sensitive information can be obtained from another source. So there is the capability to put together a really very complete information profile about a consumer.

The CHAIRMAN. Do you want to add to that, Mr. Medine?

Mr. MEDINE. Yes. In addition to that, the consumer may visit a website that might reveal sensitive items, like certain health conditions or religious or political affiliations that might be linked to somebody's name. There is also the capability of making identifiable months or even years of web browsing that you had thought were anonymous that could then become identified to you. There have certainly been instances publicly where people have been associated with past browsing that has made them uncomfortable.

There is also the issue of merging online and offline data as well. That is, you think your shopping online is one thing, your shopping offline or your habits offline are different, but to have them merged raises special concerns as well.

So this is the most innocuous of non-personally identifiable information used to target a relatively simple ad. But clearly there is the capability of gathering personal and sensitive information through this process.

Ms. BERNSTEIN. That is really where the intrusiveness comes about and why so many people are expressing concerns about it. In addition, it is really secret. People do not know this is going on, and that I think is the most—most people react very negatively to the fact that there is——

The CHAIRMAN. How do you let them know that it is going on?

Ms. BERNSTEIN. Well, you could let them know by various notices that could be either on the website or that would be required to be on website where it begins in the first instance, and then you could have a subsequent notice in the site itself so that the consumer knew that that was going on. But it would be fundamental notice that does not now occur.

The CHAIRMAN. Could you have something that would flash that said "Information is being transmitted concerning your visit to this website; do you object?"

Ms. BERNSTEIN. You could have that, certainly.

The CHAIRMAN. Well, I guess that question is also something for the next panel.

Finally, I guess if you could carry it to its extreme, for someone who is a very heavy user of the Internet, you could compile information which would over time give someone a dossier compiled of your political, religious, financial information—literally everything about your life. Is that your view, Mr. Medine?

Mr. MEDINE. That is certainly a potential here when you are web browsing, which many people think of as being anonymous and they appreciate being anonymous so that they can freely move around, gather information, and it may no longer be anonymous if an identifiable cookie is placed on your computer.

The CHAIRMAN. Finally, what is your degree of optimism about reaching some kind of a deal with the online advertising industry?

Ms. BERNSTEIN. We have had good talks with them and I think they are very anxious to put an effective self-regulatory program in place. As the Commission said in its earlier testimony, Mr. Chairman, the Commission did not view a self-regulatory program in isolation, but rather expressed its view that the most effective program is a self-regulatory program that is supported or buttressed by a fundamental law that would support the program.

I would say it is about—oh, we could flip a coin, but better than half and half. How is that?

The CHAIRMAN. Well, let me just say that we obviously would like to see an agreement that is acceptable to one and all. You have heard views, strong views, expressed by both Senator Burns and Senator Wyden that legislation is necessary. So if you do reach an agreement, I think you are going to have a selling job at least with some members of the Committee as well as other members of Congress.

I thank you for being here today.

Senator Hollings.

Senator HOLLINGS. Well, Ms. Bernstein, we only said that legislation was necessary after five years of the Federal Trade Commission working on it. The FTC put out reports and reviews that suggested the voluntary approach was the proper approach. Having done that for over five years, Mr. Pitofsky, your Chairman, came here and testified that he thought that legislation was necessary. That is correct; is that not right?

Ms. BERNSTEIN. Yes, it is absolutely correct.

Senator HOLLINGS. I mean, do not have the Federal Trade Commission be a moving target. What we are trying to do is maintain the integrity of the Internet so that people can trust it. We are at the same starting line. We are going to have to have some kind of

regulation, I take it, for those who make a business of collecting personally identifiable privacy information.

Do you agree with me on that?

Ms. BERNSTEIN. Yes, I do agree with you.

Senator HOLLINGS. When we drew the bill, we looked at the recommendations in the five-year consideration of the Federal Trade Commission. We said that for anonymous information, like you are taking a census, we wouldn't talk about opting in there. We are only talking about opting out. If people are making a business out of this, then they can collect any kind of personal information on Senator McCain or me. Anybody in the audience can collect the information and know it and understand it.

Once they start making a commercial enterprise or business out of the thing, then we say, now hold up, you owe a duty to the public. If we do not do that, then people are going to be fearful of using the Internet. The trust that we have and the participation that we have won't continue. We want to continue Internet participation.

Now, only after five years did we really start with a bill. You toyed with it for five years and we see only the frustration, having toyed with it and not getting a voluntary response. You are not going to get advertisers. You have always got that group that won't be fair. I go to a class where the teacher grades on a curve and 95 percent of the students are honest and they study and they are ready to take the exam. The honest 95 percent finds out that 5 percent of the class has already stolen the exam. I say, wait a minute, I better get a copy of the exam, too.

That sort of breaks the discipline and the voluntariness and everything. We have tried that for five years, and you are not going to get it voluntarily. You are going to have certain advertisers who are going to use every scheme there is to get around and make money out of it.

Otherwise, we have got these states attorneys general all moving for different kinds of rules, regulations, and laws. We find that the longer we delay the greater the chaos and the greater the difficulty there is to legislate.

When the Federal Trade Commission appeared before the Committee, we asked each one of the Commissioners to critique our bill. Do you know where they are on it? I am welcome to criticism. I do not get any award for a bill. People back in South Carolina could care less whether I put it in. They do not even know I am up here hardly. The state has gone Republican; I am having a hard time. The best thing I can do is tell them I am a friend of John McCain and we get along.

[Laughter.]

So I do not have to have a bill. But I can see and ten others have seen. We have tried to look at all the features, rather than hit and run driving politically. I have got a bill in on privacy, so tell them to study it further and hope they voluntarily respond.

We are five years into the real study of it, and we have got the states all moving to laws. So it begs the question now that the federal government here in Washington move and get some orderly measure.

So we do not discourage your moving with advertisers, but if we wait on that we will never get a law. We will never get what you

finally say. Even if you got the voluntary agreement, you would still have to have a law for some kind of enforcement. Is that not correct?

Ms. BERNSTEIN. I believe that is correct.

Senator HOLLINGS. So we are going to pass some kind of law on privacy for those who are trying to make a business out of my identifiable personal information on the Internet.

You have answered the question, you said 50–50. Well, that is a good answer, but——

Ms. BERNSTEIN. I think I said better than 50–50, so I am a little more optimistic than that.

Senator HOLLINGS. Yes, but I mean, we cannot wait. You have got to get 100 percent.

Ms. BERNSTEIN. Yes.

Senator HOLLINGS. When do you think you are going to get 100 percent agreement?

Ms. BERNSTEIN. Well, we will either reach agreement or we will—the Commission has to review this, obviously, and we are still working at the staff level to see whether or not we have a program that we think we could recommend enthusiastically to the Commission. That should happen in a week or two.

Senator HOLLINGS. Now, you identified someone in the original instance as a "guru."

Ms. BERNSTEIN. Yes.

Senator HOLLINGS. What is his name?

Ms. BERNSTEIN. Her name——

Senator HOLLINGS. Her name, excuse me.

Ms. BERNSTEIN [continuing]. Is Dawne, Dawne Holz, and she is our technology guru who assisted us with putting this program together, more than assisted us, even came up with some of the names of sites and so forth so that we could do our presentation. She works with this.

Senator HOLLINGS. What we want to do here at the Congressional level is pass something that is realistic. Let me ask the guru, will you please take our bill and study it and criticize what is unrealistic, what is too burdensome, what is unenforceable? Any kind of criticism that you can give from your experience, we would appreciate here at the Committee level.

Take that bill for me and criticize it so that we can correct it or not pass it or whatever it is, knock it out. I would appreciate it.

Ms. BERNSTEIN. Senator, each of the Commissioners I know is at work preparing their own views, as you have asked.

Senator HOLLINGS. But I want the guru.

Ms. BERNSTEIN. Yes. Well, the guru will——

[Laughter.]

Senator HOLLINGS. I want the guru. You know, sometimes the Commissioners, they are political just like me. It is like sort of delivering lettuce by way of a rabbit. The guru's ideas do not come through. I want her ideas.

Ms. BERNSTEIN. You have it, sir. You will have it.

Senator HOLLINGS. Thank you very much. Thank you, Ms. Bernstein.

The CHAIRMAN. Thank you, sir. Thank you for your kind words.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Ms. Bernstein, if an agreement is reached on online profiling, how could the profiling industry guarantee that all of the profiling companies are going to participate?

Ms. BERNSTEIN. They can guarantee it of all the companies are signatories to the agreement. That leaves open, of course, the issue of new entrants into the industry and whether they could be bound. That is always a difficulty when one is dealing with a self-regulatory program and it is probably one of the underlying reasons why in the past self-regulatory programs that have had an underlying legal structure have been the most effective ones, because then everyone is bound even if there is a new entrant.

Senator WYDEN. What is troubling to me, and I think it is what Senator Hollings is touching on, as well, is that you are not likely to bring into the system of oversight the people who most need to be monitored. I think my next question would be who would enforce an action against a company that was violating the agreement? Are profilers going to do this? Are they going to run their own enforcement program? Are advertising agencies, websites where banner ads are running going to enforce this? Who is going to enforce this?

Ms. BERNSTEIN. If they did not do what they have promised to do in an agreement, a final agreement, the FTC could. The FTC's underlying authority is to prevent deception and therefore we could bring an enforcement action if they failed to live up to their promises. So that is one method of enforcement.

In addition, other groups have made arrangements for third parties to audit their compliance with agreements, and if those auditors turn up violations that could also be referred to the FTC, as others have done.

Senator WYDEN. So signatories can be brought before the Federal Trade Commission. But, again, the people, frankly, that I'm most concerned about are not the people who sit down and work with you on these kinds of pieces of legislation. They're the ones that operate in the shadows and certainly are engaged in some practices that are far more serious than the one we saw today involving golf.

Now, you identified four core principles for personal data, that is what the FTC did, and that is why I tried to separate out personal data from profiling, which is the area we are looking at today. Now, with respect to personal data, the FTC said it is important to deal with notice, choice, access, and security.

What arguments would there be for not applying these principles to data collected by online profilers?

Ms. BERNSTEIN. There is none. In fact, the Commission's report that was released today on online profile articulates those same four fundamental elements of fair information practices—notice, choice, access, and security—and enforcement.

Senator WYDEN. Now, you have been in the consumer protection field an awfully long time. I happen to think you give public service a good name because of the work that you have done in consumer protection. I think I would like you to outline whether there are any consumer laws now on the books that significantly limit what online profilers could do with respect to, say, medical and sensitive information?

Ms. BERNSTEIN. In regard to medical and sensitive——

Senator WYDEN. Let us just say, are there any laws on the books today that limit in a significant way what online profilers can do with important significant information?

Ms. BERNSTEIN. There are some, but they are not comprehensive and do not do what you are suggesting. But as you know, the recent Financial Modernization Act (Gramm-Leach-Bliley) did provide some protections for consumers for the collection of financial information and, while we are not expert in it, there has been some legislation in connection with medical information that is being, I believe, worked in the regulatory process from the Health and Human Services. Those are the only ones that we know of.

Senator WYDEN. But it does not exist today, and I think that is the important point. I think both the questions asked by Chairman McCain and by Senator Hollings are extremely important. We all want to see the self-regulatory initiative succeed and, from the very beginning, I have said they ought to have a wide berth. But people who are not signatories to these voluntary agreements, based on what you have just told us, as of today those that are not and are not willing to try to subscribe to strong consumer protection standards can do any darn thing they want with respect to sensitive medical information and online profiling.

I do not think that is right. I do want to give the private sector a wide berth, but I think we do need to have enough oversight and enough leverage on the part of government to be able to proceed against those who would exploit and rip off the citizens of this country with respect to sensitive medical information and other areas. I think that is why we ought to be trying on a bipartisan basis to put together a bill.

Mr. Chairman, I thank you.

The CHAIRMAN. Thank you.

Senator Bryan.

Senator BRYAN. Thank you very much, Mr. Chairman.

Ms. Bernstein, let me continue where Senator Wyden left off. Among those core values, notice it would seem to me is the most fundamental and basic right that a consumer would have, that is to be informed as to what is occurring with respect to his activity or her activity. Is there objection to establishing a legislative floor, to say at least there is a requirement that you must provide notice if you are collecting this kind of information? Is that something that is resisted by the industry?

Ms. BERNSTEIN. I do not believe so, and in fact the Commission's legislative proposal that was discussed before this Committee two weeks ago would require a website on which there would be a third party operating to disclose that to a consumer. So that was already contemplated in terms of the notice requirement that the Commission was recommending.

Senator BRYAN. I guess what I am saying, Ms. Bernstein, does the industry agree with that? I know that was the proposal that was advanced, but do they agree with that?

Ms. BERNSTEIN. Yes, they do.

Senator BRYAN. So we have an agreement that legislation that provides one of those core values, that is notice, would be appropriate?

Ms. BERNSTEIN. Yes.

Senator BRYAN. Okay, so at least we have crossed the Rubicon on that issue. What are the sanctions that attach to those companies that agree to a self-regulatory agreement if one of the parties violate the terms of the agreement, in general? Just do not do that again, or if you do that again we are going to really get pretty upset with you, kind of the Bobby Knight approach to regulation?

Ms. BERNSTEIN. No, we do not agree with the Bobby Knight approach. As I said before, the FTC has authority under its deception authority to proceed to bring an action that would force them to comply with the agreement and under some circumstances we could seek penalties, as you know.

Senator BRYAN. Would that be monetary fines of some kind, Ms. Bernstein or Mr. Medine?

Mr. MEDINE. Well, there would be injunctions and possible consumer redress if we could establish actual injury, and certainly going forward actual fines or enforcement proceedings if they fail to comply with an FTC order.

Senator BRYAN. Just in general—you may have many options—what would the maximum fine be? Suppose you have a signatory to the agreement who has a habit or practice of consistently violating the provision? This is not just, we goofed, we are sorry, we are not going to do that again. What would be the hammer that the FTC could bring down upon that violator?

Ms. BERNSTEIN. Well, under existing law the penalties are $11,000 a day per violation. So that could add up to a very significant amount of money.

Senator BRYAN. Indeed it could.

Now, with respect to those who are not participants to the agreement, there are no penalties that would attach; am I correct?

Ms. BERNSTEIN. Under present circumstances, no. If they are not signatories, they would not be subject unless they took some other actions.

Senator BRYAN. Are there other actions covered in the law?

Ms. BERNSTEIN. Right.

Senator BRYAN. Do you have any idea as to what percentage of the universe out there would be willing to sign onto such a self-regulatory agreement?

Ms. BERNSTEIN. We have—there are about a dozen companies and we believe that that represents about 90 percent of the industry.

Senator BRYAN. So we would still have 10 percent that would be operating beyond the ambit of whatever agreement would be entered into?

Ms. BERNSTEIN. That is what we know at the present time, and it is an estimate, Senator.

Senator BRYAN. I appreciate that.

Ms. BERNSTEIN. But it may be that it is greater than that.

Senator BRYAN. Ms. Bernstein, you made the point that currently, in the example that was cited, this was not personally identifiable information.

Ms. BERNSTEIN. Right.

Senator BRYAN. You also made the point that it might be possible, in response to the Chairman's inquiry, to in effect combine

a personally identifiable database with this and then really put a great deal of information in it. Is there currently any law that prohibits that?

Ms. BERNSTEIN. No, there is not.

Senator BRYAN. Let me be clear on that. So you are saying that tomorrow, at the end of this hearing, if a determination was made by any commercial website or one of these cookie companies or however we would characterize them, it would be possible for them to combine the personally identifiable database with the non-personally identifiable information that you provided there and that could be done without any violation of the law at all?

Ms. BERNSTEIN. That is correct, Senator.

Senator BRYAN. Now, is there objection by the industry to legislation that would say, you shall be prohibited from combining those two types of database?

Ms. BERNSTEIN. We have not discussed legislation with them, Senator. That really has not been a part of our discussions to date with them. Rather, we have been trying to work through a self-regulatory program——

Senator BRYAN. And I understand that. But would you not agree that we have agreement essentially that there ought to be a requirement in law of notice? Would it not be appropriate to have legislation that says, look, you cannot combine those two databases?

Ms. BERNSTEIN. I will not be representing the views of the Commission, so this makes it a little uncomfortable for me. And I am not sure you want my personal views, but my personal views are——

Senator BRYAN. What would your personal view be? You have done a great deal. We understand that for the record you have made the disclaimer that you are not speaking on behalf of the Commission.

Ms. BERNSTEIN. Right.

Senator BRYAN. And I am not trying to entrap you, Ms. Bernstein.

Ms. BERNSTEIN. I know you are not, sir.

Senator BRYAN. But you are a witness with considerable experience and a great deal of credibility, as my colleague from Oregon pointed out.

Ms. BERNSTEIN. It would seem to me that, unless there is at a minimum an opt-in by consumers, that is if a company is ever going to combine personal and non-personal information that the consumer would have the opportunity to have a very full disclosure of what was going to happen to them and a very firm opportunity to say yes or no to that. And that would be at a minimum.

Senator BRYAN. Now, is there any technical reason that one could not require an opt-in provision in terms of this whole profiling issue that we are talking about? Is there any technical reason, anything systematically that would prevent that?

Ms. BERNSTEIN. Not that I know of.

Senator BRYAN. And my friend from South Carolina's guru would agree with that statement, would she?

Ms. BERNSTEIN. Guru, you agree with that?

Ms. HOLZ.

[Nods affirmatively.]

Ms. BERNSTEIN. She agrees.

Senator BRYAN. Guru indicates that——

Ms. BERNSTEIN. Let the record show.

Senator BRYAN. Let the record reflect that the guru agrees with the witness.

Mr. MEDINE. Hearing no objection.

Senator BRYAN. We thank the guru.

Finally, if I may, because I know there are many others that want to comment on this, in terms of providing the greatest measure of protection to the consumer would not the opt-in, that is to say, look, before we are going to do this profiling we need your prior permission. Does that not provide the ultimate or best protection to the consumer?

Ms. BERNSTEIN. I believe most people would agree that that provides the greatest amount of protection or, put another way, it allows the consumer the greatest control over their own information; and that really is where the control should rest.

Senator BRYAN. By and large, we are talking about the consumer's personal information, activities, shopping habits, or otherwise, of the individual. I know every one of my colleagues fully understands that, but the opt-in requires the prior consent. That is, none of this activity could occur unless the consumer affirmatively agreed.

Ms. BERNSTEIN. That is correct.

Senator BRYAN. The opt-out permits the company to do so, notify the consumer, and then the consumer can say, stop, I do not want you to do that again; is that the essence of it?

Ms. BERNSTEIN. Well, an opt-out could be that they could not do it unless they gave the consumer notice of the opportunity to not have it done. So it is just a slight difference in the way I think you phrased it, Senator.

Senator BRYAN. So would that mean, in effect, that silence is acquiescence under what you have just said? In other words, the consumer is notified, but you do not require his or her affirmative consent, but if they take no action at all silence is acquiescence?

Ms. BERNSTEIN. Having given them the opportunity to opt out, yes.

Senator BRYAN. I appreciate that. Thank you very much to our witnesses and thank you very much, Mr. Chairman.

The CHAIRMAN. Senator Burns.

Senator BURNS. Thank you, Mr. Chairman.

I do not know what ground my colleagues have covered here, but even though Senator Wyden and I have worked on a bill that principally is an opt-out type of an approach, which I think is the correct approach until somebody convinces me otherwise, I am still concerned about enforcement. How do we know who the bad actor is, or who takes unlawful information and either markets it or it pops up somewhere else, and then there is no paper trail or there is not anything to go back and see who really was the first to misuse it? Because once the information is out there in cyberspace, it just roams around out there and it becomes the property of the guy that has got the biggest net to catch it.

What kind of—what do you recommend as an enforcement mechanism? How do we do that?

Ms. BERNSTEIN. Well, one of the things that has worked effectively in other areas we believe, Senator, is a third party audit or a third party firm that will on a systematic basis review what practices each of the sites are engaging in, sample it, and find out whether or not the protections are being provided.

You can also have consumers who are surfing the net. They can also report, as they often do, to an enforcement mechanism or, in the case of a law, to the FTC. We have a very, very good way, I think, of collecting consumer complaints, and then a law enforcement action can be brought. But that requires, of course, what we have talked about previously, and that is either a system where they have not done what they promised to do in self-regulation or a legal structure that would permit that kind of enforcement.

Senator BURNS. Does that also pertain to the people who collect information on consumers through any other mode other than electronically? In other words, any place else than the Internet? Every time I buy something that says: congratulations, you bought this great new thing here, in order to get your warranty you have to send in this card, but you are going to answer some questions; what about those?

Ms. BERNSTEIN. In the sense of if they tell you something that is not true, represent something that is not true? That is against the law.

Senator BURNS. Even in the collection of this information and what they are going to do with it?

Ms. BERNSTEIN. If they tell you that they are not going to do with it what they are going to do with it, then it could be considered deceptive under the FTC Act.

Senator BURNS. What if there is no statement at all?

Ms. BERNSTEIN. Then it makes it very difficult for the FTC to proceed, because no statement has been made and there is not a specific requirement that it be made under existing law. That is why the Commission recommended legislation on general privacy two weeks ago.

Senator BURNS. You see, I am very supportive of some privacy legislation. I am very supportive of that. I just think that the consumer has that right. It is one of the American core values that we must protect, a person's own privacy. It gets even more sensitive whenever we start talking about financial arrangements and those kind of things, and also with medical records and some other privacy things that I do not think the public needs to know anything about.

But I am still concerned about whether we are placing certain restrictions on those folks who are in the electronic business or the Internet business and not placing the same restrictions on the people who collect personal information even at grocery stores—and they make no statement on how that information is going to be used?

Ms. BERNSTEIN. Well, there are two things. First of all, there are some significant differences in the so-called e-commerce marketplace, as you have already alluded to. It is faster, it is quicker, they

have access to more information, and they can more quickly obtain that information, in a way that has not happened before.

But most recently there has been increased public attention on just what you raise, and that is, is there a need to make sure that there is a level playing field across these various media so that the same protections consumers expect in the offline world would be provided in the online world and vice versa?

Senator BURNS. You see, I think I read a story, was it yesterday—and I have got such a fantastic memory, but it is short about the implementation of Senator Bryan's legislation with regard to child privacy on the act that we passed through here and which we were very supportive of. But yet they are still having problems on implementation and enforcement.

That is the reason I ask those questions, because I think we can pass this thing and say we have done a good thing and then not revisit the situation later on. I think that would not serve the industry or the consumer very well.

I thank the chairman.

The CHAIRMAN. Senator Cleland.

STATEMENT OF HON. MAX CLELAND, U.S. SENATOR FROM GEORGIA

Senator CLELAND. Thank you very much, Mr. Chairman.

Ms. Bernstein, Mr. Medine is it? I am still struggling with the terminology. The terminology, I find, is fascinating about the Internet: mouse, web bugs, cookies, and spam—all found in every kitchen in America. What is your understanding of what a web bug is, Ms. Bernstein?

Ms. BERNSTEIN. My understanding of what a web bug is, it is a very tiny image that can be placed on a computer and indeed can be placed on a cookie itself and it cannot be detected visibly at all. It also collects information, not exactly the same way that a cookie does, which is a file, a little file of personal information.

Do you want to add anything to that, guru?

Ms. HOLZ. No.

Ms. BERNSTEIN. That is my understanding of what a web bug is. They are both used in different ways.

Senator CLELAND. Are you saying that a web bug can be put on someone's personal computer when they use the Internet and a cookie can be imposed on an Internet user without their knowledge?

Ms. BERNSTEIN. Yes.

Mr. MEDINE. Web bugs are typically found on web pages and they are really hidden code on web pages that essentially sends a message back to a third party, typically a network advertiser, saying, does this consumer have a cookie—and reading the cookie if the consumer has one on their file—and if not, placing a cookie.

But what's unique about web bugs is you do not see them and they may even appear on a page—unlike the pages that we showed earlier, there may not even be an advertisement on that page. You may not have any reason to suspect that a third party is in any way monitoring your web browsing.

Senator CLELAND. So as you browse you may leave cookies?

Mr. MEDINE. The web bug can place cookies or read cookies, yes, even when you are unaware that that is going on.

Senator CLELAND. That is amazing. Spam, what is spam?

Ms. BERNSTEIN. Other than the pink meat that you get, spam is unsolicited——

Mr. MEDINE. E-mail.

Ms. BERNSTEIN [continuing]. E-mail, unsolicited. It comes in over your e-mail.

Senator BURNS. It is like junk mail.

Ms. BERNSTEIN. Right, it is junk mail in every sense.

Senator BURNS. In your mail box.

Senator CLELAND. And the ultimate unwanted access is the Love Bug, right?

Mr. MEDINE. Which is a virus.

Senator CLELAND. A virus.

Ms. BERNSTEIN. Right.

Senator CLELAND. Mouse, web bugs, cookies, spam, and virus—amazing terminology to apply to this new technology.

Let me just say, Mr. Chairman, I think bringing the privacy rights of Internet users to the forefront of the Senate's attention is, quite frankly, critical. I think most people when they use the Internet think of it in many ways starting out, much like I would, using a telephone. A telephone is a direct line. You do not assume that it is a party line. You do not assume that there is somebody out there monitoring your call. You assume that what you say is in private between you and the hearer.

I think most Americans would be shocked if they picked up a telephone, dialed a number, and found out later that their phone call was being monitored, their preferences were being tracked with a cookie, and that ultimately if they hung up all of a sudden they could get multiple phone calls back unsolicited. I think that would be relatively shocking to the average individual out there. But that is exactly, apparently, what is happening to Internet users. Is that correct?

Ms. BERNSTEIN. That is correct, and we agree that Americans are shocked by it to the extent that there is survey data that suggests that, when they know about it.

Senator CLELAND. Because it seems to me that, much like the privacy of a phone, if one goes to the Internet one goes to it with a sense of privacy. It is you and the computer, and you and the information, and usually not a whole bunch of people standing around. It is pretty much a private moment, shall we say. It is kind of deceptively private and personal. It is kind of deceiving.

Now we find out that there is some deception out there. I am not sure, quite frankly, what role we have to play, but we are trying to find that out here.

Thomas L. Friedman, who wrote the book "Lexis in the Olive Tree: Understanding Globalization," says that maybe government is more needed rather than less. He said that government should be downsized, but it should be raised in quality, and said what we have to worry about is not so much government tapping your phone line or big brother, but little brother, somebody else out there.

He says in the web world everybody is connected, but nobody is in charge. And one wonders what the role of the FCC is and what

the roles of the Senate Commerce Committee and the Senate are in installing some sense of being in charge, some sense of rules, some sense of instituting or guaranteeing privacy.

I think privacy is the currency of the Internet. If that is destroyed, I think people will not go to the Internet or be as open, or as frank, or as consuming of the Internet and its products as we would be comfortable in doing.

Is that your sense?

Ms. BERNSTEIN. Yes, it is, Senator. In fact, you have hit on something that many have written about also, that one of the great benefits of the Internet and Internet commerce was the anonymity, that you could do what you wanted to do at your own pace and make your own choices. That can be destroyed by practices that impact on the anonymity that you might have come to and hopefully could expect.

Senator CLELAND. Yes, I think there is a certain expectation that when you use the Internet, that one is not so much anonymous, but it is private. It is private, and it is personal. The exchanges that take place there in effect belong to you and you should have the ability of choice.

Now, that is where we come to opt-in and opt-out. I am not sure I follow the bouncing ball here, but it seems to me the underlying principle is that I do not want web bugs, I do not want cookies, I do not want spam, I do not want anything messing up my communications here unless I choose for that to happen. If I choose, then so be it. I am still empowered with that choice.

I think we are looking at something here that we have to come to some decision on. The Internet and the web can certainly be very empowering. It can facilitate commerce, and it can facilitate the flow of information worldwide. The Internet can help heal diseases and communicate to people, all kinds of wondrous things. But if the medium itself is compromised, shall we say, by these terms, I think we shoot ourselves in the foot. We make the medium less than it can be.

Is that your sense, Ms. Bernstein?

Ms. BERNSTEIN. It is indeed, and we know that consumer confidence has already been somewhat impacted because of fears of just what you suggest, Senator, that they are fearful that their privacy will not be protected.

Senator CLELAND. Fear is a terrible thing. Fear can drive the stock market up or drive it down. Millions of people can react in fear just by one or two, shall we say, horror stories. We are not in the horror story business here, but the point being we are trying to find that role here. We do not want to kill the Internet, and we do not want to kill the goose that lays the golden egg. I understand that information technology is now the number one force driving the American economy, that Internet business, e-commerce, is growing at 6 to 8 percent a year.

This growth is, quite frankly, incredible. But I think one of the things that can kill the goose that lays the golden egg is an attrition of consumer confidence. You have that in the old economy, too. If you lose confidence in a manufacturer or product, all of a sudden overnight sales drop, and things happen that are not good.

So we appreciate you working with us and your guidance and advice in helping us work through these issues. We do not want to be too active here where we interfere with people's commerce and their communication, but, by the same token, I think it does rest and reside on a certain level of confidence and therefore privacy that is assumed and that ultimately I think should be guaranteed if the Internet is going to go ahead and grow.

Thank you, Mr. Chairman.

[The prepared statement of Senator Cleland follows:]

PREPARED STATEMENT OF HON. MAX CLELAND,
U.S. SENATOR FROM GEORGIA

Thank you, Mr. Chairman, for holding this Committee hearing on one of the most important issues facing Americans today, at least for those Americans who are not on the short end of the digital divide. We owe Internet users our undivided attention in developing ways of ensuring their privacy while not unduly overburdening the Dot Com companies or place them at a competitive disadvantage with off-line businesses. I believe that there is a solution that be crafted which respects the advertiser's ability to collect consumer information on the Internet and Americans' right to privacy.

By bringing the privacy rights of Internet users to the forefront of the Senate's attention, we are setting a course in a positive direction to alleviate the fears that many have concerning how their private information is acquired, stored, shared and used by others. In this fast-paced electronic age, information is being collected and stored at the rate of billions of bits per second. The information that users send over the Internet passes through dozens of different computer systems on the way to its final destination. Each of these systems may be managed by a different system operator, each with its own capability of capturing and storing online communications. It is little wonder that Internet users have concerns about their online activities.

Network advertisers are developing relationships with consumers that they don't know and, in many cases, these relationships are unwanted by the consumer. Placing cookies and "web bugs" on one's PC and tracking their movements in such an apparently underhanded manner seems very wrong on its face. What kind of a technology is "web bugs" anyway? In my mind bugs are pests that you use a bug zapper to get rid of. The alarming trend of using cookies and placing "web pests" on peoples' PCs that is being practiced by more and more firms, some of whom are represented here today, can't be a good thing if consumers are unaware these actions are being taken.

While some might consider targeted ads directed at a person to be helpful, many others consider them to be bothersome. For example, spam, or unwanted e-mail solicitations, is one form of advertising unwanted by just about everyone. What concerns me the most is the vast databases that are being generated to aim ads based on "inferential" or "psychographic" data. The ever increasing use of cookies, web bugs, and inferential data is only the beginning. With data collection technology, such as it is, peoples' innovativeness with how to apply this technology and the speed at which data can be processed, there is no telling how or what data will be collected in the future. One thing we can be certain of is that the information gathering industry will not be the same tomorrow as it is today. It is disconcerting to think how many current Internet users are unaware that their communications are being monitored and their activities tracked.

Today, there are an estimated 17.8 million websites registered worldwide and every day more are coming online. Each of these websites has the potential of collecting data that many consider private and many of them are actually collecting such information. I recognize that there are firms out there who are helping to ensure that industry's self-governing online privacy becomes a reality. One is the Better Business Bureau. Since it began certifying sites, the Bureau has certified just over 6,000 of the 17.8 million websites in existence today. While some in industry may believe this is a good start at self-regulating privacy concerns, I believe industry is falling short in its attempt to show it is capable of self regulation in this field.

I am looking forward to the dialog that will take place this morning and to hearing the distinguished witnesses address how the legislation that has been offered, or should be offered, can appropriately balance the consumer's right to privacy and the advertiser's ability to collect and utilize personal information. I am very interested in ensuring that a comprehensive, enforceable online privacy policy is afforded

to all Americans. It is our collective responsibility to do this so the Internet can continue to grow at an exponential rate, businesses are not burdened by overly burdensome restrictions and consumers can be assured that their privacy rights will be protected.

The CHAIRMAN. Senator Kerry.

STATEMENT OF HON. JOHN F. KERRY, U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Thank you, Mr. Chairman.

I regret coming in late because I know it has been an interesting discussion, and there is nothing worse than trying to pick up on it without having been part of the flow. So I was just trying to get as quick an update as I could. I do not want to, hopefully, be repetitive.

I have been spending more and more time in the last weeks trying to reach out to the folks in the industry who are on the cutting edge of changing things so rapidly and trying to get a better sense of what the play is and what the possibilities are within this privacy issue. I have come away from those discussions perhaps more confirmed, Mr. Chairman, in my sense, that we need to be careful about how fast we move.

I know there is bubbling up a sort of congressional sense of outrage that wants to protect appropriately our citizens' right of privacy, and I want to do that, too. But I become more convinced that the more you dig into it, the more complicated it becomes as to exactly what you can mandate effectively from this vantage point at this time.

Let me be precise. On the access issue, for instance, it is very difficult to provide the full measure of access that some people are asking for and still maintain the integrity of the recordkeeping on the other side that you want. How does somebody get access to their record to change whatever it is they want, and what is the guard against the input that they might want to change it with, the information that they have?

You can run down the line here on various aspects of the issue and you keep running into walls. Enforcement, I gather, has been raised by a number of my colleagues as an issue. It is almost a certainty that whatever we pass will be unenforceable unless we are passing something that sets some very clear standards and expectations that are meetable. Whether or not they will be meetable will depend to a large degree on where the technology goes and what the cooperative effort is going to be within the industry itself.

I think there is a medium ground, and I have tried to express that in the prior hearing that we had. But I think that, on greater analysis, my colleagues are going to share with me a sense that there may be a first step. Now, we are here focused on the online profiling, I believe, which in a sense it sort of underscores the predicament that we face.

The last hearing that we had was also focused on sort of online and we are focused on the Internet. But privacy is privacy is privacy. I mean, if privacy is a right and privacy is something that attaches to every American, it attaches to them online and offline. And, to the best of my knowledge, no one in the U.S. Congress has

put forward a full measure of what has happened to Americans offline.

Am I correct? Is there not a very significant intrusiveness that takes place in the marketplace offline?

Ms. BERNSTEIN. There certainly is some. There are, however—as you know, Senator, there have been some responses to that. Organizations like the Direct Marketing Association have put in place systems so that consumers can indicate that they do not want to receive certain kinds of telephone calls from sales persons or mail calls.

The Telemarketing Sales Act put some restrictions on what messages can be limited by consumers on the telephone. So I think it is not quite as bereft of any kind of protections for consumers as you suggest. Could there be more? I am confident that there could be.

Senator KERRY. That is a voluntary system.

Ms. BERNSTEIN. The DMA is, but the——

Senator KERRY. So it is not mandated by Congress.

Ms. BERNSTEIN [continuing]. Telemarketing Sales Act was mandated by Congress.

Senator KERRY. But you can get very significant, through private sources and otherwise, extraordinary amounts of information regarding any fellow citizen. I mean, you can get their criminal record. You can get what their credit card expenditures have been for some particular months through various sources. It is not a crime to do that.

You can do some remarkable profiling through purchases that take place. For instance, if I walk into a store here in Washington, swish my card through the credit machine, every purchase that I have made is known to those people. They can do whatever targeting they want.

So what we are doing here is we are really talking about conceivably in the outcome, depending on what we do, picking some winners and losers and affecting the marketplace as against another component of the marketplace. I mean, if privacy is the concern, privacy applies to everybody in every context, does it not?

Ms. BERNSTEIN. Yes, it does.

Senator KERRY. So why are we focused on one sector of the marketplace versus others?

Ms. BERNSTEIN. I think the focus has been on the online marketplace particularly because it is new, it does have many benefits for consumers that they would like to be able to use, and at the same time there have been increasing concerns about what happens to their information when they are using it. It is new. Everyone wants it to flourish because of the benefits it can bring, but it also has to have a balance of having people feel confident or they will not use it.

Senator KERRY. I agree with the Chairman that there is a special status with respect to medical information, and there is a special status with respect to financial information.

Ms. BERNSTEIN. Whether online or offline.

Senator KERRY. Correct, online or offline, and they ought to probably be treated similarly. But what is the harm with respect to this

protection we are seeking to provide with respect to the other aspects of the targeting and profiling? What is the harm?

Ms. BERNSTEIN. Well, one of the harms is that, at least in what we have been discussing today, is that consumers have no idea that this is going on.

Senator KERRY. Which, the profiling?

Ms. BERNSTEIN. The profiling. They have no idea.

Senator KERRY. So my concept of privacy, of what we should do at this point, is to mandate the level of notice and to encourage the maximizing of anonymity. I have spent some time lately trying to sort of test different sites and see where privacy appears. I look for how fast it leaps out at me, and how quickly can I see the word. I also look for what they are going to do. And there is a difference, there is a variance, I will concede that.

Clearly, we could legislate some standard that would encourage people—or not encourage, that would mandate and that would flow to your jurisdiction that as a fair trade practice people must post right up front what the options are. That is maximizing choice.

In the context of measuring against the harm that may be done, is that not a balance?

Ms. BERNSTEIN. The Commission has already recommended just that notice and just that choice in connection with all commercial website activity. So it would certainly go a long way toward bringing about a much better balance than exists today.

Senator KERRY. Well, let me go a step further. If citizens are as concerned as you say they are, then the opt-in, opt-out issue becomes more important. Some people would argue that the initial opt-in is when you buy your computer, turn it on, and go to a site. That is opting in.

Ms. BERNSTEIN. It is correct that some people argue that.

Senator KERRY. Then, if on that site there is a prominent display about how the information may or may not be handled, they have a next threshold level at which they can exercise again a choice of opt-in, opt-out, correct?

Ms. BERNSTEIN. Under present circumstances, Senator?

Senator KERRY. No, assuming you had adequate notice that was posted.

Ms. BERNSTEIN. Right.

Senator KERRY. So then the consumer is making a choice, correct? And the down side of harm is that it may be that they had adequate posting of X, Y, or Z profiling process or they may be targeted for some sale or something. If their financial and health information is completely and totally protected, would you not have gone an extraordinary distance here to sort of set a standard as to how we view privacy without becoming overly intrusive and overly regulated and overly structured in a way that might inhibit the creativity of the marketplace?

Ms. BERNSTEIN. I think everyone agrees that it would go a long way to have those kinds of protections for financial and medical information. There are other areas of sensitive information, at least to some people, for example, their religious preferences or organizations that they belong to, that they may consider as highly confidential to them.

Senator KERRY. Is any of that protected in the offline world?

Ms. BERNSTEIN. I do not know that it is routinely collected.

Senator KERRY. The answer is no.

Ms. BERNSTEIN. I believe not.

Senator KERRY. Okay. So the bottom line comes to this question of what definition of "privacy" are we prepared to recommit ourselves to with respect to the American people, online or offline, so that we are not somehow picking winners and losers in the process. I will pursue that later, and I thank the chair.

The CHAIRMAN. Thank you, Senator Kerry. I thank my friend.

We have been almost an hour and a half and we have another panel. So I thank you, Ms. Bernstein, Mr. Medine, and guru. Thank you very much.

The next panel is: Mr. Jules Polonetsky, who is the Chief Privacy Officer of DoubleClick; Daniel Jaye, the Chief Technology Officer of Engage Technologies; Mr. Marc Rotenberg, who is the President of the Electronic Privacy Information Center; and Mr. Richard Smith, an Internet consultant.

Mr. Polonetsky, we will begin with you. Welcome and thank you for your patience.

STATEMENT OF JULES POLONETSKY, CHIEF PRIVACY OFFICER, DOUBLECLICK

Mr. POLONETSKY. Thank you, Mr. Chairman. Thank you, Senators. Thank you for holding this hearing on the critical issue of online profiling and Internet privacy. As Chief Privacy Officer at DoubleClick, I report directly to the company's Board of Directors to ensure that DoubleClick is effectively implementing its privacy policies and procedures. I act as a resource for Internet users. I work with advertisers and publishers to oversee their privacy policies and I work to educate the public about Internet privacy.

I appreciate the opportunity to testify today. In order for the Internet to continue to flourish—in order for this revolutionary medium to keep growing at such a rapid pace and be the engine for the greatest economic expansion in U.S. history—the Internet industry must make consumers comfortable that their privacy is being protected online, and at the same time publishers and ad servers must continue to customize and personalize web content and advertising so that users can get the information they want and websites can generate the revenues necessary to stay in business and keep content on the Internet free.

Currently, a vast majority of websites offer content free of charge. From *The New York Times* to *The Washington Post* to Encyclopedia Britannica, sites offering directions, weather information, content is offered to consumers for free. Why? Because of effective Internet advertising. By keeping the Internet free, Internet advertisers help bridge the digital divide for consumers. Internet advertising revenue also helps smaller startup websites offer unique and diverse content and compete with more established businesses.

As the consumer affairs commissioner in New York City for Mayor Giuliani for the past two years, I saw firsthand the consumer benefits of effective advertising. In markets where merchants were competing successfully, consumers had many choices and were easily able to find the products and services they needed.

In markets where advertising was limited or ineffective and where it was difficult for merchants to reach the right consumer at the right time, such as funeral services or prescription medications, prices varied by as much as 40 percent or 50 percent from location to location. The result: many consumers overpaying for services and products they needed.

On the Internet, advertising is effective for consumers and advertisers when ads reach the right consumer at the right time. Internet advertising companies use information to attempt to deliver the ads to consumers that the consumers are likely to click on.

As Senator Kerry noted, this happens every day in the offline world. Catalogue companies share their mailing lists with each other. Magazines share subscription lists, and political candidates use voting lists so they can send persuasion or fundraising mail only to the voters likely to respond. This is the heart of offline direct marketing and it is critical to effective advertising on the web.

Now, we at DoubleClick understand and take very seriously the privacy issues raised by the technological tools used for effective web advertising. We also understand that the different types of information used need to be treated very differently. Not surprisingly, consumers understand that certain information in the wrong hands can be harmful to them and that some information, like marketing data, does not pose a threat.

Research that we conducted showed that consumers are very concerned about the collection of social security numbers, a fear of identity theft. They are concerned about their credit card numbers, information that could be used against them. People have very practical concerns. They are worried about the collection and sharing of sensitive credit information that could be used to deny them mortgages, sensitive health information that could be used to deny them insurance.

It is DoubleClick's policy not to use sensitive information for profiling when we deliver an ad. We do not use health information, we do not use sensitive financial information, visits to adult sites, sexual information, information about children. The example that the FTC presented and that, Senator McCain, I think you referred to as relatively innocuous frankly is the kind of ad serving that we do.

Consumers are much less concerned about transaction data used for marketing purposes, but we do believe that they have a right to know—even if it is not sensitive data—data about basic transactions. Consumers have the right to know what kind of data net advertisers are using and they have the right to have control over that use. There are significant steps that industry can and should take to give consumers more confidence in and more control over their web experience. Primary among them are notice and choice.

Consumers need and deserve real choice. They need to know the type of data that is being collected about them and they need to have the ability to opt out, to choose not to participate if they want to. We recently finished one of the largest Internet education campaigns in web history. We served more than 100 million banner ads connecting consumers to privacychoices.org, a website dedicated to consumer privacy education, offering a two-clicks-and-you-are-out policy for consumers who wanted to opt out of targeted advertising.

At DoubleClick, no website is allowed to contribute profile information or to have ads delivered based on any cross-web behavior unless their privacy policy links to DoubleClick to give consumers notice about what is going on and a chance to opt out.

We are also rewriting our privacy policy to make it shorter, clearer, and easier for consumers to understand. We employ an outside auditor, PriceWaterhouseCoopers, to do an external audit periodically to ensure that we are living up to the privacy commitments that we make to consumers, and we have an independent consumer privacy advisory board to help us continue to improve our privacy procedures and to respond to the new issues that will continue to arise as new forms of e-commerce develop.

Finally, as part of the network advertising initiative, we are working with the other companies in our industry to develop uniform rules for all third party advertisers to follow to ensure that our activities are clear and understood by consumers and to ensure that consumers have control over how we use information.

We recognize that consumers must know that their privacy is protected online for e-commerce to continue to flourish and we welcome your ideas for additional steps that we can take to benefit consumers.

Thank you.

[The prepared statement of Mr. Polonetsky follows:]

PREPARED STATEMENT OF JULES POLONETSKY, CHIEF PRIVACY OFFICER, DOUBLECLICK

Thank you for holding this hearing on the critical issue of online profiling and Internet privacy. As Chief Privacy Officer at DoubleClick, I report directly to the company's Board of Director's to ensure that DoubleClick is effectively implementing its privacy policies and procedures, act as a resource for internet users, work with advertisers and publishers to oversee their privacy policies and work to educate the public about internet privacy. I appreciate the opportunity to testify today.

In order for the Internet to continue to flourish—in order for this revolutionary medium to keep growing at such a rapid pace and be the engine for the greatest economic expansion in U.S. history—the Internet industry must make consumers comfortable that their privacy is being protected on-line. And, at the same time, publishers and ad servers must continue to customize and personalize web content and advertising so that users can get the information they want and websites can generate the revenues necessary to stay in business and keep the Internet free.

Currently, a vast majority of Web sites offer content free of charge. From *The New York Times* to *The Washington Post* to Encyclopedia Britannica and sites offering directions and weather information, content is offered to consumers for free. Why? Because of effective Internet advertising. By keeping the Internet free, Internet advertisers help bridge the digital divide for consumers. Internet advertising revenue also helps smaller start up Web sites offer unique and diverse content and compete with more established Web sites.

As the Consumer Affairs Commissioner in New York for Mayor Giuliani for the past two years, I saw firsthand the consumer benefits of effective advertising. In markets where merchants were competing successfully, consumers had many choices and were easily able to find the products and services they needed. In markets where advertising was limited or ineffective and where it was difficult for merchants to reach the right consumer at the right time—such as funeral services or prescription medications—prices varied by as much as 40% from location to location and many consumers overpaid for services and products they needed.

On the Internet, advertising is effective for consumers and advertisers when ads reach the right consumer at the right time. Internet advertising companies use information to attempt to deliver the ads to consumers that they are likely to click on.

This happens every day in the off-line world. Catalogue companies share their mailing lists with each other. Magazines share subscription lists. And political can-

didates use voting lists so they can send persuasion or fundraising mail only to likely voters.

This is the heart of off-line direct marketing. And it is critical to effective advertising on the Web.

Now, we at DoubleClick understand and take very seriously the privacy issues raised by the technological tools used for effective Web advertising. We also understand that different types of information need to be treated differently.

Not surprisingly, consumers understand that certain information in the wrong hands can be harmful to them and that some information—like marketing data—does not pose a threat.

Research conducted for DoubleClick showed that consumers are very concerned about the collection of social security numbers—in other words, a fear of identity theft—credit card numbers and information that can be used against them. People have very practical concerns—they are worried about the collection and sharing of sensitive credit information that can be used to deny them mortgages and sensitive health information that can be used to deny them insurance.

It is DoubleClick's policy not to use sensitive information for profiling when delivering an ad. We do not profile using health information, detailed financial information, visits to adult sites or sexual information, or information about children.

While consumers are much less concerned about transaction data used for marketing purposes, we believe they have a right to know what type of data is being used by network advertisers and have the right to have control over that use.

There are significant steps that industry can and should take to give consumers more confidence in and control over their web experience. Primary among them are notice and choice. Consumers need and deserve real choice. They need to know the type of data that is being collected about them and have the ability to opt-out—to choose not to participate—if they want to.

We recently finished one of the largest Internet education campaigns in Web history . . . 100,000,000 banner ads connecting consumers to www.privacychoices.org, a website dedicated to consumer privacy education and offering a two-clicks-and-you're-out policy for those who wish to opt-out of targeted advertising.

At DoubleClick, no Web site is allowed to contribute profile information or receive ads based on cross web behavior unless their privacy policy links to DoubleClick to give consumers notice and a chance to opt-out.

We are also re-writing our privacy policy to make it shorter, clearer and easier to understand.

We employ PriceWaterhouse Coopers to provide an outside audit to ensure we are living up to the privacy commitments we make and we have appointed an independent Consumer Privacy Advisory Board to help us continue to improve our privacy procedures and respond to new issues that will arise as new forms of e-commerce develop.

And finally, as part of the Network Advertising Initiative, we are working with the other companies in our industry to develop uniform rules for all third party advertisers to follow to ensure that our activities are clear and understood by consumers and to ensure consumers have control over how we use information.

We recognize that consumers must know that their privacy is protected online for e-commerce to continue to flourish and we welcome your ideas for additional steps that we can take to benefit consumers.

Thank you.

The CHAIRMAN. Thank you very much.

Mr. Jaye, welcome.

STATEMENT OF DANIEL JAYE, CHIEF TECHNOLOGY OFFICER, ENGAGE TECHNOLOGIES

Mr. JAYE. Thank you. Thank you, Mr. Chairman. My name is Daniel Jaye. I appreciate the opportunity to appear before you today. I am the Chief Technology Officer and co-founder of Engage, Inc., of Andover, Massachusetts. When I joined with CMGI Chairman and CEO David Weatherall to create Engage in 1995, we were guided by the fundamental proposition that effective, tailored online advertising was vital to the Internet's future, but could ultimately be effective only if consumers found online targeted adver-

tising a valued customized information service and not an unwelcome intrusion. This is only more clear today.

If the Internet is going to bridge—and not widen—the digital divide, advertising support is essential. Today, however, three out of four Internet ads remain unsold or undersold, and the great majority of websites remain unprofitable. The traditional advertisers we need will commit to the web only if they can achieve the effectiveness attainable offline and something more as well. That is where online profiling comes in.

Using various business models and technologies, online network advertisers enable website visitors to receive news, information, and ads customized in real time to their demonstrated interests. At Engage, we have developed a distinctive anonymous profiling model that enables online marketers to deliver the relevant ads to the right audience. In this model, while we do provide notice and choice, we do not know a consumer's name, address, social security number, or any other personally identifiable information.

We do not maintain information about the specific websites a browser visits. We do not collect any sensitive or controversial data, such as personal medical or financial data, ethnic origin, religion, political interests, or review of adult content. And we do not merge anonymous profiling data with personally identifiable data, no matter what the source.

Instead, we simply derive an apparent interest level score by looking to the aggregate amount of time a browser has spent on different types of content, very similar to the demonstration we saw earlier. We do not look at who they are or where in particular they have been on the web. Our patent-pending, dual-blind technology creates a firewall that prevents our customers from gaining access to our interest profiles or determining a visitor's real world identity.

Industry-wide as well, elegantly simple technological tools are emerging for consumers to ensure their privacy. We are particularly excited about an outgrowth of the Platform for Privacy Preferences project, P3P, that is specifically focused on cookies. Engage has authored and is working with other industry leaders on this trust labels technology that would recognize automatically whether a website's use of cookies meets third party seal organization standards and the user's own standards.

Moreover, any third party that attempts to set a cookie but does not meet these standards will trigger a warning on the computer screen, instantaneously allowing the consumers to block the business from collecting data. Unless and until it reforms its practices to meet the standards of privacy seal organizations, the bad actor will actually be locked out of the marketplace. This more than any regulation will drive widespread, indeed global, compliance with seal programs.

In addition, market forces are driving the online industry to raise the bar for protection of consumer privacy through effective industry standards, through increasingly vigorous seal of approval programs, through contractual commitments that extend the reach of industry standards to our business partners, and through stepped-up consumer and business education.

Through the network advertising initiative, we are ensuring that our network advertiser segment of the marketplace embraces each of these mechanisms and expands upon prevailing industry standards in a clear, public, and enforceable way. You should be hearing soon about the particulars of the significant standards and practices to which our sector has committed.

The growing marketplace premium on privacy protection makes the commitment to self-regulation of our business particularly credible. We welcome the spotlight on privacy. Engage feels confident that its own technology, business models, and commitment to consumer privacy will continue to meet or exceed the highest of any industry standards or government mandates.

But the early adoption of a regulatory framework or, worse yet, a patchwork of regimes could undermine these surging market incentives to develop and deploy technological advances and privacy protection. Instead of setting a floor that turns into a ceiling as well, policymakers would, I believe, be well served to test the dynamism of technological innovation and the power of the market to deliver on this promise before moving forward.

Thank you.

[The prepared statement of Mr. Jaye follows:]

PREPARED STATEMENT OF DANIEL JAYE, CHIEF TECHNOLOGY OFFICER, ENGAGE TECHNOLOGIES

Thank you, Mr. Chairman. I appreciate the opportunity to testify before you today on these issues of importance to your Committee, to Internet users, and to the future of our Internet economy.

My name is Daniel Jaye. I am the Chief Technology Officer and Co-Founder of Engage, Inc. of Andover, Massachusetts. Engage is a leading provider of technology and services that allow website operators and advertisers to tailor their commercial and editorial content in innovative ways likely to be of the greatest interest to a visiting Internet user—all without tracking, or ever learning, an individual's identity.

Since co-founding our company in 1995, I have been engaged in the design and development of privacy-sensitive online marketing solutions—including inventing the Internet's first anonymous profiling technology, participating as a founding member of the initial so-called "P3P" specification and as author of the related "TrustLabels" specification (developments I'd like to highlight shortly). I have also actively participated in a number of significant industry online privacy standards initiatives, including the Network Advertising Initiative (NAI). And I have recently served as a member of the Federal Trade Commission (FTC) Advisory Committee on Online Access and Security, and a panelist in the FTC/NTIA Online Profiling Workshop in November 1999.

I would like to address three topics today:

- First, the fundamental role served, and the basic models used, by online network advertisers;
- Second, the technological tools and developments that are bolstering the power of industry—and indeed the power of consumers themselves—to promote privacy-sensitive online practices; and,
- Third, the potent market forces that are compelling online businesses to provide consumers real assurance that they can surf the web without unwittingly sacrificing their personal privacy.

I might note that I offer these comments not in an effort to demonstrate that there could never be a place for legislation in this area, nor out of any concern about the direct impact of proposed privacy legislation on our company's practices. Engage feels confident that its own technology, business models, and longstanding commitment to consumer privacy would continue to meet or exceed the highest of any industry standards or mandates. Yet, I offer these comments because I respectfully believe that it is essential that any legislative deliberations fully appreciate the vital

role, the dynamic technology, and the palpable marketplace forces that shape the online advertising business.

Keeping The Internet Free For All Consumers Through Effective Online Advertising

Let me briefly explain, then, how "online profiling" offers a tool critical to underwriting the Internet's emergence as a remarkable toll-free bridge spanning an otherwise widening societal divide in access to information and commerce. Early online entrepreneurs learned quickly that sustaining a rich array of information and services on the Internet, readily accessible to all consumers, would require a model based on advertising support—and free of subscription fees. And, based on this prevailing model, the Internet has flourished as a remarkably vibrant and innovative source of freely accessible information, entertainment and commerce.

Yet if advertising is truly to provide a viable, long-term foundation for the Internet economy resting upon it, website operators must harness the medium's unique marketing capabilities to allow advertisers to deliver relevant ads to the right audience. Today, however, three out of four Internet ads remain unsold or undersold. And, not coincidentally, the great majority of websites remain non-profitable. The traditional advertisers that we must attract to the web will come in requisite numbers only if they can achieve the measurability and effectiveness that they can achieve offline—and something more, as well. Profiling technology enables this advertising and content to be more effectively targeted to consumers' interests, thus offering a vital means for fulfilling the Internet's rich potential—for consumers, advertisers, and website operators alike.

Different online companies employ different business models and technologies to offer customized news, information and ads on topics of demonstrated specific interest, even when a visitor might be viewing more general interest web pages. And, the types of information collected and used for online profiling can vary among personally identifiable information (PII), non-personally identifiable information (non-PII), or a combination of the two.

- PII is data used to identify, contact, or locate a person, such as name, address, telephone number or e-mail address.
- Non-PII is data that does not identify a particular person and is typically compiled from anonymous clickstream information collected as a browser moves among different websites (or a single website).

The collection of online data relies upon the use of "cookies," which are simply small files of information that most websites place on a user's browser—to provide, in Engage's case, a unique anonymous identifier or, importantly, a message that the browser is set to opt-out from collection of any data about its users.

Harnessing Technology To Make Online Advertising Effective *And* Privacy-Sensitive

When I joined with CMGI Chairman & CEO David Wetherell to create Engage in 1995, we were guided by the fundamental proposition that effective, tailored online advertising was vital to the Internet's future—but could ultimately be effective only if consumers found online targeted advertising a valued, customized information service and not an unwelcome intrusion. From the outset, then, we developed an innovative technology to enable online marketers to understand the interests of website visitors based strictly upon anonymous, non-personally identifiable information.

Relying only on the apparent interests, broad demographics, and general location of a visitor reflected in interest profiles, Web site publishers, advertisers, and merchants can customize web pages and offer content, ads, promotions, products and services tailored to the visitor in real-time—and, at the same time, protect the consumer's privacy by not collecting personal (or otherwise sensitive) information of any kind. In fact, in our anonymous model:

- We do not know a consumer's name, address, social security number or any other personally identifiable information;
- We do not maintain information about specific web pages a browser visits or how long a visitor stays;
- We do not collect any sensitive or controversial data, such as personal medical or financial data, ethnic origin, religion, political interest or review of adult content; and,
- We do not merge anonymous profiling data with personally identifiable data, no matter the source.

Instead, our anonymous profiles consist of a score signifying the apparent level of a user's interests in various categories. We simply look to the aggregate amount of time a browser has spent on different types of content—not who they are, or where in particular they have been on the Web. Our conviction from the start has been that it should never be possible for Engage or anyone else to determine (or even "triangulate") a visitor's real world identity based on our abstracted data.

And we employ additional technological tools and practices to ensure this anonymity. We use firewalls—technological barriers to protect a system—to secure the (already) non-personally identifiable information we collect through a patent-pending technology we call "dual-blind" identification: this way individual websites we work with do not have access to our interest profiles or know what other sites a user may have visited. There is no user interface through which anyone else can gain access to an individual profile. And, even with these technological protections in place, and only non-personally identifiable data at issue, we also provide consumers effective choice regarding whether to participate. We offer clear information about our data collection practices and an opportunity to opt-out of our anonymous information gathering.

In short, Engage's business model not only accommodates, but is in fact borne of, consumer's interest in protecting their privacy interest.

Privacy-Driven Technological Innovation Is Further Empowering Industry And Consumers Themselves To Raise The Bar

Continued technological innovation promises our online industry—and the web visitors themselves—sophisticated yet simple tools to support consumer privacy interests. I can report first-hand that the online industry has indeed brought to bear in the interest of consumer privacy the same zeal for technological break-throughs that have characterized—and fueled—the Internet itself. The result: a remarkable progression of emerging solutions that will offer consumers previously unimagined forms of notice, choice and protection of their own personal privacy demands.

Emerging tools offer not only instantaneous and automatic notice and choice, but more than that, they also would empower consumers essentially to set for themselves just what measure of privacy they demand—and to avoid any sites that fail to meet their personal standards. The Platform for Privacy Project (P3P) at the World Wide Web Consortium (W3C) would enable a web server to communicate automatically how it collects and shares user data so users can define what privacy standards they prefer for that particular site or in general. Engage was a co-author of the P3P Protocol Specification.

Beyond this, we are very excited about a specific application of P3P in the context of "TrustLabels" for cookies. To directly respond to the leading concerns over third party data collection and transparency, Engage has authored and is working with other industry leaders on a specification for TrustLabels, which would allow web servers to provide notice to consumers concerned about certain uses of cookies and would allow consumers the ability to accept or reject a site's data practices. This technology critically serves the goal of universal compliance with privacy standards. It permits consumers to compel online businesses to be privacy-sensitive because those businesses that attempt to set a cookie and do not meet consumers' privacy demands will cause a warning alert to be displayed on the computer screen of the user, allowing a choice (probably "NO") to be made solely by the consumer regarding whether to permit the business to collect data. The business will be unable to collect the data it seeks, unless and until it reforms its practices to meet the standards of privacy seal organizations. The bad actor will actually be locked out of the marketplace. This, more than any regulation, will drive universal compliance with seal programs. And, on the Internet, such technology-based enforcement does not stop at national borders. Certainly this is the sort of technological innovation that no one would wish to discourage with a premature regulatory framework that could stunt this continuing evolution—or, worse yet, a patchwork of such regimes across jurisdictions.

Extending Privacy-Sensitive Practices Through Industry Self-Regulation

Along with this commitment to developing robust technological tools to empower consumers, online industry leaders have relied on a complementary set of additional tools to raise the bar industry-wide for the protection of consumer privacy:

- First, adopting effective standards for industry collection and use of consumer data;
- Second, giving those standards teeth through enforceable and increasingly vigorous seal of approval programs;

- Third, extending the reach of those standards by incorporating them into contracts with other online businesses not already subject to such standards; and,
- Finally but critically, actively educating consumers and business customers about our business and the available means for effectively safeguarding privacy on the Web.

In the few short years over which the Internet has blossomed, the online industry has—through rapidly growing use of these tools—made tremendous strides in voluntary, but self-regulated adoption of "the right way" to do business. And through the Network Advertising Initiative, we are ensuring that our network advertiser segment of the marketplace embraces and expands upon prevailing standards—in a clear, public, and enforceable way.

You will hear in the very near future, I believe, in greater detail about how our NAI standards will effectively incorporate all of the key self-regulatory tools I just described—substantive standards, independent third party certification and enforcement, binding commitments on our customers to follow the same standards, and a campaign to educate the public and our website customers alike.

The Power of Marketplace Demands For Privacy-Sensitive Practices

I will confess that, for Engage, the standards and practices contemplated by industry largely codify the standards we have set for ourselves from the outset. But by no means does that suggest that this self-regulatory initiative, and the recurring spotlight on our industry's business practices, is not making a difference. To the contrary, as a whole, we are working to set a bar and, in certain respects, raise the commonly prevailing bar. More than that, we are fully unleashing an already significant and growing set of marketplace forces—the force of privacy-sensitivity as a competitive advantage. It is a force that we welcome—indeed one we have long harnessed. It is a force that public policy must take care not to squelch. And it is a force that makes the commitment to self-regulation in our business all the more credible.

Our customers know that consumer comfort and security is critical to use of the Internet. In this competitive climate, those businesses serving consumers online ultimately will embrace only those technologies and practices that can provide tailored and effective online advertising *without* compromising consumer privacy. This is a powerful bottom-line force, as ongoing marketplace developments bear witness.

Conclusion

The potent combination of technological innovation, industry standards, contractual requirements extending those standards, enforceable privacy seal programs, consumer and industry privacy education, and FTC enforcement offers a highly reliable and uniquely effective response to online privacy concerns. These initiatives bolster what are already formidable marketplace checks on online businesses' protection of consumer privacy. The needs of our customers to attract—and not repel—consumers will ensure that we get the job done.

But so too is it critical to ensure that we do not needlessly undermine the effectiveness of online advertising by freezing the development of new technological tools to meet consumer and business needs. Instead of setting a floor that turns into a ceiling as well, the power of the market and the dynamism of technological innovation promise continued remarkable developments to protect privacy interests. As I suggested at the outset, the viability of e-commerce, of our advertising-supported Internet, and thus of all the Internet's tremendous economic and societal benefits depends on it.

Thank you.

The CHAIRMAN. Thank you very much.

Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman, members of the Committee. It is a pleasure to be here today. It was actually at a similar hearing a year ago that I described for you a company named DoubleClick, the Internet's largest advertising network, and another company named Abacus Direct, the country's largest database catalogue firm, and I explained following the announcement

of a recent merger that the joining together of the online information in the Abacus Direct database and the surfing records that were being maintained by DoubleClick would raise profound issues for Internet privacy, that users would strongly object to this type of profiling of their Internet activity, and that you would see a public response.

Indeed, that is what happened over the past year. The public responded, the FTC responded, State attorney generals responded, because people understood that in their use of the Internet—in the desire to obtain information online and receive the benefits of electronic commerce it did not seem fair or right that they should have to sacrifice their—privacy.

Now, the online advertising industry will say: We are providing great benefits. We are providing free content. We are making it possible for people to get access to information and systems. But I think it is important to keep two points in mind.

First, advertising has always supported the delivery of editorial content. Whether it is a radio broadcast, a TV spot, magazine ad, or a billboard, there have always been ways for advertisers to market to consumers to support the delivery of information. What is different about the Internet, and it is different, is that this is the first time that it has been possible for advertisers to profile the people who receive information, to build detailed dossiers about their interests, their preferences, their likes, and their dislikes. In this respect the Internet world is different from the offline world. There is a different type of privacy problem made possible by the creation of a digital network.

Now, a second point to keep in mind is that Congress has in the past confronted this issue of how we deal with the creation of personal profiles. This is not the first time. In fact, more than 30 years ago when people looked at the practices in the credit reporting industry and said, look at this detailed information that is being put together about how people live, whether they are married, what they earn, what time they show up at work, there has to be some control on the collection and use of this information.

So Congress 30 years ago passed privacy legislation to control the collection and use of credit record information, to make sure that improper information was not collected and that the information that was collected was not used improperly.

Similar issues were raised about the potential of Big Brother databases in the Federal Government. In the 1960's, Federal agencies were bringing in automation and people realized that it would be possible to create very detailed profiles of American citizens. So, over time a legislative framework called the Privacy Act was put in place which gives every citizen in America the right to limit the collection and use of information about them and, critically, to see the information which is collected.

My suggestion to you today is that what we are facing with Internet profiling is in fact not a new problem. It is a familiar problem. It is the detailed collection of information, the creation of profiles, enabled by technology. Now, of course it is a wonderful technology and we really do not need to dispute the benefits of the Internet. The question is, are we going to have to trade our pri-

vacy, lose control of this information, to receive the benefits of the Internet.

I think over the last five years as the FTC and the sponsors of legislation, this Committee, privacy groups—my own, Junkbusters and others—we have realized that there is simply not a need to make this trade. We do not need to choose privacy or the benefits of the Internet. We really should have both.

Pulling it all together, I think the key point here is that when I came to you a year ago and said that this type of profiling is going to create problems, I also suggested that there were ways to do online marketing, online targeting, that would be good for business, good for consumers, and would not create these types of privacy problems. So what we needed, and what we still need, is the baseline privacy legislation that establishes an opt-in requirement, that gives people the right to access those profiles, and in some cases the right to have their personal information deleted if they no longer have a relationship with a company or they do not want to have a future relationship with a company.

Those baseline standards will encourage the development of very good online business practices, very good privacy technology. They will not stand in the way of innovation and they will give people the benefits of the Internet and provide privacy protection.

So I thank you very much for the chance to be here, and I will be pleased to answer your questions.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Summary

Privacy organizations that favor legislation to protect privacy have also been the leaders in the effort to establish good technology to protect privacy. Our view is that good privacy technologies will depend very much on the regulatory environment. Laws such as export controls that limit the availability of encryption or the requirements of the Communications Assistance for Law Enforcement Act, now before a federal appeals court, will discourage the development of good techniques to protect privacy. On the other hand, laws that implement Fair Information Practices, such as the Privacy Act of 1974, will have a positive impact on the development of technology. Privacy legislation is appropriate for the Internet because it will have a positive impact on the development of technologies to protect online privacy.

In the matter of Doubleclick, we first brought the Committee's attention to this problem at a similar hearing a year ago. We warned that self-regulation would fail to protect privacy and that there would be a public backlash against the company's plan to profile Internet users. We think the lesson is clear that legislation is necessary. Even good models for online advertising can quickly change without baseline privacy rules.

Going forward, we think the key is the development of techniques that implement common-sense Fair Information Practices and that minimize or eliminate the collection of Personally Identifiable information. Techniques for profiling that are not based on the identity of an actual user may be acceptable. But any system of profiling that could be linked to a user, even if that is not intended at the beginning should be subject to legal safeguards. The experience with Doubleclick has made this clear.

In terms of P3P, we do not view this as a technology that will promote privacy. It builds on the very weak "notice and choice" approach that is increasingly asking consumers to trade their privacy for the benefits on electronic commerce. It is not fair to force consumers to make this choice. Good technologies that aim to protect consumer privacy will not be built on this model.

We need privacy legislation to establish baseline standards for electronic commerce. We also need to look closely, with input from technical experts and experts in privacy, at how best to develop technologies that protect online privacy. We need

a much broader right of access in the online world than currently exists in the offline world precisely because the online world enables such far-reaching profiling. Finally, we need to think more deeply about the true nature of profiling in the online world. The establishment of persistent profiles, beyond the control or scrutiny of the individuals affected, can stigmatize and reduce opportunity for some even as they create benefits for others.

Testimony

My name is Marc Rotenberg, and I am Executive Director of the Electronic Privacy Information Center in Washington, DC. I am grateful for the opportunity to appear before the Committee this morning and also for your efforts in developing good privacy legislation that responds to growing public concern. Last year I testified before you on the growing risks to Internet privacy and described a firm named Doubleclick that had announced a merger with Abacus Direct. I warned in my testimony that Doubleclick proposal to profile Internet users showed the problems with the self-regulatory approach to privacy protection and that it would lead to a vast privacy backlash.

This morning I will focus my comments specifically on one of the central questions in the ongoing effort to protect privacy online—what is the relationship between privacy legislation and privacy technology? With legislation pending before the Committee, and many companies developing privacy technologies, I am sure you are trying to understand the relationship between privacy legislation and privacy technology. Are they alternatives? Should we have both? What happens with technology if we continue to go forward without legislation?

Privacy Advocates Have Long Encouraged the Development of Technology to Protect Privacy

To answer these questions, I need to say a few words about the establishment of EPIC. The Electronic Privacy Information Center, which has long favored the adoption of legislation to protect Internet users, has also been on the front lines to ensure that Internet users would have access to the best technology to protect privacy. Several years ago there was a widespread belief in government that it would be necessary to limit the availability of strong technology, such as encryption, that would protect personal privacy. We strongly opposed this view and said that these technologies should be widely available to the general public. We argued that privacy technology was good for consumers, good for business, and ultimately good for national security. We prepared a letter to the President by experts, opposing the Clipper proposal to establish the escrowed encryption standard. That letter was later endorsed by 50,000 users of the Internet who agreed that good technology was critical to good privacy. The administration eventually changed its views and today the United States policy on encryption favors the development of good tools to protect personal privacy, though I should add that it is still the case that electronic mail is not routinely encrypted, though I think it should be.

Since the Clipper campaign, we have also urged the development and adoption of the very best technical means to protect personal privacy. Our website contains a popular page—Practical Privacy Tools, which was featured in the New York Times just last week. The page includes techniques for encryption, anonymity, cookie management, and more.

Members of the EPIC staff have even trained human-rights advocates and journalists in different parts of the world how to use encryption to protect their private communications from police forces and governments that would send a person to jail for what he might write in a private message. We supported the widespread use of anonymous re-mailers, PGP, robust encryption, and other privacy tools, when many industry groups waited quietly in the wings for the policy debate to play out.

Although lobbyists like to characterize privacy advocates as favoring "heavy-handed Government regulation" in fact we were far ahead of industry on proposing technical solutions to privacy protection. We have been pressing for good technical solutions to protect privacy before the vast majority of Internet-based companies were even established.

And when groups in industry or government have gone forward with technical standards that threaten individual privacy—the Clipper chip, the Intel Processor Serial Number, the FBI wiretap standards, the Microsoft Global Universal Identifier—we launched national campaigns, in association with such groups as Junkbusters, the ACLU and others to bring public attention to the growing risks to privacy.

Privacy Legislation is Critical to Privacy Technology

So why do we favor legislation? The answer is that our experience over the last ten years shows that you will get better technologies to protect personal privacy

where there a legal framework in place that establishes baseline privacy standards. The Clipper proposal came about in the United States but not in Europe or Canada. One of the reasons is that European and Canadian privacy laws and European and Canadian privacy agencies prevented the adoption of a technical standard that would have enabled such widespread surveillance of privacy communications.

Doubleclick pushed forward with its profiling scheme in the United States but not in Europe because European law would have required to Doubleclick to follow a set of privacy rules once it started collecting personal data. Doubleclick decided it didn't want to bother complying with privacy rules so it pushed forward in the United States.

Many of the Internet protests that are taking place in the United States result from the failure to develop good privacy standards. Some might say that this is because the US is a leader in technology and first to experience the social consequences when companies go too far. But in fact, in many critical sectors—online banking, Internet use, cell phone use—the US is not the leader but is still facing enormous public concerns about the loss of privacy. The reason is simply that whereas other countries have made some effort to update their privacy laws to keep pace with new technology, the US stubbornly refuses to do so. And in the United States where privacy legislation is in place, you simply do not see the type of invasive profiling that companies like Doubleclick have pursued on the Internet.

The message here is simple: privacy laws encourage good business practices and good privacy technologies. Where those laws exist, you can have innovation and privacy protection. Where the laws do not exist, you may still have innovation, but I doubt you will have privacy protection.

The Profiling Problem is Not New

Although the Internet and Doubleclick appear to raise new problems, in many ways Congress has confronted similar problems in the past and developed appropriate legislative solutions.

More than thirty years ago there was a proposal to establish a centralized databank in the United States called the National Data Center that would have provided detailed profiles on American citizens. The purpose was benign. It was believed that such a databank would be very useful to social scientists and others, but the implications were severe. People understood that the collection of these permanent profiles, made possible by computerized automation, would pose a threat to the privacy and liberty of American citizens. The proposal for the National Data Center was withdrawn and over time a comprehensive legal framework—the Privacy Act of 1974—was established to safeguards the rights of American citizens. The Privacy Act imposed on all federal agencies essential privacy rights and responsibilities—"Fair Information Practices"—that would limit would federal agencies could do with personal information and gave every American the right to see the information about them that was collected.

Significantly, the Privacy Act did not slow the use of computers. It simply made the people who were designing those systems more aware of their obligations to protect the privacy interests of the people whose information was collected. In other words, the Privacy Act helped ensure that as automation was introduced in the federal government, privacy was built-in at the outset.

Now I want to be clear at this point, that I am not defending all data collection practices by the federal government. I think there are any number of programs where data collection is too intrusive. Nor do I think the Privacy Act is beyond criticism. Recent amendments appropriately strengthened the penalty provisions to help ensure that there would be sufficient incentives to pursue enforcement, and recent court opinions have asked, appropriately in my view, whether the Privacy Act should apply to the White House.

But the critical point is clear: law is necessary to limit profiling, such law does not discourage innovations, and the US Privacy Act provides a clear example of how such laws can operate successfully.

Lessons of Doubleclick

To understand Doubleclick, I think it is important to think about how advertising has operated traditionally. Whether in the print world with magazine ads and billboards or the communications world with radio spots and TV ads, advertisers large and small have been able to reach their audience without collecting any personal information. This is true when 30 million people watch the same beer commercial on a television football game or when 30 people see an ad for a used kitchen table in the classified section of a morning newspaper. Advertisers communicate information to an audience without trying to create detailed profiles.

Advertisers have always been able to tailor ads to specific markets. With the Internet it is even easier to do. The subject matter can be more focused, the information more timely. Advertisers also get almost instantaneous feedback on which ads are working and which are not. Follow an auction on one of the auction sites and you will see just how well the Internet enables targeted advertising between buyer and seller and still protects privacy.

All of these factors suggest that the Internet could be a very effective way for marketers to reach customers with a minimal privacy intrusion. But Doubleclick, and in fairness, several of its competitors, pushed the envelope and decided that reaching customers, regardless of the privacy consequences, was the way to go. Not content with the most effective and efficient form of advertising ever made possible, these companies began plans to profile net surfers, to link anonymous clickstream data with detailed and personally identifiable purchase records. They called it "personalization" but the process is "profiling" and the method involves the secretive collection of personal information about consumers.

The schemes were deeply flawed, both as a matter of policy and technology. Doubleclick essentially ignored all of the generally accepted privacy rules. People could not see what information would be collected or determine how it would be used. Doubleclick couldn't even comply with their own privacy policy. As we pointed out in our complaint to the Federal Trade Commission, the privacy policy at the Doubleclick website was constantly being revised. First, Doubleclick's privacy policy assured users who received targeted ads from Doubleclick that they would remain "completely anonymous." Then Doubleclick dropped the reference to anonymity and said the information was not "personally identifiable." More recently, following the merger with Abacus Direct, Doubleclick said that if it joined the two databases it would further revise its privacy statement to reflect its "modified data collection and data use practices."

There was no way any consumer could make a meaningful decision about whether to disclose personal information to Doubleclick. Doubleclick could essentially do with the information whatever they wished. They might as well have scrapped their privacy policy and put up three words "subject to change."

The technology was just as bad. Even Doubleclick's business partners were not aware of how personal information was being collected. Kozmo dropped Doubleclick when they realized that videotape rental records were being transferred by the advertising network, most likely in violation of the Video Privacy Protection Act. Web sites offering healthcare advice learned to their chagrin that they were passing on medical information on their visitors through the Doubleclick network. Even the opt-out scheme proposed by Doubleclick had problems. Customers who wanted privacy would be required to store a Doubleclick cookie on their computer. Not a very smart idea when consumers, trying to protect their privacy, are routinely deleting cookies.

By the time Doubleclick dropped the plan, the company was facing investigation from the Federal Trade Commission, two state attorneys general, and a host of private litigants. Doubleclick's problems were hardly caused by the campaigning of a few privacy advocates; virtually anyone who thought about the long-term implications of profile-based advertising saw the problem.

Doubleclick CEO Kevin O'Connor was right to admit a mistake and should be commended for responding, albeit belatedly, to growing public concern about privacy in the online world. The question now is what lessons will be learned. Is this simply a matter of "issue management," or is there an opportunity for a genuine exploration of how to develop business models for the Internet that are profitable and also respect consumer privacy? My hope is that the industry will take the second course. But this will mean taking seriously the need to develop strong and effective privacy measures.

If net advertisers intend to collect personal information on Internet users, they should follow the most stringent Fair Information Practices. That's not just about giving individuals "notice and choice," it's about allowing individuals to know what the company knows about them, and to object to the use of the information and even to have it permanently deleted if they wish. It's about being more open and accountable in how personal information will be used. Access to a privacy policy is never as good as actually being able to see how someone else will use your personal data.

Better of course would be for innovative firms to take advantage of the extraordinary flexibility of the Internet and develop advertising models that do not rely on the collection of personally identifiable information. Several advertising firms currently do this and others should consider it as well. There is every reason to believe that advertising models that respect consumer privacy can be made to work in an environment as dynamic as the Internet.

Support for privacy legislation that would establish baseline standards across the industry would also be a good move. Self-regulation has its advantages, but in the world of privacy it simply protects bad actors. A better approach would establish simple, uniform, predictable rules for business and consumers. A legal principle in support of anonymity will do a lot to spur the development of robust technologies of privacy.

One argument that simply does not fly is that the surreptitious profiling of customers' private activities—what websites they visit, what articles they read, what pictures they watch—is necessary to support the Internet. That's an argument without bounds and one the Net advertisers should drop quickly if there is going to be a real discussion about how to protect privacy online. The Internet is growing rapidly in countries that do not permit these practices. In fact Internet penetration is higher in several countries that have stronger privacy rules than the United States.

Consumers are serious about the need for privacy protection on the Internet, and they do not see a need to trade their privacy for their ability to use the Net.

The Danger of Notice and Choice

Too often, the privacy problem is viewed as requiring the offering of notice and choice to consumers. But this is not the approach that the United States has typically taken to ensure privacy protection in other sectors, even those where there is rapidly changing technology. The privacy of cable subscriber records is protected because of a provision in the Cable Act. The privacy of video rental records is protected by the Video Privacy Protection. The privacy of telephone calling records is protected by a series of laws and regulations. But "choice" is what consumers face where there is no baseline privacy protection.

You have probably already heard about something called "P3P" and you are no doubt going to hear more about this in the future. This is a technical proposal developed by the World Wide Web consortium to facilitate the collection of personal information on the Internet. Many in industry believe that this standard will help solve the privacy problem because it will facilitate choice about privacy practices. But the real choice offered is not how to protect privacy, but how much privacy to give up. The FTC Chairman made the point very well that the reason we need privacy laws today is that consumers are too often asked to give up their privacy for some benefit.

We need strong technical measures that give people greater control over the collection and use of personal information, and that limit where possible the collection and use of personal data. Consumers should not be forced to choose between the protection of privacy and the benefits of electronic commerce.

Recommendations

First, we need privacy legislation to establish baseline standards for electronic commerce. Until there is legislation, you will see public protests grow. But in those sectors where there is good legislation, you will hear fewer complaints, except to see that the laws are in fact enforced. Even where companies are doing the right thing today, there is no assurance that they will continue to do so tomorrow. Remember that Doubleclick began with the exact same approach to Internet advertising that some today will hold up as a model. But that model collapsed because there were no baseline privacy rights in place to hold it up.

Second, we need to look closely—with far more input from technical experts and experts in privacy—at how best to develop technologies that protect online privacy. Too many of these standard-setting discussions are dominated by the industry groups that have opposed privacy legislation and would much prefer technical standards that encourage people to trade privacy rather than to retain privacy. Privacy experts believe that we can develop good technical standards for privacy protection built on a legal framework that protects the interests of consumers and still encourages innovation. We do not think that users of the Internet should face a bewildering range of choices to protect their reasonable expectation of privacy in the collection and use of their personal information.

We need a much broader right of access in the online world than currently exists in the offline world precisely because the online world enables such far-reaching profiling of private behavior in a way that is simply not possible in the physical world. The FTC's recent report on this subject failed to make clear this essential point.

Any company that creates a persistent profile on a known user, or that could be linked to a known user, should be required to make known to that user all of the information that is acquired and how it is used in decisions affecting that person's life. The profile should always be only "one-click" away—there is no reason on the Internet that companies should force users to go through elaborate procedures or

pay fees to obtain this information about themselves. Access will promote transparency and accountability. It is vital to consumer trust and confidence.

It would also be appropriate in many cases to give individuals the right to compel a company to destroy a file that has been created improperly or used in a way that has caused some harm to the individual. Data could still be preserved in an aggregate form, but individuals should be able to tell a company that they no longer have permission to make use of the personal information that they have obtained.

Finally, we need to think more deeply about the true nature of profiling in the online world. Profiling raises significant questions about identity, grouping, and what information people receive and what information they do not. Of course, such lines are drawn all the time, but it is the establishment of persistent profiles, beyond the control or scrutiny of the individuals affected, that can stigmatize and reduce opportunity for some even as they create benefits for others. Privacy law will help make companies more accountable and reduce the risk of unfair or inaccurate decisionmaking.

Conclusion

We are not simply talking today about Internet privacy. More and more of our lives—entertainment, private communications, banking, reading, buying products, getting the news—all of this is taking place online. We are really talking about the future of privacy in the twenty-first century and whether there will be good standards in place to protect personal information or whether companies will be free to build secret, elaborate profiles that will determine where we go and what we see in this new world.

Technology will clearly play a role in privacy protection. Technologies that protect privacy will enable online transactions without requiring the disclosure of actual identity as much as possible. Technologies that protect privacy will minimize or eliminate the collection of personally identifiable information.

But technology is not enough. Legislation that enforces common-sense Fair Information Practices is necessary to protect the interests of Internet users and it will also play a critical role in the development of these new technologies. It will protect privacy where privacy technologies have not been deployed. It will properly place burdens on companies that chose not to use good techniques to protect privacy. And it will support the development of technologies that will genuinely protect privacy.

We are living in a time when we can still exercise choice over the future of the Internet. I don't mean simply the choice of a single person trying to comprehend a complicated privacy policy, but the choice of a country to safeguard its basic freedoms even as it enjoys the benefits of new technology. Legislation is the way we express this choice and legislation is the path toward technologies that will safeguard privacy interests in the future.

References

Phil Agre and Marc Rotenberg, eds., Technology and Privacy: The New Landscape (MIT Press 1997)

EPIC Doubleclick page
[www.epic.org/doubletrouble/]

EPIC, Online Guide to Practical Privacy Tools
[http://www.epic.org/privacy/tools.html]

Oscar H. Gandy, Jr., Exploring Identity and Identification in Cyberspace, *Notre Dame Journal of Law* (forthcoming)

Junkbusters Doubleclick page
[www.junkbusters.com/doubleclick.html]

Peter G. Neumann, Computer Related Risks (Addison Wesley 1995)

Marc Rotenberg, Testimony and Statement for the Record on The Online Privacy Protection Act of 1999, S. 809, Before the Subcommittee on Communications of the Senate Committee on Commerce, Science and Transportation, 106th Cong., 1st Sess. (July 27, 1999), reprinted in Congressional Digest, February 2000

"Weblining," Businessweek, March 26, 2000
[http://www.businessweek.com/2000/00—14/b3675017.htm]

"Kozmo Delivers 'Consumer Racism?', MSNBC, April 12
[http://www.zdnet.com/zdnn/stories/news/0,4586,2534749,00.html]

Attachments

1. In the Matter of Doubleclick,, Complaint and Request for injunction, Request for Investigation and Other Relief, Electronic Privacy Information Center (EPIC), before the Federal Trade Commission, February 10, 2000 [http://www.epic.org/privacy/internet/ftc/DCLK—complaint.pdf]
2. "Privacy on the Internet," *New York Times,* February 22, 2000 (editorial)

Attachment 1

Before the

Federal Trade Commission
Washington, DC 20580

In the Matter of	)
	)
DoubleClick Inc.	)
	)

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

INTRODUCTION

1. This complaint concerns the information collection practices of DoubleClick Inc. and its business partners. As is set forth in detail below, DoubleClick Inc. has engaged, and is engaging, in unfair and deceptive trade practices by tracking the online activities of Internet users and combining that tracking data with detailed personally-identifiable information contained in a massive, national marketing database. DoubleClick Inc. engages in these activities without the knowledge or consent of the affected consumers, and in contravention of public assurances that the information it collects on the Internet would remain anonymous. The public interest requires the Commission to investigate these practices and to enjoin DoubleClick Inc. from violating the Federal Trade Commission Act, as alleged herein.

PARTIES

2. The Electronic Privacy Information Center ("EPIC") is a public interest research organization in Washington, DC. EPIC is a project of the Fund for Constitutional Government ("FCG"). FCG is a non-profit charitable organization established in 1974 to protect civil liberties and constitutional rights. EPIC's activities include the review of governmental and private sector policies and practices to determine their possible impacts on individual privacy interests. Among its other activities, EPIC has prepared reports and presented Congressional and administrative agency testimony on Internet and privacy issues.

3. DoubleClick Inc. ("DoubleClick") was organized as a Delaware corporation on January 23, 1996. DoubleClick's principal offices are located at 41 Madison Avenue, 32nd Floor, New York, New York 10010. At all times material to this complaint, DoubleClick's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

4. DoubleClick's business partners include more than 1,000 companies that have agreed to display DoubleClick advertising on the Web sites they operate and to enable the placement of "cookies" on the computers of Internet users who visit their Web sites. At all times material to this complaint, such companies' course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

THE IMPORTANCE OF PRIVACY PROTECTION

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

6. U.S. privacy law has by tradition protected the privacy of consumers in the offering of new commercial services enabled by new technologies. For example, the Cable Act of 1984 protects the privacy of cable subscriber records created in connection with interactive television services. The Electronic Communications Privacy Act of 1986 protects the privacy of electronic mail transmitted over the Internet. The Video Privacy Protection Act of 1988 protects the privacy of rental records for video recordings of commercial programs made available to the public for home viewing.

7. Many Americans are today "concerned" or "very concerned" about the loss of privacy, particularly with regard to commercial transactions that take place over the Internet. One recent poll has indicated that the "loss of personal privacy" is the number one concern facing the United States in the twenty-first century.

8. The Federal Trade Commission today plays a critical role in protecting consumer privacy, particularly with respect to the offering of commercial services over the Internet, and the resulting collection and use of personal information.

STATEMENT OF FACTS

DoubleClick's Tracking of Online Activities

9. DoubleClick is a leading provider of Internet-based advertising. The company places advertising messages on Web sites that are part of the "DoubleClick Network," which consists of highly-trafficked Web sites grouped together by DoubleClick in defined categories of interest. Participating sites include AltaVista, The Dilbert Zone, Macromedia, U.S. News Online, PBS Online, Multex Investor Network, Travelocity and Major League Baseball.

10. DoubleClick tracks the individual Internet users who receive ads at Web sites in the DoubleClick Network. When a user is first "served" an ad, DoubleClick assigns the user a unique number and records that number in the "cookie" file of the user's computer. When the user subsequently visits a Web site on which DoubleClick serves ads, DoubleClick reads and records that unique number. DoubleClick has acknowledged that "Web sites usually place certain information ('cookies') on a user's hard drive usually without the user's knowledge or consent." [1]

11. Using the unique numbers contained in cookies, DoubleClick's "DART" technology enables advertisers to target and deliver ads to Web users based on pre-selected criteria. As a user visits Web sites that utilize DoubleClick's technology, DART collects information regarding the user and his or her viewing activities and ad responses. According to DoubleClick, "[t]he sophisticated tracking and reporting functionality incorporated into DART provides advertisers with accurate measurements of ad performance based on selected criteria." [2] In early 1999, the company described the technology as follows:

> DART's dynamic matching, targeting and delivery functions enable Web advertisers to target their advertising based on a variety of factors, including user interests, time of day, day of week, organization name and size, domain type (i.e., commercial, government, education, network), operating system, server type and version, and keywords. In addition, DoubleClick offers the ability to match geographic location of the user's server and organization revenue, if known, through third-party databases. . . . Further, in order to deliver the advertisements on the pages that are likely to result in the best response, DART improves its predictive capabilities by continuously collecting anonymous information regarding the user's viewing activities and ad responses.

Among other capabilities, DART technology allows advertisers "to track a user to the advertiser's own Web site to determine what actions a user takes following a clickthrough."

12. Through the use of cookies and DART technology, DoubleClick's collection of consumer information is extensive. In December 1998, the company received over 5.3 billion requests for the delivery of ads generated by approximately 6,400 Web sites. DoubleClick estimates that more than 48 million users worldwide visited Web sites within the DoubleClick Network during December 1998. According to Media Metrix, 45.8% of Internet users in the United States visited Web sites within the DoubleClick Network during the same month. During the fourth quarter of 1998, DoubleClick placed approximately 18,000 Internet advertisements for over 2,300 advertisers. In calendar year 1998, DoubleClick's DART technology delivered approximately 34 billion advertising impressions worldwide.

13. DoubleClick reportedly has compiled approximately 100 million Internet user profiles to date.

---

[1] DoubleClick Inc. Form 10–K/A (Amendment No. 2) for Calendar Year Ended December 31, 1998.

[2] *Id.*

DoubleClick's Prior Assurances of Anonymity

14. DoubleClick has publicly represented that any information it collected about Internet users and their online activities was, and would remain, anonymous. Thus, the "Privacy Policy" displayed at the DoubleClick Web site in 1997 (attached hereto as Exhibit A) provided:

> DoubleClick does not know the name, e-mail address, phone number, or home address of anybody who visits a site in the DoubleClick Network. All users who receive an ad targeted by DoubleClick's technology remain completely anonymous. Since we do not have any information concerning names or addresses, we do not sell or rent any such information to third parties. Because of our efforts to keep users anonymous, the information DoubleClick has is useful only across the DoubleClick Network, and only in the context of ad selection.

The "Privacy Policy" displayed at the DoubleClick Web site in 1997 did not state that it was "subject to change," or otherwise indicate that the assurance of anonymity was in any way conditional.[3]

Likewise, the "Privacy Policy" displayed at the DoubleClick Web site in 1998 (attached hereto as Exhibit B), when the company served some 34 billion advertising impressions, provided:

> All users who receive an ad targeted by DoubleClick's technology remain completely anonymous. We do not sell or rent any information to third parties. Because of our efforts to keep users anonymous, the information DoubleClick has is useful only across sites using the DoubleClick technology and only in the context of ad selection.

The "Privacy Policy" displayed at the DoubleClick Web site in 1998 did not state that it was "subject to change," or otherwise indicate that the assurance of anonymity was in any way conditional.

15. DoubleClick's business partners have similarly represented that DoubleClick cookies generated at their Web sites were anonymous and that no personally-identifiable information would be collected by DoubleClick or its business partners as a result of the placement of DoubleClick cookies.

DoubleClick's Acquisition of Ababus Direct

16. On June 13, 1999, DoubleClick entered into an agreement to acquire Abacus Direct Corporation ("Abacus"), a leading provider of specialized consumer information and analysis for the direct marketing industry.

17. Abacus created and directs the Abacus Alliance, a cooperative arrangement through which more than 1,050 direct marketers contribute their customers' purchasing histories to Abacus for inclusion in a comprehensive database. As of December 31, 1998, the Abacus database contained over 88 million detailed buyer profiles compiled from records of over 2 billion catalog purchasing transactions. Abacus claims that the Abacus Alliance members include over 75% of the largest consumer merchandise catalogs in the United States. The database is continually enhanced as members contribute current sales transaction information and as additional companies join the Abacus Alliance.

18. Since at least as early as 1998, the Abacus database has contained information identifying and tracking the activities of Internet users. On November 2, 1998, Abacus formed a strategic alliance with Catalog City, Inc., an on-line catalog Web site offering on-line shopping services to catalog shoppers, to jointly promote each others services and share certain "e-commerce data." That information includes consumer e-mail addresses and phone numbers, online transactions and "click data."

DoubleClick's Intention to Combine "Personally-Identifiable Information" and "Non-Personally-Identifiable Information"

19. Subsequent to entering into the agreement to acquire Abacus, DoubleClick began to distance itself from its earlier assurances that users would "remain completely anonymous." A revised "Privacy Policy" posted on the DoubleClick Web site in or around June 1999 (attached hereto as Exhibit C) stated:

[3] The attached print-outs of material displayed at the DoubleClick Web site in previous years were obtained from cached copies of Web pages that EPIC accessed through the Google search engine at http://www.google.com/

> 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 e-mail address. DoubleClick does, however, collect certain non-personally-identifiable information about you, such as the server your computer is logged onto or your browser type (for example, Netscape or Internet Explorer). The information collected by DoubleClick is used for the purpose of targeting ads and measuring ad effectiveness on behalf of DoubleClick's advertisers and Web publishers who specifically request it. . . .
>
> In addition, in connection solely with the delivery of ads via DoubleClick technology to one particular Web publisher's Web site, DoubleClick combines the non-personally-identifiable data collected by DoubleClick from a user's computer with the log-in name and demographic data about users collected by the Web publisher and furnished to DoubleClick for the purpose of ad targeting.
>
> There are some cases when a user voluntarily provides personal information in response to an ad (a survey or purchase form, for example). In these situations, DoubleClick (or a third party engaged by DoubleClick) collects the information on behalf of the advertiser and/or Web site. This information is used by the advertiser and/or Web site so that you can receive the goods, services or information that you requested. Where indicated in some requests, DoubleClick may use this information in aggregate form to get a more precise profile of the type of individuals viewing ads or visiting the Web sites.

20. Under the heading of "Future Plans," DoubleClick stated as follows in its revised "Privacy Policy" posted on the DoubleClick Web site in or around June 1999:

> On June 14, 1999, DoubleClick and Abacus Direct Corporation announced their plan to merge in the third quarter of 1999. Abacus currently maintains a database consisting of personally-identifiable information used primarily for off-line direct marketing. DoubleClick has no rights or plans to use Abacus' database information prior to the completion of the merger. Upon completion of the merger, should DoubleClick ever match the non-personally-identifiable information collected by DoubleClick with Abacus' database information, DoubleClick will revise this Privacy Statement to accurately reflect its modified data collection and data use policies and ensure that you have adequate notice of any changes and a choice to participate.

There is no indication that DoubleClick's business partners, who operate the Web sites at which Internet users convey personally-identifying cookies to DoubleClick, made similar revisions to the privacy statements posted at their Web sites.

21. On November 23, 1999, DoubleClick completed its acquisition of Abacus. For the first time, DoubleClick stated that "personally-identifiable information" (including "the user's name, address, retail, catalog and online purchase history, and demographic data") would be combined with "non-personally-identifiable information collected by DoubleClick from Web sites on the DoubleClick Network." Specifically, a revised "Privacy Policy" currently (as of February 9, 2000) posted on the DoubleClick Web site (attached hereto as Exhibit D) states as follows:

> On November 23, 1999, DoubleClick Inc. completed its merger with Abacus Direct Corporation. Abacus, now a division of DoubleClick, will continue to operate Abacus Direct, the direct mail element of the Abacus Alliance. In addition, Abacus has begun building Abacus Online, the Internet element of the Abacus Alliance.
>
> The Abacus Online portion of the Abacus Alliance will enable U.S. consumers on the Internet to receive advertising messages tailored to their individual interests. As with all DoubleClick products and services, Abacus Online is fully committed to offering online consumers notice about the collection and use of personal information about them, and the choice not to participate. Abacus Online will maintain a database consisting of personally-identifiable information about those Internet users who have received notice that their personal information will be used for online marketing purposes and associated with information about them available from other sources, and who have been offered the choice not to receive these tailored messages. The notice and opportunity to choose will appear on those Web sites that contribute user information to the Abacus Alliance, usually when the user is given the opportunity to provide personally identifiable information (e.g., on a user registration page, or on an order form).

> Abacus, on behalf of Internet retailers and advertisers, will use statistical modeling techniques to identify those online consumers in the Abacus Online database who would most likely be interested in a particular product or service. All advertising messages delivered to online consumers identified by Abacus Online will be delivered by DoubleClick's patented DART technology.
>
> Strict efforts will be made to ensure that all information in the Abacus Online database is collected in a manner that gives users clear notice and choice. Personally-identifiable information in the Abacus Online database will not be sold or disclosed to any merchant, advertiser or Web publisher.
>
> Name and address information volunteered by a user on an Abacus Alliance Web site is associated by Abacus through the use of a match code and the DoubleClick cookie with other information about that individual. Information in the Abacus Online database includes the user's name, address, retail, catalog and online purchase history, and demographic data. The database also includes the user's non-personally-identifiable information collected by Web sites and other businesses with which DoubleClick does business. Unless specifically disclosed to the contrary in a Web site's privacy policy, most non-personally-identifiable information collected by DoubleClick from Web sites on the DoubleClick Network is included in the Abacus Online database. However, the Abacus Online database will not associate any personally-identifiable medical, financial, or sexual preference information with an individual. Neither will it associate information from children.

The Inadequacy of DoubleClick's "Opt-Out" Procedure

22. The most recent version of DoubleClick's "Privacy Policy" purports to offer users the ability to "opt-out" of the information sharing activities described above. It states, in pertinent part:

> While some third parties offer programs to manually delete your cookies, DoubleClick goes one step further by offering you a "blank" or "opt-out cookie" to prevent any data from being associated with your browser or you individually. If you do not want the benefits of cookies, there is a simple procedure that allows you to deny or accept this feature. By denying DoubleClick's cookies, ads delivered to you by DoubleClick can only be targeted based on the non-personally-identifiable information that is available from the Internet environment, including information about your browser type and Internet service provider. By denying the DoubleClick cookie, we are unable to recognize your browser from one visit to the next, and you may therefore notice that you receive the same ad multiple times.

23. The vast majority of Internet users who receive cookies from DoubleClick never visit the DoubleClick Web site and therefore never learn of the "opt-out" procedures described by the company. DoubleClick cookies are placed on users' computers when users visit third-party Web sites that display ads placed by DoubleClick. Users are rarely given notice by such third-party Web sites that they need to visit the DoubleClick Web site in order to understand DoubleClick's data collection activities or learn about any available "opt-out" procedures.

24. A large percentage of DoubleClick cookies are placed on the computers of users who visit the AltaVista Web site. Approximately 18.7% of DoubleClick's revenues for the nine months ended September 30, 1999, resulted from advertisements delivered on or through the AltaVista Web site. Approximately 41.2% of DoubleClick's systems revenues for the nine months ended September 30, 1999, resulted from AltaVista billings.[4]

25. Visitors to the AltaVista Web site are not provided notice that their use of the AltaVista site will result in the placement of DoubleClick cookies on their computers. The AltaVista "Privacy Policy" displayed on February 9, 2000 (attached hereto as Exhibit E) provides, in pertinent part:

> AltaVista uses one or more third party companies to serve advertisements at our site. These companies may use cookies to ensure that you do not see the same advertisements too often, but they also may collect information about you when you view or click an advertisement at our site. Cookies that are received with advertisements are read and placed by one of our advertising companies,

[4] DoubleClick Inc. Form 10–Q for the Quarterly Period Ended September 30, 1999

> and AltaVista does not have access to them, nor can we control how they are used.

The AltaVista "Privacy Policy" does not contain any reference to DoubleClick.

Inaccurate Information Posted by DoubleClick's Partners

26. Some third-party Web sites that generate DoubleClick cookies do inform users of their relationship with DoubleClick and that DoubleClick places cookies on the computers of users who visit such third-party sites. Some of those Web sites continue to assure users that they will remain anonymous. For instance, the "Privacy Stuff" page at the Dilbert TV Web site (attached hereto as Exhibit F) displayed the following information on February 9, 2000:

> United Media contracts with DoubleClick to sell and manage the advertisements that you see on this site. The advertisements help us bring you the United Media site without charge. DoubleClick uses "cookies" to improve the quality of your visit to the Dilbert TV Web site. . . .
>
> DoubleClick uses cookies to make sure that you do not see the same advertisements repeatedly and when possible, shows advertising that is relevant to you based on what you have seen previously. Cookies are anonymous. DoubleClick does not know the name, e-mail address, phone number, or home address of anybody who visits the United Media site or any other site in the DoubleClick Network. All users receiving an ad from DoubleClick through the United Media site therefore remain entirely anonymous to DoubleClick; DoubleClick does not have any information to sell or rent to other parties.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

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

DoubleClick's Activities Constitute Deceptive Trade Practices

28. DoubleClick has publicly represented that any information it collected about Internet users and their online activities was, and would remain, anonymous.

29. In truth and in fact, DoubleClick intends to combine data it has consistently described as "non-personally-identifiable information" with users' names, addresses, retail, catalog and online purchase histories, and other personally-identifiable information contained in the Abacus database. Therefore, DoubleClick's representations concerning the anonymity of information it collected and collects about Internet users were, and are, deceptive practices.

DoubleClick's Activities Constitute Unfair Trade Practices

30. DoubleClick's collection of information about Internet users, through the placement of cookies on users' computers and the linkage of cookie-generated data with information contained in the Abacus database, is performed without the knowledge or consent of the great majority of Internet users who receive DoubleClick cookies. Users who receive DoubleClick cookies on their computers do not knowingly access the DoubleClick Web site. Many of DoubleClick's partners, who operate the Web sites which generate DoubleClick cookies, provide either no information or inaccurate information about the placement of such cookies and the manner in which data about users will be collected or used. As a result, the great majority of users who receive DoubleClick cookies neither know that their activities are being monitored, nor are aware of any "opt-out" procedures that might be available.

31. DoubleClick's collection of information about Internet users, through the placement of cookies on users' computers and the linkage of cookie-generated data with information contained in the Abacus database, without the knowledge or consent of Internet users, is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition, and therefore is an unfair practice.

32. DoubleClick has publicly represented that any information it collected about Internet users and their online activities was, and would remain, anonymous.

33. DoubleClick's plan to combine "non-personally-identifiable information" with users' names, addresses, retail, catalog and online purchase histories, and other personally-identifiable information contained in the Abacus database, in violation of its representations to the contrary, is likely to cause substantial injury to consumers

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

Consumer Injury

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

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

36. Absent injunctive relief by the Commission in this matter, other companies will be encouraged to collect personally-identifiable information from consumers in an unfair and deceptive manner.

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

REQUEST FOR RELIEF

WHEREFORE, EPIC requests that the Commission:

A. Initiate an investigation into the information collection and advertising practices of DoubleClick and the Web sites on which DoubleClick places advertisements and/or generates cookies on the computers of Internet users;

B. Order DoubleClick to destroy all records it created concerning Internet users during any period of time in which DoubleClick or any of its business partners were assuring the anonymity of the information DoubleClick collected;

C. Order DoubleClick to obtain the express consent of any Internet user about whom DoubleClick intends to create a personally-identifiable record, and to develop such means as are necessary to ensure that the user has access to the complete contents of the record;

D. Order DoubleClick to pay a civil penalty equal to fifty percent (50%) of the revenues it obtained as a result of the practices described herein, or such other civil penalty as may be appropriate;

E. Permanently enjoin DoubleClick from violating the FTC Act, as alleged herein; and

F. Provide such other relief as the Commission finds necessary to redress injury to consumers resulting from DoubleClick's violations of the FTC Act.

Respectfully Submitted,

Marc Rotenberg Executive Director	David L. Sobel General Counsel

---

Attachment 2

Privacy on the Internet

February 22, 2000, *New York Times*

As the Internet matures, preserving user privacy and anonymity is becoming a significant problem. Technology now makes it possible for online businesses and advertisers to turn the Internet into a realm where activities and habits are monitored and recorded, largely without consumer knowledge or consent. Unless businesses can protect privacy, the erosion of trust could seriously harm e-commerce as well as cause the public to become wary about using the Internet for education, research and other important non-commercial functions.

In the offline world, a big part of personal privacy is simply the freedom to remain a face in the crowd. No one tracks a shopper as he visits various stores in a mall or keeps notes on what products he looks at. But in cyberspace, that shopper's be-

havior—which Web sites he visits, and which ads he clicks on—can all be instantly recorded and compiled, albeit through computer-based identifiers rather than by name. Most consumers have little idea that unseen advertising networks on the Internet track their movements across multiple Web sites. Most do not know that Web sites can collect and sell data about them. But consumer concerns are rising, and businesses are getting worried about a privacy backlash.

This month the Electronic Privacy Information Center, an advocacy group, filed a complaint against DoubleClick with the Federal Trade Commission, alleging unfair trade practices in its tracking of the online activities of millions of Internet users. DoubleClick, the leading Internet advertising company, places ads for its clients on about 1,500 Web sites—including many of the most heavily used sites such as AltaVista—that are part of the DoubleClick network. When a computer user views an ad on a network site, DoubleClick places a "cookie" file on the user's computer hard drive that carries a special identifying number. The cookie allows DoubleClick to monitor the user's computer—though without being able to identify the user by name or address—whenever he visits a network site, and note the content he is viewing to deliver a targeted ad that is customized to a user's interests.

Last year DoubleClick acquired Abacus Direct, a company that has a database of millions of names, addresses and other personal information collected by the nation's largest direct-mail catalogues. Now DoubleClick is building an online version of Abacus, and will be able to match personally identifiable information on purchasers collected by the online Abacus with DoubleClick's data on those individuals' subsequent Web activities.

DoubleClick says it will give users the opportunity to opt out of this matching. But privacy advocates fear that this kind of data collection will become widespread in cyberspace, and that personal information—from browsing habits to the research one might do on the Web—could potentially be released to employers, insurers and others. Industry's answer to these worries is self-regulation and the creation of privacy policies. Unfortunately, even good policies are largely unenforceable. A new study by the California HealthCare Foundation of 21 major health-related Web sites found that many violated their own stated privacy policies, and shared personal information collected from visitors without their permission.

One solution is to give users easier ways to block the collection of information. DoubleClick, responding to public criticism, has begun a campaign to tell users how to opt out of tracking. The World Wide Web Consortium, the group that designs standards for the Web, is creating a new way for Web sites to transmit the site's privacy policy automatically, and allow users to signal only the information they are willing to share.

Also, several Internet privacy bills have been introduced in Congress. Businesses are concerned that government regulations could hinder the Internet's dynamism. Many users may want to receive ads aimed at their interests. But all users should get a meaningful choice about how personal data are collected and used. Maintaining privacy will be integral to the Internet's future, if only because consumers need to feel safe enough to participate.

The CHAIRMAN. Thank you very much.

Mr. Smith, welcome.

STATEMENT OF RICHARD SMITH, INTERNET CONSULTANT

Mr. SMITH. Thank you for the invitation here to speak today before this Committee. My background is technical. I have been in the computer business for approximately 30 years and have also run my own businesses for about the last 20 years.

Since September of this past year, I have taken a sabbatical and begun looking at the issues of Internet privacy and security. What I would like to do today is talk a little bit and expand upon the excellent presentation that was made by Jodie of the FTC here of some of the technology that is going on behind the scenes here.

In my written testimony, I have—I want to start off here with exhibit A here, as I call it, which illustrates one of the issues of how ad targeting is done today. This is from the AltaVista search engine. If you have used the search engine, you probably noticed after a while that the banner ads that you see at the search engine

are related to what you are searching for. This is not an accident, because companies can purchase keywords and whatever keyword you type in you get a relevant ad. So for example, here I have typed in "sports cars" and I get a Toyota ad. I type in "vacation homes" and I get an ad for move.com.

This practice has been going on for 3 or 4 years and is really, I would say, not necessarily a privacy-unfriendly technology. But we get down into some other interesting issues here. I found this one accidentally. I typed in "growing pot" and I got an anti-drug ad. This actually comes from the White House, so even the government is involved in buying these keywords.

We are doing some medical conditions here. I typed in "AIDS" and get a pitch for an anti–HIV drug. "Compulsive gambling," I get a banner ad for an online casino. I think that is a little mess-up there.

Given the political nature of this today, I thought I would also try "Al Gore" and "George Bush" here. It looked like they are owned—pardon me—the keywords are owned by women.com.

The idea here is that this illustrates sort of the birth of online profiling, is that the Internet ad companies noticed that you could begin discerning a lot about people by how they search. This is, as Daniel has talked about, one of the ways that information is put into our profiles, by watching everything we search for. As a matter of fact, at the AltaVista search engine, Engage today is using this kind of information.

I want to go on to the topic of web bugs because that came up a little bit earlier. It is a technology. Basically the idea is you have a web page and you put an invisible image on the page, if you are a network advertiser or a marketing company, to monitor who comes to web pages. They act like banner ads in the sense that they provide back the same information, but they obviously, they are totally hidden. They are only one by one pixel in size.

The problem that I have with them is I think they have very much undermined the trust in the Internet because they are very much a tracking device. Some sites that have web bugs on them today are I think we would all agree very sensitive in nature. For example, Procrit, it is a drug from Johnson and Johnson, has approximately five web bugs on the website from DoubleClick. The home page is one of the pages bugged, as well as each of the conditions, the page on AIDS, the page on kidney diseases, and the page on cancer.

So we can see in this case here that DoubleClick has been hired to do monitoring of users at that site. So I am kind of interested about this idea that network advertisers do not get into monitoring sensitive issues.

Another technology, or it is not really a technology, but a problem that we have with network advertisers, is that of what I term as data spills. The idea behind a data spill is that if you type in data on a web form and it goes into the website—for example, an example I found was at Intuit you would type in information about your financial information to see if you could get a mortgage. That information was accidentally leaked off to DoubleClick through the use of banner ads.

This is a bug, this is a problem or a mistake that the Intuit website made, but that does illustrate that this data that is being sent in to the ad networks sometimes is very personal in nature. In a two-month period, for example, I found approximately ten data leaks to DoubleClick—things like my name, address, and e-mail address.

Another issue that I would like to get into real quickly here is the issue of notice. The industry talks about one of the things that we need here is notice and the idea that websites would link to the privacy policies of network advertisers so they could learn about the online profiling. Well, over the weekend I did a quick check here with the AltaVista search engine and found, for example, with the case of DoubleClick, although they have 12,000 websites that they provide banner ads to, only about 130 of those sites had links to their privacy policy. So if you wanted to opt out at DoubleClick, there are very little ways to understand about that.

The same thing was true with Engage and its family of companies. AltaVista shows less than a hundred links to their privacy policies.

Finally, I would like to end up my testimony with just a quick remark to give folks an idea how different the Internet is than any other media in terms of tracking. On my computer I monitor all traffic that goes in and out of the computer on the Internet. Over the past 6 months I have had 250,000 transactions, that is web pages and images and java script applets that have been downloaded. Of those, 27,000 URL's went back to DoubleClick. So they got back 27,000 URL's of web pages that I was at.

So we are dealing with a very different medium than anything else in the offline world. For example, my credit card company, my bank, and my telephone company do not know about anywhere—do not get that amount of information about me each and every day. That works out to about 150 transactions a day.

Thank you very much.

[The prepared statement of Mr. Smith follows:]

PREPARED STATEMENT OF RICHARD SMITH, INTERNET CONSULTANT

Introduction

To begin with, I would like to first thank the Chairman and the Senate Committee on Commerce, Science, and Transportation for this opportunity to testify today on the issue of online profiling and its impact on consumer privacy. It is indeed an honor to be here.

My own background is that I have spent almost 30 years in the computer software business both as a software engineer as well as a business owner. I retired last September as the President of Phar Lap Software, Inc., a company I co-founded 14 years ago. Since leaving Phar Lap, I have worked as a consultant specializing in Internet security and privacy issues.

The issue of online profiling is very controversial. The reason is quite simple to understand. Most consumers are very bothered by the fact that companies are monitoring their Web surfing habits. In addition, consumers are almost never informed about these monitoring activities and have never been asked if it is okay. To many people who learn about online profiling for the first time, their first impression is that it is something right out of Orwell's *1984*.

In my testimony today, I will be focusing on two major areas. To begin with, I will talk about how data is collected by Internet ad companies for use in online profiles. To date, I do not think that ad companies have been totally straight with consumers with their data collection practices. The second area I want to talk about today is the lack of proper notice to consumers about online profiling. I will be using real-life examples of some of things that I have seen in my own use of the Internet.

Along the way, I want to also suggest an alternative to online profiling which is content-based targeting for banner ads. Content-based targeting is typically employed in the off-line world (newspapers, TV, and magazines). It is much more privacy friendly than online profiling because it requires no tracking of individual users as they surf the Internet. The most banner ads shown today are already using content-based targeting because it is easy to understand and favored by advertisers.

How Data Is Collected For Online Profiles

To begin the discussion of data collection practices of Internet ad companies, the best place to start looking is at Internet search engine sites. Everyone seems to have their own favorite search engine and mine happens to be AltaVista. It also turns out that the AltaVista site has business relationships with DoubleClick and Engage who both are also testifying here today.

Most people probably have noticed at one time or another that the banner ads that they see on a search results page are related to what they are searching for. This is no accident. AltaVista employs DoubleClick to show banner ads at the site. One of the services that DoubleClick provides for advertisers is the ability to "purchase" keywords at the site. When a company owns a particular keyword or phrase, their banner ads will appear of the search results page for the keyword or phrase. Keywords are typically purchased on a month-by-month basis. They can be purchased either on an exclusive basis or can be shared with other companies.

Exhibit A illustrates how some common keywords such as "sports cars" and "vacation homes" will show relevant banner ads at AltaVista. A version of Exhibit A is also available at my Web site that shows in real-time what banner ads are being shown for common keywords. This demonstration is available at:

http://www.tiac.net/users/smiths/commerce/avads.htm

Advertisers like keyword targeted ads because it is more likely that people seeing their ads will be interested in their products. DoubleClick and AltaVista also like keyword targeted ads because they can charge a premium for them. This premium is typically 2 to 3 times more than standard ads at AltaVista.

But what about the consumer? How do they feel about keyword-targeted ads? The answers are a bit more difficult to come by. When many consumers notice keyword-targeted ads for the first time they get a bit uncomfortable. They realize that someone is watching them as they search the Internet with AltaVista. Most folks do not like to be watched and one of the first association that comes to mind is 1984. On the other hand, I think most people will agree that if they are going to see banner ads at Web sites, they might as well be relevant to their interests.

AltaVista did not help matters much, because until January of this year, they did not disclose to users that banner ads can be targeted to search phrases. They also have made mixed efforts in informing users about their relationship with DoubleClick. However, a savvy Web user today who reads the AltaVista privacy policy will learn both about keyword-targeted ads and DoubleClick.

So do keyword-targeted ads present a privacy problem for users? I personally do not think so. In the Yellows Pages, we see ads for car dealerships in the automobile section. The same is true with the search results page for "cars" at AltaVista. I believe that this type of content-based targeting is valuable to both advertisers and consumers. It is an example of good Internet marketing.

However, there still are the concerns of consumers that they are being watched when they see keyword-targeted ads. How can these concerns be addressed? The first part of the solution is to provide adequate notice to consumers about the practice. For example, some of the search engine companies are now disclosing this practice in their privacy policies. The real answer for consumers is to make it clear that that their search strings are never saved in a database. Except for keeping aggregate statistics on the popularity of keywords, people's search strings should be discarded. More about this issue shortly.

But how does DoubleClick know what ad to display for a search keyword in the first place? Very simply, AltaVista gives DoubleClick, everyone's search strings. The hand-off is done right on the search results page. A banner ad is displayed as a image, and the URL of image is specially constructed by AltaVista to include the search string. Here is what one of these banner ad image tags looks like for the search string "sports cars":

```
<IMG SRC="http://ad.doubleclick.net/ad/altavista.digital.com
/result—front;kw=sports+cars;cat=totext;ord=1804224227?"
border=0 height=60 width=468>
```

You will notice that the search string is embedded as the "kw" parameter in the image URL.

So DoubleClick is being sent everyone's search strings at AltaVista. Pretty obviously you can learn a lot about a person by observing what they are searching for on the Internet. The ad network companies have realized this also and invented the idea of online profiling. The basic concept is for the ad server computers of the ad companies to track over time what an individual is searching for and to provide relevant ads to according to their search history. These personalized banner ads can be shown whenever someone searches for a keyword that has not been purchased by an advertiser. These same personalized ads can also be shown at other Web sites in the same ad network.

However it is pretty cumbersome for an ad network to remember every little search string that someone has used. Such a list does not lend itself to quickly selecting an ad for a user. In general, an ad server must decide on what ad a user sees in about 1/100 of a second. So in order to meet this time constraint, Internet ad companies instead build profiles of people. A profile is a table that rates a person on their level of interest in particular subjects. A profile might contain up to a thousand different subjects areas. These subjects areas might include things like sports (golf, tennis, football, etc.), travel (US, Canada, Europe, etc.) and food (cooking, gardening, etc.). A person is then scored for each of these subject areas. A score is a percentage. Zero percentage meaning no interesting, while one hundred percentage means extremely interested. These scores are updated in real-time from search strings and other data.

Advertisers can then target groups of users by instructing an Internet ad network to show their ads to people who have certain characteristics in their profiles. For example, a ski resort may want to have their ads to be shown only to people who appear by their profiles to have a strong interest in skiing. The targeting might also be indirect. A car company might target ads for their luxury models at people who show an interest in European travel, while their middle-of-the-road models might be pitched to people who show an interest in American travel.

An online profile is created for a user the first time they are shown a banner ad from a particular Internet ad network. All of the scores in the profile are set to zero. The profile is stored at the ad server computers. It is updated in real-time according to the following information that is received by Internet ad networks:

- What search strings an individual searches for
- What Web pages an individual visits
- What banner ads an individual clicks on

A user can be tracked by an Internet ad company on any Web page that a banner ad appears that is served by the company.

In addition to their profile, a user is also assigned a unique customer ID number. This ID number is stored with the profile to identify who the profile belongs to. The ID number is also sent back to the user's computer as a cookie and stored on the hard drive of the computer. Then as the user surfs the Web and is shown more banner ads, this customer ID number is sent back to the Internet ad network with each and every request for a banner ad. The cookie is the mechanism that allows Internet ad networks to track people over time.

Cookies are anonymous in the sense that they do not say who a person is. However, personal information can be associated with a cookie and stored with a profile if a user provides this information to an Internet ad company. This is typically done using some sort of online contest or sweepstake where users are required to provide their names, addresses, and phone numbers. As an example, DoubleClick operates a Web site called NetDeals (http://www.netdeals.com) for this purpose.

In addition, using a technique called "cookie synchronization", it is possible for one Web site to provide an Internet ad network with personal and demographic data about users. Again this information can be associated with a cookie and stored in an online profile. Excite@Home is apparently using this technique to provide registration data to its sister company, MatchLogic, an Internet ad company.

On paper, the economic benefits of online profiling seem self-evident. In theory, a profiled banner ad should have an increased response rate because it is being better targeted. Advertisers can purchase a smaller number of ad impressions in order to get the same results. Ad networks can charge more money per ad impression because the higher perceived value. Consumers are suppose to benefit because they will see less ads about products that they no interest in.

However in practice, the value of online profiling is yet to be proven. The industry has not released any studies that show response rates are significantly higher for profiled ads. In addition, the response rates need to go up more than the costs of profiling. These costs include the premium paid for ads themselves plus the time it takes to figure out what profile works best for a particular ad. This second point

is very important. It is unclear if advertisers can use all of the data that Internet ad companies can provide them. This point was made recently in a *New York Times* article by Saul Hansell:

> **"So Far, Big Brother Isn't Big Business"**
> http://www.nytimes.com/library/financial/personal/050700personal-privacy.html
> May 7, 2000
>
> "The few advertisers that have tried these systems have not yet given up on them. But most say the response to their ads does not go up enough to be worth the extra cost and bother. It seems easier for them to buy cheap shotguns, in effect, than expensive laser-guided rifles."

Regardless if online profiling systems make economic sense or not, from a privacy standpoint, they present some real dangers. These systems are monitoring people as they surf Internet. What data is being collected and what is being saved away is not made very clear. All of the uses of this data is not disclosed and may change over time. Also in spite of claims by Internet ad companies that the profiles are anonymous almost all of these companies maintain separate databases with personal data that can be combine with the anonymous profiles at anytime using cookie synchronization.

However the real danger that I see with online profiling is that Internet ad companies have set up extensive monitoring systems to provide data for profiling. It is almost like they have put hidden microphones in our homes and our offices and they listening to what we do all day long. Pretty obviously if you deploy hidden microphones, you are going to pick up information which is personal in nature. And this is exactly what I have found on my own computer. The data collection systems that the Internet ad companies are currently running are getting personal and sensitive information that almost everyone will agree is none of the business of these companies. The problem here is one of collateral damage

Data Spills

The first problem that I have seen at many Web sites is the problem of data spills. A data spill is where information that is typed into a form at a Web site is accidentally sent off to an Internet ad company. Data spills are caused by poor Web site design Because I do logging of my Internet traffic from my computer, I can detect data spills. In a two-month period, I found close to 10 data spills of personal data to DoubleClick. These data spills include things like my name, home address, Email address, and birth date. Web sites that were sending off this data to DoubleClick included well-known sites like AltaVista, Real Networks, HealthCentral, Quicken, and Travelocity.

My Web site includes a write-up that describes how data spills occur in the first place and how they can be prevented. The URL of the write-up is available at:

> http://www.tiac.net/users/smiths/privacy/banads.htm

In the write-up, I talk mostly about DoubleClick. They are going to be receiving the most information from data spills given that they are largest provider of banner ads. However, the problem can occur with any banner ad network and all companies are receiving this kind of personal data from Internet users. A recent example of data spill really illustrates the point. I found that on my computer the sign-up page for the contest Web site, Jackpot.com, gave away my Email address to three different companies all at the same time. The companies receiving my Email address were Flycast, YesMail, and Sabela. The Jackpot.com privacy policy states they never share personal data, but they seem to have a tough time keeping this promise. My enquiry to the company about the issue was answered with a denial that there was any problem. The customer support person simply repeated the claims of the privacy policy.

In general, Jackpot.com is the exception rather than the rule. Other Web sites have been more response and fixed the problems right away when I have brought them to their attention. In addition, in some discussions I have had with the Internet ad companies, they have made it clear that they do not want this of type of unsolicited personal information from users. However, from their perspective it is a problem they cannot directly solve because the issues are with the Web sites running the banner ads and not at the ad servers.

In the near term, I am hoping to see Internet ad companies publicly commit to not use this unsolicited personal data from data spills. The best place to do this I think is in their privacy policies. The idea here is to acknowledge the problem that Web sites may accidentally give away personal data, but the Internet ad networks will discard it and not make use it.

Over the long term, there is a simple technology solution to the problem that can be implemented by Web browser companies. This solution involves eliminating referring URLs for being sent in situations where a data spill is likely to occur. Referring URLs can contain the personal data in a data spill.

Web Bugs

Besides banner ads, Internet Ad companies also track users with something I've nicknamed "Web Bugs." A Web Bug is an invisible image on a Web page that sends back the cookie of an Internet ad company to their servers. The main purpose of a Web Bug is to track what pages users are going to the Internet. Given that images are invisible on the page, the averagel user has no way of knowing that they are being tracked in this manner. In addition, to my knowledge, no Web site or Internet ad company has every disclosed the use of Web Bugs in their privacy policies.

Pretty obviously, people in the Internet ad business do not call these invisible images "Web Bugs'. Instead they use names like "clear GIFs", "1-by-1 pixels", "tracker GIFs", and sensors. Since no one has come up with a consistent name for them, I will continue to use the term "Web Bugs".

Even though there has not been very much public discussion about Web Bugs, they seemed to be employed by most Internet marketing companies. In my discussions with these companies, I have been told that they are used for these purposes:

- The see who has come to a Web site after viewing a banner ad
- To transfer both personal and non-personal information from a Web site to an Internet ad company
- To provide data to an online profile
- To count ad impressions and page hits

More technical information on Web Bugs can be found at my Web site at this URL:

http://www.tiac.net/users/smiths/privacy/wbfaq.htm

In addition, I have set up search page that will locate Web pages that employ Web Bugs. The page operates by giving special search string to AltaVista that has located the hidden images. The URL of the search page is:

http://www.tiac.net/users/smiths/privacy/wbfind.htm

The page will locate Web Bugs that have been placed around the Internet from more than 20 different Internet marketing companies

Although Internet ad companies represent that they do not do profiling of sensitive areas such as children, medical, financial, and sexual issues, most of them will use Web Bugs on pages that deal with these areas. Here are a few illustrations of Web pages that employ Web bugs that I believe most people will find troubling:

- Kids Zone of Santa.com (http://www.santa.com/santa/kidszone/index.htm)
- Procrit.com (http://www.procrit.com)
- Rodale Press (http://www.sexamansguide.com/a/home/order.rhtml)
- Metropolitan Life (http://metlife.com/Salescareers/Apply/Docs/online__interview.html)

The Procrit Web site is the most interesting use of Web Bugs on the list. Procrit is product of Ortho Biotech which is a subsidiary of Johnson and Johnson. The drug is used to fight anemia in patients with a number of different conditions including AIDS, cancer, and kidney disease. Hidden image files from DoubleClick are strategically placed on the Procrit Web site in order to distinguish if someone is at the site because they are interested in treatments because of AIDS vs. cancer vs. kidney disease. Needless to say, I believe that most visitors to the Procrit site would be very surprised to learn they are being monitored in this way. However, unless someone understands HTML source code and knows where to look, they would never see the Web Bugs at the site.

Web Bugs appeared to be employed by all of the Internet ad companies. AltaVista has found more 30,000 placed by DoubleClick and about 1,000 placed by Engage. Be Free, another Internet marketing company, has more a half of a million according to AltaVista.

Personally I am surprised that Web Bugs are ever used. When discovered, they undermine people's trust in Web sites. Some sites I know have stopped using Web Bugs when they received enquires from the press and consumers about their presences on the sites. Two such sites were Nabisco Kids and the United States Air

Force. Web Bugs are also playing a role in a number of the privacy lawsuits that have been filed against Web site and Internet ad companies.

The problem that I see with Web Bugs is that supply information on the sly to Internet ad companies that can be used in personal profiles. Given that this tracking is being done with no notice or consent, I find use of Web Bugs very problematic.

Notice and Banner Ad Networks

I want to shift gears for a second and talk about the problem of notice with online profiling. Most consumers are unlikely to be aware that they are being tracked as they surf the Web. I suspect that most consumers would be surprised that their computers are sending back information to Internet ad companies about what articles and Web pages they are reading online. They would probably also be more even dismayed to learn that some of this information actually is being used for profiling purposes. Most consumers are in the frame of mind that Web is just like other media such as television or newspapers. Reading an article in a newspaper is obviously anonymous unless a person chooses to tell someone else about what they have read. However, reading the same article in the online world can be very different. Two or three different companies may know what article someone has read, how long the article took to read it, and where the person went on the Web when they were done.

Over the last 3 or 4 years, the industry has settle on the use of Web site privacy policies to inform consumers about what data is being collected by a Web site and what is done with the data. Today almost all popular Internet sites have privacy policies in places. In most areas these privacy policies do an acceptable job of inform a consumer what they can expect with information. One very notable exception is the use of online profiling at their sites.

In addition, all of the major Internet ad companies also have privacy policies that describe how banner ad networks work, what data is being collected by these networks, and the details of online profiling. Also, most of the Internet ad companies offer an "OPT-OUT" to allow consumers the ability to turn off tracking and profiling.

However, there is one major flaw with the privacy policies of Internet ad companies. Consumers have almost no way of ever seeing these privacy policies. The problem here is the Internet ad companies are hidden in the background at Web sites and consumers by and large do not know anything about the companies. Web sites, in the own privacy policies, have not helped the situation very much for consumer. Although a Web site privacy policy may talk some about the Internet ad company they use, Web sites almost never link to the privacy policy of ad networks. For example, the AltaVista search engine finds less than 150 links to DoubleClick's privacy policy. Yet, DoubleClick has more than 12,000 Web sites that they provide banner ads for. A similar situation exists for Engage, less than 100 links are found to the Engage privacy policy, yet Engage and its sister companies provide banner ads for more than 6,000 sites.

There clearly is a problem here of Internet ad companies providing proper notice about online profiling.

Conclusion

The bottom line for me on online profiling is that Internet ad companies are getting too much data about us. Their ad networks function as tracking systems the gather data about us from search strings, banners ads on Web pages we visit, data spills, and Web Bugs. Clearly the data collection systems of the Internet ad companies are gathering more information about us than is necessary to show banner ads.

I know that many people involved in regulation issues around Internet advertising support the concept of OPT-OUT from online profiling. At the present time, I feel extremely uncomfortable with OPT-OUT for the following reasons:

- It is nearly impossible for consumers to learn about how they can OPT-OUT to online profiling because of lack of almost any kind of reasonable notice about online profiling.
- Invisible Web Bugs can provide data to the online profiles and consumers have no method of knowing that they are being tracked.
- Data spills are providing personal data about users to Internet ad companies and the industry has taken no public steps to stop the problem
- Many of Internet ad companies have divisions or sister companies that maintain databases of personally identified data that can be combined with the anonymous profiles at any time.

I want to conclude my testimony with one quick statistic from my own travels around the Internet. As I mentioned earlier, I run software on computer that logs all of my transactions on the Internet. The last 6 months, I had about 250,000 Web transactions total. More than 10% of these transactions were with DoubleClick. This works out to about 150 transactions per day. This means that DoubeClick is receiving 150 URLs of Web pages I am visiting each and everyday. In the offline world, I cannot think of one company that it is getting this amount of data about me. Not my phone company, not my bank, and not my credit card company.

Thank you again for this opportunity to address the Senate Commerce Committee.

Exhibit A -- Relevant banner ads at AltaVista

AltaVista, like most Internet search engines, show banner ads on search results pages. Banner ads in many cases are related to the what is being searched for. Releaent banner ads are shown because advertisers can "purchase" individual keyword or phrases. When particular search string is typed in, the banner ad of the company that owns the phrase is displayed at the top of the search results page.

This table shows in real-time a list of sample search phrases and the banner ads that "own" them at AltaVista.

Search String	Banner ad
Sports Cars	You can see the river. You can smell the pines. You can just feel the mountain air. 2000 4Runner
Vacation Houses	move.com Secure a mortgage Find a dream home Use moving resources
Credit Cards	GE Select Platinum MasterCard Great Rate • No annual fee
Growing Pot	Marijuana after soccer practice.
AIDS	HIV If you're interested in HIV There's a smart way to reach HIV treatment goals... CLICK HERE
Alzheimers	Senior Housing Search - Find Retirement Communities, Assisted Living & Nursing Homes Choose A State Search SENIOR HOUSINGNET www.seniorhousing.net
Compulsive Gambling	YOU COULD BE
Al Gore	• Democrat • Republican Can you influence his vote? FIND OUT HOW COUPLES VOTE women.com
George Bush	• Democrat • Republican Can you influence his vote? FIND OUT HOW COUPLES VOTE women.com

The CHAIRMAN. Thank you very much, Mr. Smith.

Mr. Polonetsky, you know that we discussed DoubleClick's "permission" in order that one can opt out at the last hearing. Now you are going to simplify that, according to your testimony.

Mr. POLONETSKY. Yes, the proposed simplified policy that we have given to your staff, and we welcome your reaction, is a one-page clear, effective explanation of what the privacy policy is. I think that, in an effort to give all the possible information that

anybody might want, our earlier privacy policy was, as you pointed out, long and detailed and complex.

The CHAIRMAN. Why was it like that to start with?

Mr. POLONETSKY. I think we felt that we ought to give all the information that anybody would want in all the detail should anybody want to have all that detail. I think what we need to do is put a cover page that has the simple, basic information, with an opportunity to get more detail if you want to click on a link and get that information.

The CHAIRMAN. Well, I guess I will ask you and Mr. Jaye: According to Mr. Smith, the AltaVista search engine finds, as he said, less than 150 links to your privacy policy and yet you have 12,000 websites that you provide banner ads for. In your case, Mr. Jaye, less than 100 links were found to Engage's privacy policy, yet Engage and its sister companies provide banner ads for more than 6,000 sites.

What is your response to that, Mr. Jaye?

Mr. JAYE. Unfortunately, Mr. Smith and I have an e-mail dialog and I should have gotten back to him when he mentioned that to me, because unfortunately the search string that he used at AltaVista was not necessarily the right search string. We actually provide a deep link directly to our opt-out page from sites that link to us. So if he was searching for our privacy page it would not show up.

We have 3,000 sites, for example, in the Flycast network, which is a company we acquired earlier this year, and we have gone through a certification process as we have brought them online and we have all those sites compliant. We have actually kicked out sites that are not compliant. So I think that we just need to probably spend a little bit more time on going over a couple of the details there.

In some cases also, when we deal with a third party in our business we are working with networks and what happens is that the site discloses that they are working with Engage and the third party, but the link may actually be to a slightly different form of the web page to let them know, for example, this site is part of the Flycast network, which is working with Engage.

So I think that we can probably put that to rest, at least in our case.

The CHAIRMAN. Mr. Polonetsky.

Mr. POLONETSKY. If I can respond to that as well, Senator. In February, DoubleClick announced that every new contract that we signed with a client would have in that contract language requiring that that U.S. web publisher had a clear and effective policy with a link to DoubleClick, and every single one of our new contracts has had that.

I have been going through the 1,000 or 1,200 sites that are in the DoubleClick network, taking a look at their privacy policies and requiring that they change that and link to us. So I think the numbers for us are substantially more than Mr. Smith laid out as well. Frankly, it is our firm policy that anybody that we will do business with, anybody frankly who has information that is being contributed to a profile, certainly has a link to our policy or I do not sign off on that site's participation.

The CHAIRMAN. Mr. Jaye, should consumers have access to the profiles that network advertisers keep about them when they are linked to personally identifiable information?

Mr. JAYE. When they are linked to personally identifiable information, yes.

The CHAIRMAN. Mr. Rotenberg.

Mr. ROTENBERG. Yes, Senator. I think without the ability to see the information that is being collected, the privacy policies do not really mean very much because they are very general, they are very confusing, and you really cannot make an informed decision. I think one of the points also in Jodie Bernstein's presentation with respect to cookies, even if you try to exercise choice, which is what she described with the browser software, you will see a screen that gives a web domain, an expiration date, and then a value field that is just a string of characters. It has no meaning to you.

For that reason, you have to see what information is being collected about you and how it is being used.

The CHAIRMAN. Mr. Polonetsky.

Mr. POLONETSKY. I think it ought to depend on the type of information. I think if we are talking about sensitive information, the kind of information consumers would be concerned could be used against them or could cause harm, there ought to be a higher level of protection. But I think that basic information, such as the kind of information that is used in the offline world for marketers to make decisions about what offers to send, the standard there for non-sensitive information could be opt-out as long as it was clear, as long as the consumer knew what the rules were when they were at the site.

The CHAIRMAN. What type of information should I have access to?

Mr. POLONETSKY. You should have access I think to a reasonable amount of information to the extent that the site has that information easily available.

The CHAIRMAN. Who should decide that?

Mr. POLONETSKY. Well, we served on the FTC Committee on Online Access and Security, as did Engage and some of the others at the table, and I think there is not a one-size-fits-all answer. There is some information that is probably easily available and we certainly, if we use personal information, will make that kind of information available.

Other information may be difficult. If I walk into a Macy's, whether it is an online version of Macy's or offline, and I say, I have shopped here once a year, could you please give me a record of everything I have ever bought—the question is what is the tradeoff? Are there certain kinds of information where consumers really need and really should have access? Are people making decisions about credit, about mortgages, information that is going to affect their lives substantially? If it is non-sensitive marketing information, I think the standard of access might be different.

The CHAIRMAN. Mr. Smith.

Mr. SMITH. Well, yes, it is a complicated problem of providing access, and there are also some privacy downfalls to it in the sense that if you allow somebody else to get information there are problems. But I would really love to know, for example, of those 27,000

transactions that DoubleClick got about me in the last 6 months which are very personal in nature, which ones they are saving and which ones they are not.

The CHAIRMAN. Finally, the issue of the moment seems to be that the FTC and the online advertisers are in serious negotiations. I would like to know the confidence level of the witnesses in the ability of the parties to come to agreement, and would that then negate any requirement for legislation?

Mr. Polonetsky.

Mr. POLONETSKY. I am not the person at the table for our company, but I can tell you that we are optimistic that they are progressing in a positive way. I think we all agree that strong standards of notice and choice that are adopted by all in our industry will provide a real strong level of protection for consumers. So we think that a system of self-regulation could be very effective.

The CHAIRMAN. Mr. Rotenberg?

Mr. ROTENBERG. Mr. Chairman, I think even if there were agreement between the industry and the FTC on practices in this area, it would not be sufficient to protect privacy. I say this for several reasons. First of all, we have followed very closely the self-regulatory efforts in other areas involving such groups as TRUSTe and BBB Online, and I think the sense at this point is that those are not providing adequate protection in the online world.

The second point, as a matter of process, I have been personally disappointed that the FTC has not involved the privacy community in this proceeding. I think we have a right to participate. We were, after all, the group that initiated the complaint at the Federal Trade Commission. We identified the flaws in those privacy policies, and we think if the FTC proposal is going to be responsive it has to address the issues we raised.

The CHAIRMAN. Mr. Jaye.

Mr. JAYE. As was reported evidently this morning in the *Wall Street Journal,* I guess I am optimistic about our likelihood of reaching agreement, and I stand by that comment. I think that the industry has been working very hard—I am one of the people at the table from my company—to try to come to agreement on a baseline set of standards that will meet the legitimate consumer concerns about data protection and privacy with regard to network advertisers.

I think that there has been a very good faith dialog going on and I hope that we will be able to come to an agreement. Whether or not there is a legislative backdrop or not is somewhat independent, because I think in the end self-regulatory programs in this area will be more effective for jurisdiction issues and many other issues.

The CHAIRMAN. Mr. Smith.

Mr. SMITH. Well, I have not been privy to any of the negotiations also, as Marc has pointed out. I am also a programmer, so I am not sure that I can comment so much on the legal issues here.

But overall, I think one of the concerns I think raised in the earlier testimony, what if somebody just does not want to participate and then we have that problem? That could just see a breakup of those kinds of regulations.

The CHAIRMAN. Senator Wyden. I thank the witnesses.

Senator WYDEN. Thank you, Mr. Chairman.

Mr. Polonetsky, I am interested in knowing when DoubleClick collects information from a website how detailed the information is about a consumer's activities there? For example, if I visit a bookstore site, do you have full information about the titles I browse through as well as what I purchased?

Mr. POLONETSKY. The answer is not at all. What DoubleClick does is we deliver an ad when somebody is at perhaps a site where books are being sold. So the information we have is that we delivered a sports ad to this cookie ID when it was at this sports site.

Senator WYDEN. What about recording search terms that I type in?

Mr. POLONETSKY. When one goes to a search engine and types in a keyword that one is searching for, the page that is generated—let us assume one goes to a page and types in "golf"—the search page that is generated is going to be a golf page. So the information that DoubleClick gets is: serve a sports ad here, serve a golf ad here, because the search term is going to provide a golf page, so put in golf. That is the kind of information that we would have in terms of paying an advertiser and paying the website for the ad that was served and the ad that was delivered.

Senator WYDEN. How many users at this point do you have profiles on?

Mr. POLONETSKY. We actually do not currently serve ads based on profiles. I know that that is a misconception that many have. We currently serve ads based on some of the visible demographics of the browser at the site, geographic information——

Senator WYDEN. What kind of numbers are we talking about there?

Mr. POLONETSKY. So those are not profiles at all. We are, however, developing such a product, as some others are doing, and will have one in the near future. But we are not currently working with profiles. We will probably have say 40 or 50 million when we do, because we serve ads at many sites. But we currently are not serving ads across the web based on profiles. We are serving ads based on somebody is going to a sports site, we know we have showed three ads to this unique cookie ID on other sites; let us serve this sort of ad into that site.

Senator WYDEN. Now, Mr. Rotenberg, most of the users never visit the website of the online profiler that is collecting information. So we are wrestling with this question of notice and choice and how to deal with the collection of profile information there. Would host websites serve as intermediaries between the consumer and the profiler? How would you see that working? For those of us who want to make sure that those kinds of FTC principles apply to profiling, how would you address this question of notice and choice specifically?

Mr. ROTENBERG. Senator, I think the whole process has to be much more transparent. One of the very interesting things about Jodie Bernstein's presentation, when she described what was taking place with the cookie tracking online you saw boxes go up. I think she used the phrase "US Advertising," maybe that was the ad network, "US Advertising is now gathering information for this purpose, US Advertising is now linking information for this purpose."

I actually believe that those are the types of notices that consumers who are online should be able to see as the information flows. In other words, you have to literally understand as you move from one website to the next what information about you has been obtained and how it will then be used.

Now, at that point you can make a decision and you can say: Well, I do not want to be a part of an advertising network that collects information about me in this way or uses it in this way. There should be a box there that says: I am not going to be a part of this.

But as long as we have these very complicated arrangements where people cannot really evaluate what is going on, frankly, it would not matter whether you had to go to the advertiser's website, a consortium's website, or the website that you visited originally to express a preference, because you would not understand what the preference was you were expressing.

Senator WYDEN. In your view, how critical is the distinction between personally identifiable information and the non-identifiable data that is collected by profilers?

Mr. ROTENBERG. Well, I used to think it was about the brightest line that there could be. But I have actually changed my view on this, because I understand now that it is possible to take a profile that is not linked to a known user and subsequently link it to a known user. In fact, that is exactly what happened with DoubleClick. And I am a little surprised to hear them say that they are not creating profiles. Now, they have tens of millions of unique cookie ID's. Maybe that is the phrase we should be using. Currently today, tens of millions of unique cookie ID's, and those are the ID's that make it possible when Richard Smith surfs the web for an advertiser to know that three ads have gone out to that unique cookie ID which Richard Smith is standing behind and therefore we have to put a different ad.

Now, if that unique cookie ID can be linked to Richard Smith, even though it may not currently be linked to Richard Smith, then I think we need some legislation in place to control that practice.

Senator WYDEN. Let me do this, because I have one other important question I want to ask about litigation. But Mr. Polonetsky, do you want to respond to Mr. Rotenberg's point, because I think that the reason I asked the question about what you all were doing specific to individuals is that is of course what the American people want to know. You all are sort of the most visible company in this area and Mr. Rotenberg just described a way with the use of the cookie ID that a fair amount of personal information was in effect being collected or certainly utilized.

Mr. POLONETSKY. Sure, let me clarify if I can. First of all, we are not using any personal information at all. What we are doing is when a browser comes to a site that browser is assigned a unique ID. If DoubleClick is serving an ad on that site, DoubleClick knows that this Nike ad was served to this unique ID.

We also know that most folks, if they have not responded to an ad after two or three times, do not keep showing the same ad over and over and over again. So what we will keep a record of is this ad was shown one time, two times, three times, so then do not show this same ad again, show a different ad the next time that unique ID shows up at a site where DoubleClick is serving ads.

So I do not know that that would be considered profiling. I think that would be frequency capping, making sure the same ad is not shown over and over. I would say that a profile is keeping track of all the different sites that a unique ID was at and then building a record saying, well, this is a cookie that spends a lot of time on sport sites, on news sites, so let us show them a certain kind of an ad when that anonymous ID shows up again at a different site.

Senator WYDEN. Mr. Rotenberg is smiling and that indicates to me that he is probably concerned about the ramifications of that on individuals.

Since time is short, I want to ask just one other question. It is really for you, Mr. Jaye, and you, Mr. Polonetsky. That is, with folks in the industry facing lawsuits with respect to the practice of online profiling, do the two of you, Mr. Jaye and Mr. Polonetsky, believe that by defining the appropriate scope of profiling behavior that that might head off some of the disputes that seem to be headed for a lawyer's full employment program here?

Mr. Jaye.

Mr. JAYE. At Engage we feel comfortable that since we started the company we have had privacy—finding the balance between the consumer's right for privacy and the marketer's need for effectiveness—in the form of anonymity. We feel very comfortable in our position with regard to those types of risks.

Certainly there is still the possibility of some sort of action that would be perhaps without merit, waste our time, waste the government's time. But at the same point, we are concerned about moving quickly. For example, just to take a point, this issue about web bugs. I think web bugs are a very legitimate concern because they are not visible to the consumer. But one very important use of this technology is not for any type of profiling, but simply for the ability of reporting to an advertiser the percentage of visitors who saw an ad who actually subsequently made a purchase, not at an individual level at all, but the ability to basically tell the advertiser did they spend their money wisely.

If we cannot provide that level of reporting, the ad spending on the Internet is not going to be sustained. So it is very important to proceed very carefully to make sure we draw the lines so that we do not inadvertently carve out the ability for the advertising to be supported while at the same time addressing the very legitimate concerns about invisible tracking.

Senator WYDEN. Mr. Polonetsky.

Mr. POLONETSKY. I agree. I think that education, definition of the terms, transparency so consumers are aware of what is taking place is the key. Much of the research I think that is out there academically and certainly much of the work that we have done at DoubleClick has indicated that as people are aware—as they understand the technology, as they understand what control they have over any information and how it is used—they become increasingly comfortable with their surfing on the web and what is taking place.

So one of the reasons why I think we talk about notice and choice is it is an easy way to show a consumer what is going on at a site. It is one of the reasons why we ran our online ad campaign and I think it is probably key in terms of self-regulation—

making sure that consumers understand what we do as the greater American public starts spending more and more time shopping and using the benefits of the web—that people understand how it works and how they have control over what happens on the web.

Senator WYDEN. The central problem, of course, is that millions of people, as Mr. Rotenberg has talked about——

The CHAIRMAN. Senator Wyden.

Senator WYDEN. And I will wrap up with this, Mr. Chairman. The central point is that——

The CHAIRMAN. I am not trying to cut you off. If you would like to at least let Senator Kerry go and then we will come back to you.

Senator WYDEN. I will wrap up right now.

The CHAIRMAN. Thank you. Thank you. No, please.

Senator WYDEN. This was just my last point. I happen to share your view on education and it is clear. But what Mr. Rotenberg said that is central to this is that millions of people are not at this point empowered with enough information to make these choices, and that is why I am hoping that we will be able to get some legislation that defines the appropriate scope of profiling behavior.

I thank you, Mr. Chairman.

The CHAIRMAN. I thank Senator Wyden and I again appreciate his deep involvement in this very important issue.

Senator Kerry.

Senator KERRY. Thank you, Mr. Chairman.

Mr. Smith, could you repeat for me. You mentioned something about 27,000 transactions. That is more than a bank. I did not quite get the whole thing.

Mr. SMITH. Right, yes. I log each time a web page is fetched or an image is fetched on my computer and sent out to companies on the Internet. In 6 months I had 250,000, a quarter million of these transactions—web pages that I went to and images that I saw. More than 10 percent of those went to DoubleClick.

With that, each transaction was for like a banner ad. There would also be the URL of the web page that I was at. So if I was at Quicken, they would get what page I was on at Quicken.

Senator KERRY [presiding]. But you said something to the effect that that represented a lot more information than any bank has on you, or something.

Mr. SMITH. Yes.

Senator KERRY. But that is not the kind of information that a bank collects or needs or that you give a bank. I mean, the bank has your social security number.

Mr. SMITH. Correct.

Senator KERRY. And the bank has an address.

Mr. SMITH. I was talking about quantity here, not necessarily quality.

Senator KERRY. Well, but your quantity was for a specific purpose. You are not the average person shopping in some way. You were out there really analyzing this.

Mr. SMITH. Well, I might be using it a little bit more, but I suspect for a regular person it might be 100 transactions, 50 to 100 transactions in a day.

Senator KERRY. But what I am trying to understand is the information that they gleaned from that was essentially non-personal, am I correct?

Mr. SMITH. No, that is not correct.

Senator KERRY. What was the personal nature?

Mr. SMITH. Well, I will just go through some of the list here: my name, my home address, my e-mail address, what plane flight my daughter was taking to Philadelphia from Boston, these sorts of things; on buy.com, the movie that I was renting.

Senator KERRY. Let me stop you there, because I was trying to figure out what kind of information it was. Now I want to go from there to Mr. Jaye.

I specifically want to flow out of this. I think that is the heart of what we are trying to get at here. Mr. Jaye, you listed the way Engage approaches this and what you can guarantee and a list of things that you do not do. Would you repeat that list?

Mr. JAYE. Certainly. We do not know a consumer's name, address, social security number, or any other personally identifiable information. We do not maintain information about specific web pages a browser visits, which is probably the one that is most relevant to this issue. We do not collect any sensitive or controversial data, such as personal medical or financial data, ethnic origin, religion, political interests, or review of adult content, and we do not merge anonymous profiling data with personally identifiable data no matter the source.

I think just a comment. I think the issue here has to do with the specific information about the web pages because of the data spillage issue in particular I think that Richard Smith is bringing on. That is precisely the reason why we took a data minimalization approach at Engage to make sure we did not maintain that information.

Senator KERRY. So essentially you have software that has the capacity to provide a guarantee of anonymity.

Mr. JAYE. We have made every attempt that we could. Just once again in full disclosure, the way the web works is data may be received, but there is a difference between when data is received and actually processing that data and storing that data. We do not process that spilled data, and one of the reasons why we discard it is so that it cannot be subsequently processed.

Senator KERRY. When you say discard, practically speaking how does that happen? What happens to it?

Mr. JAYE. From a technical perspective, it never gets written out into magnetic storage and where it is maintained in memory for the milliseconds or the seconds while the data around it is being processed is quickly overwritten with other data.

Senator KERRY. So, for all intents and purposes, it has disappeared, or could somebody draw it out?

Mr. JAYE. It has for all intents and purposes disappeared.

Senator KERRY. Now, Mr. Rotenberg, what is the matter with that?

Mr. ROTENBERG. I actually think it is pretty good. I think it is the type of network advertising that a year ago I explained could work for business and work for consumers. The problem, though,

is that consumers online do not have a choice about whether to get their advertising between one firm and another.

Senator KERRY. Correct. Now, if we were to mandate that the notice be up front and personal as to what the expectations are, what is going to happen to somebody, what is being offered, is there any consumer responsibility here? Is there any caveat emptor, any degree to which an informed consumer takes place on page one if it is adequately noticed?

Mr. ROTENBERG. I think consumers have some responsibility, but I think in fairness, considering the rapid growth of these various business models and the various types of advertising schemes, we are going to be doing this dozens or hundreds of times for consumers every time someone figured out a new way to collect and use personal information, which is why I think—and I do not think Mr. Jaye would necessarily disagree with me—that a simple set of fair information practices of the type that have been adopted in previous legislation—we have done this, by the way, with a lot of technology. We have done it with cable subscriber records, video rental records, e-mail.

We have put in place basic fair information practices and then companies like Mr. Jaye's do very well because they have good business models and they protect privacy.

Senator KERRY. That is essentially what I am talking about. That is a notice approach fundamentally, with a requirement as to standards that are adhered to, correct?

Mr. ROTENBERG. And access; notice and access.

Senator KERRY. Well, come to the access thing for a minute. I want to come back to the other for a second. But when you say adequate access, of course people should have access. We want to have some structure there. To what degree can you get detailed? Exactly how is access going to be implemented, specifically with respect to what sort of corrective measures are available to somebody? Once they have access, what information ought to be changed or can a person change if they do not like it?

Mr. ROTENBERG. Well, it is a problem, but I think it is also a problem that has been handled in the past. It has certainly been handled fairly well in the credit reporting world. People who disseminate information say: To the best of our understanding, this information is accurate, and the credit subject seems to disagree with what we know about this person.

So what that statute says is: Okay, give that person a right to include in the record his own interpretation about what the bill was not paid. Then the person who receives the file can see what the credit reporting agency is saying and what the credit subject is saying and make a determination about how to interpret it.

But we have not even approached that type of resolution to I think the question that you are asking, because we are still not sure about whether people should have the right to access these profiles. I think we have to take that as a starting point and then figure out how we would resolve these important questions that you have asked.

Senator KERRY. Now, what is the distinction between the profile as it has been described, that is achieved by a cookie or by ten million cookies and the profile that somebody might have created on

themselves by repeated visits to Macy's, Neiman-Marcus, and whatever numbers of stores, and they then are getting X number of catalogues coming to their house on a regular basis?

Mr. ROTENBERG. Well, I think they are different in at least two respects. One, it really is the nature of this interactive digital environment that you can collect a lot more information about individuals. That is why these——

Senator KERRY. Let us stop for a minute.

Mr. ROTENBERG. Yes.

Senator KERRY. If we have proceeded—I am not saying laissez faire. I have said we have got to have a standard and we have got to put something in place. Let us assume we put in place a very clear notice requirement with the principles of choice and access and security as subtexts of that notice. This is what we are trying to achieve as a full measure of people's ability to participate in the following way. They are the principles that have already been adopted fundamentally by the industry and others, but there is not a clarity to them necessarily.

Let us say that that is the structure you have here. But you are giving to companies like Engage and others out there the creative capacity to provide the technologies and the competitive abilities to offer people ways of satisfying their desire to have this adequate privacy. Would you not possibly excite a greater response and in fact a speedier response conceivably by approaching that for a little while here to see how this develops?

Mr. ROTENBERG. I think the critical question at this point is what direction is this self-regulatory experiment taking us.

Senator KERRY. But I have gone beyond the self-regulatory in that, because if we have gotten very specific as to the level of notice. Let me say that I have particularly become sensitive to this in the last months. I have tried to find different people's privacy and some you can see it on the home page, boom, you hit it, and it is lower down, it is not exactly leaping out at you, but you can find the word "privacy" or some protective disclosure. On others you have got to go multiple clicks away, and in some cases it is quite complicated because then you have got to type in a relatively long and complex address to go find it and get the full privacy level.

So it is clearly a discrepancy between companies as to what they are prepared to offer people in terms of disclosure. There is no question about that. But if we were more clear about that requirement of disclosure and there is a clear understanding that it is an unfair trade practice not to provide that up front choice to people adequately. You then have empowered the FTC in terms of enforcement to the degree they can and you have left it to people like Engage and others to hopefully come back with a series of competitive measures that offer people what they want.

Do you see something lacking in that?

Mr. ROTENBERG. Well, Senator, I think the problem—and I certainly understand what the proposal would—I think I understand what the proposal would accomplish. But I think the problem is that even if we have a simplified notice and a clear notice where people can make better informed choices, we will still end up forc-

ing consumers to choose between their privacy and the benefit that the website is offering.

I believe that there are solutions that will allow us to avoid those choices, so that advertisers can reach customers, so that web merchants can effectively deliver their products, without requiring consumers on the Internet to make a choice that invariably involves giving up some degree of privacy.

Senator KERRY. I think you have got to be more explicit on that, because I have a hard time envisioning it. I mean, I assume you would agree that there is a major problem if advertising cannot support the Internet, correct?

Mr. ROTENBERG. No.

Senator KERRY. I mean, the dream has been that the Internet is going to be free, fundamentally supported by advertising. But the verdict is out on that. I mean, I understand the number of—Mr. Smith, is not the number of clicks that are currently recorded as spending meaningful time or making a purchase is lower, it is about 1 percent, is it not?

Mr. SMITH. Right, it has been dropping. But also the number of banner ad impressions has been going up much faster. So it is not necessarily an indication of a problem, just that the number of ad impressions has gone way up. And the companies who are showing banner ads, revenues are rising very rapidly. So more money is coming in on advertising.

Senator KERRY. And I think if I am correct, the current prognosis is that the advertising revenues are going to go from something like $6.7 billion up to $20 billion in the next couple years. But that depends on the continuing capacity of people to be able to market effectively.

Mr. SMITH. Right.

Senator KERRY. If all of a sudden that is taken away somehow because this balance of what you are saying, the choice between adequate protection and capacity to be able to effectively figure out who you are reaching is not in balance, you could wind up with people choosing sort of what they think is going to be good for them to protect themselves, but in effect it is going to deny people the capacity to know how to advertise or how to target.

Mr. SMITH. One thing, now. The jury is also still out on whether online profiling is effective technology for ads. I do not think that has been proven at all. *The New York Times* had an article about a month ago on this exact subject.

Senator KERRY. Well, I think the point is, the point being made by Mr. Jaye, while he is speaking for a specific company and technology and it may be that others can do it as well or whatever, but the point is that they have the ability to provide a lack of profiling, a specific guaranteed lack of personal profiling and use of personal information, but still permit an adequate balance with respect to the advertising needs. Am I correct?

Mr. JAYE. Yes, that is correct.

Senator KERRY. It seems to me that if that exists, if it is there in technology and it is really an effective component of the notice that is right up front, that if somebody is, in fact, that is their *sine qua non* of participating in the Internet, they can get it. And if that

notice is required adequately up front, then have we not provided the protection?

Mr. SMITH. None of us have seen our profile, so I am not sure how we can say. We are going by the word of the companies on what they say they are doing and they are not doing. I hear from DoubleClick that they stay away from medical issues, yet they put web bugs on anti-AIDS drugs. So I do not know what to think.

Senator KERRY. I mean, there is a distinct difference between typing in a search word "AIDS" and getting back some drug advertisement or something versus some medical record of yours with respect to a test or a visit or something else. Those are two different worlds.

Mr. SMITH. Right, but in between here is——

Senator KERRY. Do not confuse it as a medical. That is not a medical.

Mr. SMITH. But what I am talking about is an invisible image at the Procrit.com website that sends back a message to DoubleClick saying you are now here and, oh, by the way, you are interested in cancer treatment. So I do not see that—yes, it is not medical records, but it is not just viewing a banner ad, either.

Mr. POLONETSKY. If I could jump in——

Senator KERRY. Yes, Mr. Polonetsky.

Mr. POLONETSKY. And perhaps explain a little bit about what these tags do. The sites want to know how many unique users have visited their site and they also want to know which of the ads they have run have brought unique users. Johnson & Johnson, which is the operator of Procrit, might be running an ad on AOL, might be running an ad on Yahoo, might be running an ad on a DoubleClick Network site, and wants to know how many people are coming, how many anonymous unique users are coming to the Procrit site from each of the sites where ads were displayed.

They use this spotlight tag, as we call it, or, as Mr. Smith calls it, a web bug, to simply anonymously keep a record of how many users are coming to the site and did they come from the ad that Johnson & Johnson ran on AOL or Yahoo. Innocuous. The information does not belong to DoubleClick. We are providing this service on behalf of the Johnson & Johnson Procrit site. We do not use it for a profile.

Senator KERRY. How do you answer the question posed by Mr. Smith as to whether or not he can have some kind of personal guarantee that that is in fact all you are doing, so that he will know that is the full profile?

Mr. POLONETSKY. He has got a number of guarantees. Number one, we employ an outside third party auditor, so the commitments that we make are audited by PriceWaterhouse–Coopers, so that we can guarantee that we do what we say we do. My role as Chief Privacy Officer, as a former consumer affairs commissioner, is to report directly to our Board and be the inside watchdog ensuring that we live up to the commitments we make.

Frankly, our clients would be very unhappy if we took information about how many users were coming to their site, and how their site was doing, and which parts of their site were getting more hits, and which ads were bringing people to their site, and used it for anything else. So we legally are bound to make sure

that any information, anonymous information that we are getting from a tag, is used specifically for that purpose: given back to the advertisers so they know how they can manage their content.

Senator KERRY. Mr. Rotenberg, if that kind of guarantee can be put in place and you have the capacity through the software being provided by Engage or others to be able to give people that option, what is the compelling rationale for something more mandated and intrusive?

Mr. ROTENBERG. Just to be clear, Senator, when you or I surf the Internet and banner ads are placed, we are not choosing between Engage and DoubleClick as the company that is going to serve ads to us.

Senator KERRY. You are saying anybody can do that.

Mr. ROTENBERG. Exactly. Anybody can be doing this in the background. And while I agree with you that I think Engage is doing some good things certainly, I do not think privacy legislation is going to undermine what Engage is doing. If anything, it may spur the development of half a dozen companies like Engage, all looking for better privacy solutions.

Senator KERRY. What is the technological response to the fact that once it is out there on the web, so to speak, anybody can grab it and try to use it and pull it down? What is the response to that, either Mr. Jaye or Mr. Smith?

Mr. JAYE. Well, first of all, it is not anyone. They require certain network connections that make certain types of transfers possible. But in particular, the commonly used technology is this thing called third party cookies, that is cookies that are set and sent back to a website other than the website the consumer is specifically visiting.

That does not mean that anyone can; only the sites that are working with each other. So for example, there usually has to be a specific relationship between the website and the third party in order for the third party to gain that data.

In terms of the technical aspects of it, that is one of the reasons why two and a half years ago I initially started working on this trust label standard at the ITF, which was a standard to focus on how do you take that cryptic pop-up box telling you that a cookie was being set and to tell you what it meant, what it was going to be used for, and more specifically make it so that the riskiest behavior to consumer privacy, which is third party cookies, would have a hard and fast requirement that those cookies would have to pass muster, they would have to be digitally signed by seal authority before they would be allowed through or else robust notice and choice would be provided to the consumer.

So I actually do disagree at the moment with the people on my left and right with regard to technical solutions addressing the legislative need, because I think that type of technology solution goes farther than any legislation could go in ensuring that we do not have bad actors who are beyond our reach.

Mr. POLONETSKY. Senator Kerry, if I could just correct the record for a second as well. There was the data spillage issue that was raised earlier and some of those were DoubleClick examples. There was a technological issue and that is the reality that there are some sites that accidentally—they should not, but accidentally—

have information sent to anyone they link to if there is a form on that page.

Now, we certainly informed our clients that they ought to take a close look and make sure they are not accidently finding unintended information. But we have also implemented a technological fix to this problem, in addition to saying please do not send us anything that we should not have, we do not want it, we do not use it, it does not go in a profile, but do not even send something that someone will get nervous about. We have set up a process where our ad servers truncate anything after the question mark.

So if we are accidentally sent information from a website that we do not want, it does not even get recorded because our technology automatically chops that off so it does not get to us.

Senator KERRY. Well, query whether you would all be better off if we were to be more mandatory in being sort of prophylactic about the capacity of that kind of accident to occur. In other words, if we make it unlawful for people to transfer and use, or to use conceivably, that kind of third party transferred information, would that have an excessively intrusive impact, based on the fact that you are saying that this would be accidental and therefore no company would set out to do it and therefore no one should be impeded by our saying that is an unlawful act?

Mr. POLONETSKY. Well, I think this is probably the best example of how self-regulation works. Here was a technological flaw which we all appreciate Richard Smith for helping point out and identifying, and all the companies who are in the industry—and frankly, this is not solely an ad server problem. If I have a website and I have got a form because I am selling something or registering and I have links to other sites that I have got partnerships with or that I am linking to because it is useful information, I can accidentally at this website be sending that information in any direction.

So this is a technology problem with the way some websites are set up. When it was identified, all the responsible sites quickly took a look and made sure they were not doing it. Frankly, those of us who are at the receiving end, who are being accused of getting this information and using it or having it, very quickly said to our clients: Do not accidentally do this, and here is how we are going to make sure it does not get to us.

So I think legislation probably cannot even anticipate some of the other practical problems. This is a perfect example of industry becoming aware of a flaw in the infrastructure of the technology of the web and then quickly fixing it so that it does not happen.

Senator KERRY. Should it be technologically feasible or even should it be a matter of public policy that if somebody did not want pop-up ads at all that that should be an up-front part of notice and they should be able to opt out of those immediately?

Mr. POLONETSKY. It has been our policy at DoubleClick since 1997 to have an opt-out link, even when——

Senator KERRY. But it isn't easy to opt out. I mean, let us be candid. There are lots of people in the country who would like to opt out of a lot of things on the net and it is very hard to do even for people that know how to use the net.

Mr. POLONETSKY. I think it is our job to make it frankly easier. The Internet is 1,700 days old; our company has been public for

two years. I think this huge growth in sites having privacy policies from 14 percent two years ago to 90 percent—I agree, now those policies need to be complete. But I think we are making real rapid progress and in an industry that is still in its infancy, and frankly, consumers will use the Internet that we are first imagining.

So I argue that if industry is moving in the right direction, is eagerly working with the FTC, working with each other, to put the appropriate protections in place, I think you are seeing the ideal of how responsive self-regulation should and can work.

Senator KERRY. What do you think, Mr. Rotenberg?

Mr. ROTENBERG. Well, I think it is fine to encourage industry to address privacy concerns, and in that respect some progress has been made. But at the end of the day, I think you really have to focus on the central question, which is, is consumer privacy being protected? That is about more than assurances. It is about what is really happening, whether people can exercise opt-out, what the purpose, frankly, of choice is in this very important policy world.

So certainly as a privacy advocate I do not want to criticize industry groups for trying to address this issue. But also as a privacy advocate, I have to say to you my sense is that the gap between the amount of privacy protection that people expect and the amount that they are receiving online continues to grow, and it is going to grow further. That is why we need legislation, to give people control over their personal information.

It may mean that more companies like Engage are going to do well in that world, because it will be a world where privacy will be important.

Senator KERRY. Did one of you want to respond to that or you are comfortable on it?

[No response.]

Senator KERRY. Well, there is no question in my judgment, as I have said at the outset, that we need to establish the standard here. The question is how far do we go and how quickly, and I think it is the balance that we need to find.

You said, Mr. Rotenberg, that it is a different kind of privacy problem on the Internet. I just wanted to explore that with you for a minute. Obviously, because it is electronic, because it is global, because it is fast, there is a perception issue there. But tell me how in your judgment? Is it the distribution network that makes it so different and raises the specter of threat?

Mr. ROTENBERG. It is the ability to track and monitor what you do. If you go into a book store, pick up a book, put it back down, find another one you like——

Senator KERRY. Right, nobody knows what book you looked at.

Mr. ROTENBERG [continuing]. Pay for it by cash—there is a tremendous amount of anonymity in the physical world, and so much of what we do—driving in our car, walking on a street, riding the Metro, cash-based transactions, this is all anonymous by and large.

In the online world, there are a great deal of incentives, understandable incentives, to collect information about what people do. You cannot do it offline, but you can do it online. That is what created the problem here. It is because this information could be collected and that there was no way to protect privacy when, for un-

derstandable reasons, I may well have done the same thing at DoubleClick or Engage in terms of building these profiles.

That is why I think Congress needs to take some action in this area. It is different.

Senator KERRY. Well, it is more intense, but as to the browsing and as to the collection of that information, again it is possible to create a standard by which people are offered the opportunity to have that be anonymous, is it not?

Mr. ROTENBERG. Anything that we can do to promote anonymity online—and you have mentioned this several times, Senator—I think should be encouraged. I think a lot of people who are familiar with the history of the Internet—and I do not just mean the last few years of the World Wide Web and electronic commerce, but know the history of how this network of interconnected databases could allow people to freely collect information—look at data, post news, read news, without disclosing identity—understand that anonymity has always been a very big part of online privacy.

It is that interest that is now being threatened. Now, as I have said before, I think advertising can be made to work, can be made to work very well. I said it in my testimony, in many ways the Internet offers a wonderful platform for giving information to consumers. But I think we have to draw some lines, and one line to draw is when we are collecting information about individuals.

Senator KERRY. There is, I assume you would agree, a distinction between—well, I think we have been over that. I do not think we need to beat that over.

On the third-party cookies, is there a specific—should that require a specific remedy legislatively directed, or is that something that under some privacy policy you think it could be contained?

Mr. ROTENBERG. I think if we have a general rule on the collection and use of personal information online that will be easiest for businesses, because they do not have to sort of go back and forth, where are we; and it will be easiest for consumers because they will know what the expectations are. I am just concerned if we try to draw too many lines particularly related to certain technologies or certain business practices that we are familiar with today——

Senator KERRY. So it is better to have a broader standard that applies, which is basically the way I think we are heading.

Mr. ROTENBERG. Yes.

Senator KERRY. Understood.

Well, I appreciate it. It is a very interesting subject with a lot of complexities, but it is very important that we try to get it right. I am very grateful to you for your input, all of you here today.

The record will remain open for two weeks. If anyone wants to update their statements, they can do so. Likewise, colleagues can submit questions in writing.

At this time the hearing is adjourned.

[Whereupon, at 12:40 p.m., the Committee was adjourned.]

APPENDIX

PREPARED STATEMENT OF MR. STEVE MARKOWITZ, CHAIRMAN AND CEO, MYPOINTS.COM, INC.

Mr. Chairman and Members of the Committee, I am Steve Markowitz, Chairman and Chief Executive Officer of MyPoints.com. I am pleased to have the opportunity to submit testimony about my own and my company's sentiments concerning the important issue of online profiling and privacy and I thank you for the forum to explain MyPoints' consumer privacy program, which, I maintain, could form the basis of an industry standard.

MyPoints.com is the Internet's most popular promotional site, and the Internet's fifth most popular shopping site. More than eight million consumers have voluntarily joined our online membership program—MyPoints®—and given us express permission to contact them via e-mail with targeted advertising offers on behalf of our clients. We reward consumers to interact with our advertisers, and our advertisers rely on us to provide them with an integrated suite of cost-effective, permission-based e-marketing tools.

The MyPoints Program was developed as a "True Opt-in®" Internet service, and express permission lies at the heart of our business model. Put simply, MyPoints has one of the Internet's strongest privacy pledges—guaranteeing to each member that his or her personal information will not be released to any third party without his or her express permission. MyPoints members are fully aware and have expressly approved of our information practices.

We feel so strongly about our True Opt-in marketing approach that we have trademarked the term "True Opt-in." However, while extremely well positioned in the competitive and volatile e-marketplace, MyPoints.com—like any company in the Internet marketing services space—is not completely insulated from the privacy concerns rumbling through Internet message boards, the national media and now, the halls of Congress. Impact on the industry at large can have an impact on every player in the industry—even players on the right side of the privacy debate. In fact, the only way to fully protect every company in this important and fast-growing industry is for a strong move by the federal government to regulate this space, and help allay consumer concerns once and for all. Self-regulation is nice in theory, but with heavy vested interests in a less than-fully consumer focused privacy policy, change will be, I fear, too slow to offset consumer concern over Internet privacy issues. Swift and sure movement by the government is the best answer.

Let me begin by explaining MyPoints' stand on privacy, and then I will address how the industry and government need to cooperate to frame effective legislation. The MyPoints privacy policy makes certain absolute guarantees to our Members. First and foremost is our pledge never to release personally identifiable information to any third party without the Member's express consent. Thus, any person who enrolls in our program does so voluntarily with the knowledge that their personally identifiable information is safe in our hands. This key concept is the foundation of our relationship with our Members, a relationship based upon trust. We send all communications to the Member on behalf of our advertisers—we do not reveal our list of e-mail addresses to anyone. Members are then rewarded simply for reading and responding to the messages they receive by e-mail and on our website.

On the Internet today, consumer privacy has become an oxymoron. Businesses have the ability to track consumers as they move about the virtual world, noting what they like, what they don't like, how long they spend at one site or another, what they buy and how much they spend.

For many businesses, the name of the game in Web marketing is data—personal data that sophisticated advertisers use to target ever more specific offers. For the consumer there is a bright side as well as a dark side. The bright side offers ever-more-relevant advertising and opportunities to extract more value from one's time online. The dark side shows itself when companies most consumers don't know exist compile deep profiles on them and manipulate personal data on behalf of advertisers most consumers never asked to hear from.

It is necessary for government and industry groups to consider both sides carefully as they inevitably make their way towards more stringent regulations regarding true consumer privacy on the Internet. However, a threshold issue has already split the Internet marketing industry into two camps—the question of who should regulate whom. Most Internet industry groups call vociferously for self-regulation. The standard refrain is that government meddling will lead ineluctably to inefficiencies in a fast-moving marketplace. **Yet, it is precisely the speed at which the Internet is developing that demands a more active role by the government in protecting consumer privacy online.**

There are more than 10 million commercial Web sites in the United States alone, and the number grows by scores every day. Unfortunately, according to the recent survey by the Federal Trade Commission (FTC), only 20% of Web-based businesses currently comply with FTC standards of fair information practices. There is also significant confusion over what "Internet privacy" really means. Ask five Web site managers to describe when a user has "opted in" and you are likely to get five very different answers. The Internet marketing industry in general has proven to be a fairly lax self-regulator. Like any big city on the information highway there is a Main Street and there are back alleys, and many "back alley" companies have been less than genuine in their dealings with consumers, especially with respect to the protection of personal information.

This leaves an important and immediate role for government to play in protecting consumer privacy by setting fair and simple guidelines and actively enforcing them. Banner bar networks are one example of where regulations would be an improvement. Many have been known to surreptitiously collect user information, and although they do give users the opportunity to opt out, this presents a barrier to the average user who simply does not know how to go about it. On the e-mailer's side, many use an "opt out" standard as well, which presents additional barriers to the unwary consumer. These and other dubious means to get the user to supply information and supposedly "agree" to its use are what have caused user alarms to sound. A clear-cut, government-enforced policy would eliminate this issue, in no way impeding the conduct and growth of legitimate Internet businesses.

Regulation is not something for the industry to fear. A major move by the government to take charge of this matter will do much to allay consumer concerns (real and imagined) about Internet security, which will in turn drive the continued embrace of the Internet. Companies that will prevail in today's Internet marketplace will do so precisely because of the relationships they have with their users. Trust is the key to building that relationship. The problem is not the collection and manipulation of data per se, but collection and manipulation of data without express permission based on full disclosure of a Web marketer's data practices. Consumers are smart. Let them make the call from there.

Many online marketers will ask, why should this be? In the offline world, after all, the rule was "opt out." Consumers were fair game for marketers so long as they didn't specifically ask to be exempted from the marketing process. But on the Internet, the rules are dramatically different. Marketers unprecedented power to deliver messages less expensively, faster, and far more effectively than ever before. And it is precisely because of the unique advantages of the medium that marketers must make a trade—the ability to utilize the medium in exchange for a higher degree of respect for the consumer's roll in creating it. **The Internet is a channel for the consumer, by the consumer.**

Thank you Mr. Chairman for allowing me to express my views on the online profiling and privacy issue and share MyPoints.com's commitment to protecting online consumer privacy.

ADDITIONAL TESTIMONY OF RICHARD SMITH, INTERNET CONSULTANT

During the Senate Commerce Committee Hearings on June 13, 2000, Daniel Jaye of Engage and myself disagreed on the issue of the number of Web sites which link to the Engage privacy policy. After the hearings, I did some further investigations of the issue to see why Mr. Jaye's and my numbers were so different. What I found is that the AltaVista search engine was able to locate more than 1,100 Web sites that contain links to the Flycast privacy policy. Flycast is an ad serving company that Engage acquired earlier this year. Clicking on one of these Flycast links actually takes a person to the Engage privacy policy and opt-out page. I believe that for the consumer this is a confusing situation about who Flycast is versus who Engage is. However, I now do agree with Mr. Jaye that Engage has worked with mem-

ber Web sites of its ad networks to have these sites link to the Engage privacy policy.