UNITED STATES OF AMERICA

DEPARTMENT OF COMMERCE

AND

FEDERAL TRADE COMMISSION

---

PUBLIC WORKSHOP ON ONLINE PROFILING

---

Auditorium

Department of Commerce

Building

1401 Constitution Ave., N.W.

Washington, D.C.

Monday, November 8, 1999

The workshop was convened, pursuant to notice, at 8:48 a.m.
PROCEEDINGS
(8:48 a.m.)

INTRODUCTORY REMARKS

MS. BURR: Welcome, everyone, to the Department of Commerce. Thank you very much.

Good morning. It is a pleasure to be here this morning to welcome you all to the Department of Commerce for a joint workshop sponsored by the Department of Commerce and the Federal Trade Commission on online profiling.

To start out this morning’s program, we will hear some words from Secretary Daley and Chairman Pitofsky. As you all know, Secretary Daley and Chairman Pitofsky have been very involved in the privacy issue for a number of years, for a number of years now, and it’s an issue that for both of them, I know from personal experience, is very important to them.

So with no further ado, I will bring you Commerce Secretary William Daley and Federal Trade Commission Chairman Robert Pitofsky.

(REMARKS OF HON. WILLIAM D. DALEY, SECRETARY, U.S. DEPARTMENT OF COMMERCE)

SECRETARY DALEY: Good morning to all of you and welcome to the Department of Commerce or, as some of us hope it will be called in the next century, the Department of e-Commerce.

Vice President Gore asked the Chairman and I to look into the issue of profiling for our government. The reason is, as we all know, in this e-world of ours every time there is a new technology, along with all the good it may bring, consumers also want to know how it may affect their privacy.

We saw that last week. RealNetworks apologized and changed its practices after the New York Times reported it was gathering users’ listening habits without notifying them.

Obviously, Americans want to know what is happening online behind their screens when all these targeted ads pop up in front of them. The ads themselves obviously can be good.

As a consumer, if I’m online and one site has figured out that I like golf courses, possibly in or around Chicago, and I get this banner ad about a great golf weekend, that is good.

But if someone has been sneaking around me, following every click I make at every site, and they share this information behind my back without my knowing it, then I, I believe like most consumers, would be rather unhappy.

The reason people have the gut reaction they do to profiling is that they don’t know what is being collected about them, they don’t have choices, and this is not good for developing consumer confidence.

As Commerce Secretary, I can tell you that we are holding this workshop to find the facts, to see the great things that profiling can do to help consumers and companies, and companies target their online advertising and their marketing.

We very much appreciate the efforts of all of you to be here to help educate all of us. Obviously, we will all be wrestling with some extremely difficult issues. I see this as an opportunity to learn about the technology that is behind profiling. I see this as an opportunity for privacy advocates to help raise awareness about these issues which are so important to the consumers. And I see this as a chance to show us why industry leadership will be better off than Washington intervention.

In 1997, when the Internet had about one-third as many people as are connected today, the President and Vice President put forward our government’s first policy and just about any government in the world’s policy on e-commerce. They wanted the privacy sector to lead and government not to do anything that would mess up the Internet.

In our opinion, this has worked. The Chairman and I have challenged the industry to lead on privacy, and we were taken very seriously. The number of web sites with privacy policies has greatly increased. Many of the largest advertisers only place ads on web sites that contain privacy policies. And the number of companies that are signing up for seal programs, like TRUSTe and BBB Online, continues to grow quickly. Obviously, we all hope the same happens here.

I know some of you have been working on a new initiative and from what we all hear you are definitely on the right track, and you may have some announcements later on today. We all look forward to hearing them.

The fact is, as clever as industry has been to create profiling technology, it has to be as
1 clever in figuring out how to respect
2 consumers’ choices. This morning Al Westin will
3 show in a survey the majority of Americans are
4 happy about receiving tailored ads. That
5 obviously will come as no surprise to any of us.
6 Americans are the greatest shoppers the world has
7 ever seen, and if someone has a bargain these
8 shoppers definitely want to hear about it.
9 But consumers also want to know what
10 is going on inside their computers. It is not
11 Big Brother that the consumers fear any more and
12 it is not even big businesses that they fear.
13 They fear businesses that they have never heard
14 of having information about them and using it for
15 purposes that they don’t even understand.
16 If a web firm fails to protect
17 consumers’ privacy, if they fail to disclose, if
18 they fail to give consumers choice, I guarantee
19 you that governments will be forced to react.
20 Because this technology knows no borders, it is
21 far better for the market to respond than for
22 governments, not only in this country but around
23 the world, to be taking unilateral action.
24 Let me draw a picture about how
25 concerned the American people are about privacy. This

1 month we will launch an ad campaign for the
2 2000 census. By mandate of the Constitution, we
3 have conducted a census every ten years since
4 George Washington was President. But for the
5 very first time, we need to run paid ads because
6 fewer and fewer people are willing to fill out
7 the survey. If they do not mail it in, we
8 literally have to hire an army to knock on every
9 home, every residence in America, to get the
10 information required by the Constitution.
11 The big reason people are hesitant
12 about the census is confidentiality and it is
13 privacy. Americans are afraid that we will do
14 something with the information, even though by
15 law we cannot share this information that is
16 personally identifiable with any government
17 agency.
18 The point is -- and I will end on
19 this -- privacy is a very big deal for the
20 American public. We see it as essential for our
21 freedom. But the benefits of the Internet and
22 profiling are enormous benefits for companies.
23 They can do a better job of offering the right
24 products to the right customers. They can do it
25 faster and they can do it cheaper.

1 No question, knowing their customer
2 is extremely important to every company in
3 America, but so is listening to your customers.
4 And if they are telling you that they want more
5 information about profiling and more choices, you
6 need to meet those needs. If you do, we will
7 have the trillion dollar e-economy that will keep
8 America the envy of the world.
9 So I hope and I know that positive
10 things will come out of this workshop, and then
11 we can report to the American people that their
12 privacy will be protected. Once again, I thank
13 you for joining us at this workshop, and good
14 luck to all of you today.
15 Now it is my pleasure to introduce a
16 real leader on privacy issues. Robert Pitofsky
17 was appointed Chairman of the FTC in April of
18 1995 by President Clinton. Previously he had
19 been a professor at Georgetown University and
20 counsel to the Washington firm of Arnold and
21 Porter. Someone who has spent a tremendous
22 amount of time in his entire life, not only as
23 Chairman, on the issues of privacy and protecting
24 the American people, it’s an honor for me to
25 introduce Chairman Pitofsky.

3 (Pages 6 to 9)
concerned about seeing to it that this marketplace achieves its full potential. We are aware that the reason people give who are not currently engaged in purchases online or who limit their purchases is that they do not think it's a secure environment, and we must take that into account.

Today we focus on a new aspect of the collection of information from people. This is a collection by firms that have no direct relationship to the customer and where the customers have no reason to believe that information is being collected. An example: If you were surfing the Web and you come across a web page and there are some ads there, information is collected that that's an ad that you are exposed to, that you saw, and information is collected from which people draw inferences from this information and tailor future ads to the supposed preferences of the viewer -- all this without the knowledge and consent of the person who is doing the viewing.

Not only do they not have notice or an opportunity to opt out, but they don't even know it is going on. That seems to me troublesome and therefore requires careful concern and careful review by all of us.

Maybe this is a good thing for consumers. It might be. We are not opposed to target marketing if the consumer remains in control of the information that is collected. Therefore, we want to learn more so we see what the possible problems are, we know what the virtues are of this technology, and we want to learn more.

That is the occasion for the workshop that we are conducting today. Our goal is to develop consumer confidence and balance the virtues and the possible problems of this kind of online marketing.

I was pleased to learn just in the last few days that leaders of industry and online privacy have agreed to provide consumers with more control in the creation of online profiles. We have had good experience to date with self-regulation in other areas of online commerce and here as well. So I look forward to learning the details of this proposal and seeing the extent to which

MR. SWIRE: Good morning.

What I'm going to talk about in my brief remarks today is an attempt to put this profiling workshop in context with some other recent privacy developments and try to define this term "online profiling" for our use today, and then briefly preview the three panels.

I think when historians, if there ever are any, of the privacy area in American law and policy look back on when privacy took off, the last few weeks may be a period that they'll look back on as an historic change in how the United States government and its people have looked at privacy. Three weeks ago the Federal Trade Commission made the final regulations for the children's online privacy area. In the last few weeks Congress has been finalizing in the financial services area an historic change that will have pretty much all of the fair information practices built into the financial services modernization that is going to go forward. There will be new notice rules and choice rules, access and security relating to financial services, and new enforcement provisions by all the functional regulators.
Then, ten days ago, President Clinton in an Oval Office ceremony announced sweeping medical privacy regulations that will require patient consent for your medical information to be used in a wide range of circumstances. So as we think of some online initiatives, financial services, medical, we see a lot of things happening right now related to privacy, and today's workshop looking at online profiling continues that trend. This workshop today was called for by Vice President Gore. He invited the Federal Trade Commission and the Department of Commerce to move forward to try to study the phenomenon of online profiling and try to see if there were any appropriate initiatives from the privacy, if possible, to have a better way of handling personal information.

In thinking about how to define "profiling," I'd like you to consider two hypothetical companies whose names I can use in public because I checked ahead of time and they have not been used. We have two companies. One is Sellstuff.com and the other we'll call Bannerad.com. To define online profiling, I think much of the attention today has been on the Sellstuff.com's of the world, what you might call first party web sites. So that means I go online, I go to Sellstuff.com, and what are the rules going to be about how Sellstuff handles my information? What we've seen is a tremendous and historic self-regulatory effort in this area. TRUSTe is here today, Better Business Bureau Online. Other groups have been working with industry to come up with a set of principles and a set of practices that make sure information will be handled well when you go to Sellstuff.com. That's the company that you thought you were dealing with.

Today the focus is on something slightly different, on what you might call third parties that are at a web site. So now I go to Sellstuff.com and there's a whole series of ads up there. One of the ads might be from Bannerad.com, a company maybe I've never heard of before, and there are various ways that Bannerad.com can collect information about me while I'm surfing, and that's the focus of today's workshop. Why is profiling different? Why is it different when Bannerad.com is selecting information and using it than when Sellstuff.com is? I think the first point is that many people don't realize that Bannerad.com is collecting that information. Many people might guess that Bannerad.com will collect information if you click on a site. You then choose to go to that site. You go to see what the ad takes you to. You expect certain things to follow from that. But almost anybody, except the experts in the field, is surprised the first time they realize that, they go to Sellstuff.com and information about that transaction is going to somebody else, is going to Bannerad. And that surprise leads to a question of what will be done next.

The concern that we have for this online profiling, for the activities done by Bannerad.com, is that there is a lack of transparency on the who and the what of the transaction. On the who, surfers don't know who is third party who's collecting information, a company they've never heard of. Surfers also don't know the what, what about them is being gathered.

So that we talk in the first session today about cookies and other techniques that help gather information, many times information that we applaud. But for now let's point out how little even a sophisticated surfer typically will find out by looking at those cookies. If a sophisticated surfer checks for the cookies and gets an alert, they'll learn the name of the company that's doing the collection and they'll also learn the expiration date, which I usually set for some number of years after the computer will be junked. So again, that's all you'll find out if you do your cookie alert: the name of the company and some distant date of when the cookie will expire. Up until today's efforts, until what I hope we'll be hearing this afternoon, the surfer would not usually learn more about the what, nor about what kind of data is being collected, and under what terms and conditions. So what we see then as a central issue is the concern about transparency for the Bannerad.com collection. With that, let's preview what the three panels are today and some of what we hope to
1 accomplish. The first panel today tries to
2 explain and explore these third party
3 technologies, what the Bannerad.com's of the
4 world can do today and what they're likely to do
5 in the future.
6                The second panel turns to the
7 benefits and risks of these new technologies and,
8 as Secretary Daley and Chairman Pitofsky said,
9 there are clear and fantastic possible benefits
10 from the ways information can be used online.
11 From the seller's side, it can mean matching a
12 product with the products the customer wants, and
13 the same from the buyer's side, that you'll see
14 just the things you're most interested in in life
15 and not engage with the things that you're not
16 interested in.
17                But there's concerns about the risks.
18 You hear this talk of -- one conversational
19 technique I've heard often since I've come to
20 Washington, they'll say:  Well, let's take that
21 offline.  Let's not do it in front of everybody.
22 Let's go off to the side and offline and discuss
23 what's happening in a more private setting,
24 things that we don't expect the whole world to
25 know about for the rest of our lives.

Page 19

1 When you are online in your surfing,
2 sometimes you think you're offline in that
3 conversational respect.  You don't necessarily
4 expect every last detail of what you're doing to
5 be exposed to lifetime scrutiny in some database
6 from a company you might not have heard of, in a
7 way you haven't perhaps seen.
8                That sense of thinking you expect a
9 certain degree of privacy and then being
10 surprised that somebody you never heard of has
11 all this stuff about you, that's a concern that
12 resonates with Americans.
13                One of the most compelling of the
14 polls on privacy came from a Wall Street Journal-NBC poll
15 earlier this fall.  It asked Americans:
16 What do you fear most in the coming century?
17 They gave a list of about a dozen horrible
18 things: overpopulation, terrorism, global
19 warming, many other things.
20                The answer that came in highest,
21 first or second for 29 percent of all respondents
22 was loss of personal privacy.  No other topic --
23 terrorism, global catastrophes, and nuclear harm -- none
24 of those rose above 23 percent.  The
25 biggest fear, according to the Wall Street

Page 20

1 Journal poll, was loss of personal privacy.
2                It's in that context that society is
3 talking about what the structure will be going
4 forward.  That leads to the third panel, which
5 has to do with the search for solutions, what
6 ought to be done.  As announced in Friday's New
7 York Times article, there appears to be exciting
8 progress toward having some new and innovative
9 self-regulatory solutions in the online profiling
10 space.  We look forward to seeing the details of
11 that and we hope they're as good as they seem to
12 be from the initial reports.
13                So with that, I'm going to close.  On
14 behalf of the administration, I commend the
15 Federal Trade Commission and the Department of
16 Commerce for their leadership on these issues,
17 and I thank all of you involved in today's
18 workshop for helping us achieve progress towards
19 a more transparent and fair treatment of personal
20 information on the Internet.
21                Thank you.
22                (Applause.)
23                SESSION I:  ONLINE PROFILING TECHNOLOGY
24                MS. BURR:  Thank you, Peter.
25                I'd like to invite the participants
MathLogic, Inc., an integrated digital marketing solutions provider.

REMARKS OF DANIEL JAYE, CHIEF TECHNOLOGY OFFICER, ENGAGE TECHNOLOGIES, INC.

Mr. Jaye: Thank you, Becky, for your introduction and for your efforts on behalf of the Department of Commerce to find the right solution that benefits both consumers and corporate marketers.

I am pleased to stand before you once again to discover our common goals, to respect the rights of consumers with regard to online privacy while simultaneously pioneering an industry that benefits all involved. I'm here to inform all interested parties about online profiling technology and its implications for consumers.

Since I founded Engage in 1995, our organization has been completely committed to providing a novel and valuable technology, a technology that enables the creation of online profiles while keeping the identity of the consumer protected and unknown to us.

Some of you may be asking, what is online privacy -- what is online profiling, rather, and what are some of the benefits? Profiling is the collection of non-personally identifiable data by Engage about a browser that enables web sites to customize ads and-or content. Profiling yields more effective marketing for advertisers and web sites, that will increase the advertising dollars spent on the Internet, which will create more free and subsidized Internet services for consumers. It's a very clear and straightforward value proposition.

Why do the advertisers need online profiling and effective marketing? Because the investments that are happening in the Internet today will have to show profitability at some point, whether it's in two months, two quarters, two years. At some point, the investments that are being made are based on the promise of being a very effective media for communicating to consumers.

Web sites have two critical needs to each this. One is to be able to measure and information its audience, being able to understand how many unique visitors have reached that web site, and what are the special interests of those visitors so that the site can be made more compelling. In addition, they need to make sure that the content and ads that are shown to those visitors are relevant and effective.

Next I'm going to talk a little bit about how third party ad networks work and exactly how they work and how important they are to being able to provide advertising infrastructure to the thousands of sites on the Internet. It begins with the web browser. The web browser, when it visits a publisher web site, for example a web site like Lycos or Yahoo, makes a request to that web site for a web page.

When that web page comes back to that web browser, it is displayed, but inside the web page there are instructions that tell the web browser to get an ad from an ad network. That browser then makes a request of the ad network for the ad to be displayed, and the ad network then selects the appropriate ad based on a number of different considerations, and that ad is then displayed inside the web page.

At a future time, if the consumer clicks on that ad, the web browser then sends an instruction called an ad click to an ad network. This is important because the web site doesn't actually know which ad was selected because the ad network made the decision.

So the ad click goes to the network so that the ad network can report on what percentage of visitors clicked on the ad as well as being able to send an instruction called a redirect to the browser, so that the web browser eventually gets the correct web page, whether that be Procter and Gamble, IBM, or some other advertiser. Then that advertiser's web site then returns the correct web page to the consumer.

You can see that in this interaction there are a number of different steps. The way in which this information is delivered up to the web site and back to the web browser relies on a return address mechanism called an IP address that many of you have heard of. It is critical that the IP address, which is an inherent part of the Internet, be transmitted to the ad network so that the ad network knows to which computer to return the ad.

What types of information do ad
networks, the ad networks for example that use Engage's solution, use? Our solutions are based on non-personally identifiable information, which we classify under two broad categories, and management and reporting data. This is data that is used to effectively run the ad service to be able to report to an advertiser how many ads were shown, how many visitors saw those ads, what percentage of those visitors clicked on the ads.

Then the second area is what we're terming ad delivery data. These are the types of data that are used to determine what ad or what content to show. In essence, ad delivery data is ad management and reporting data that is used for profiling.

When we use this type of information for ad delivery, it is typically used by ad networks to understand what the visitor wants, without knowing specifically who they are. The premise when I founded Engage was that on the Internet you didn't need to know who the consumer was to be able to deliver a relevant and effective experience. We think that this is actually an enhancement of privacy over traditional marketing methods that require identifiable information, like name and address.

Typically this type of marketing is implemented today using web cookies, a term some of you may be familiar with. Briefly, a cookie is information that is sent from a server to a browser and that the browser then sends back to that server when it returns to that web server when it requests future web pages. Once again, it goes back to the specific server that originally sent the information down to the browser.

Typically, these are used for three purposes. First, remembering what was done before. Sometimes this is called, technically, state management. Second, shopping carts, the ability to remember what purchases you have made during a shopping visit, being able to figure out what ad was displayed to that person, so when they click on an ad they go to the right advertiser's web site. Another example might be a sequencing of messages, for example telling a story. These are all examples of state management.

Remembering whether a visitor was already counted is another critical use of cookies. Advertising spending is largely gauged based on unique visitor counts. Being able to determine how many unique visitors to a web site or a portion of a web site requires the ability to identify anonymously, or non-personally identifiable, rather, an individual so that we can determine whether or not that individual was counted previously.

Then the final example of what cookies are used for is to create and access online profiles. At Engage an online profile contains a collection of non-personally identifiable information about the consumer's preferences and interests. This is inferred at Engage from the types of content visited.

At Engage our technology doesn't care what page somebody went to. What we care about is what types of content somebody went to. So it involves a non-personally identifiable number or identifier -- an example is shown on the screen -- and the collection of interest scores scaling from zero to one for that visitor or that browser. The higher the score, the stronger the interest.

The way in which this is built -- let me take you through an example. If a user visits a web site, for example Surfaround.com, he'll receive this anonymous identifier or this non-personally identifiable identifier, 23987 etcetera, and they have a score for money and finance interest, sports interest, and automotive interest based on their entire activity at that site.

Now they visit another site that is part of the Engage network -- and once again, only sites that have a business relationship and a set of contracts that cover in addition privacy policies provide information for this type of profiling at Engage. When they go to Investinstocks.com, Engage will understand, not that they went to that specific site, but rather what is important, that they have a stronger interest in money and finance.

If they visit another site that has a relationship with us, like Golfing, at that point their sports score will be enhanced and so then we will also develop a score, for example, that would indicate a level of interest in golf.

Then finally they visit an automotive site. Automotive content will then impact the
On-Line Profiling Workshop

November 8, 1999

1 automotive interest score, as well as perhaps a
2 more detailed score, the fact that this person
3 might be interested in buying the car and might
4 be receptive to advertising related to carburetor
5 systems.
6
7 What would it be used for? We talked
8 about today the example of banner targeting,
9 delivering once again golfing ads to a person
10 with golfing interests. But in addition it can
11 be used to navigation and web surfing easier, for
12 example moving content of interest to that person
13 to the top and obvious part of the page instead
14 of burying it three levels down on the web site.
15
16 Some of the things that we do at
17 Engage are areas that we think are important for
18 the industry, and some of these areas are
19 practices that we have implemented based on
20 conversations over the past several years with
21 the Department of Commerce and the Federal Trade
22 Commission. They have been very helpful in
23 providing us feedback and suggestions, and we
24 have tried to address these where we can.
25
26 First of all, we have been focused on
27 non-personally identifiable Internet marketing
28 since we were founded. In addition, we have a
29 technology called dual-blind, which is the
30 ability to add an additional layer of indirection
31 to non-personally identifiable numbers. We have
32 had contracts with our web sites that require
33 them to post a privacy policy since 1997.
34
35 We have been providing an opt-out for
36 the information that we gather, even though it's
37 non-personally identifiable, once again since
38 1997. In addition, there's a lot of information
39 that we don't need for our business, so we don't
40 retain it. So for example, we don't keep IP
41 address information at a detailed level. We
42 don't keep track of the specific URL's or pages
43 and the content and which visitors visit that
44 information, and we don't track sensitive
45 interest categories, such as medical information,
46 local content interests, medical interests,
47 etcetera.
48
49 Then finally, we make sure that the
50 data we have in our cyberdata center is
51 structured so that no combination of this data
52 can be reversed back to an individual. Sometimes
53 this is called triangulation. For example, we
54 don't keep the combination of zip code and the
55 exact date of birth of the individual, because in
56 many instances that can uniquely identify an
57 individual person.
58
59 Very briefly, our dual-blind
60 architecture is something that allows an ad
61 network that uses our solution to pass this non-
62 personally identifiable information. We then can
63 pass back to that ad network a list of types of
64 ads that are the relevant ads for that visitor.
65 It uses multiple levels of identification so that
66 we can ensure that no ad network or site that
67 works with us can ever correlate data with any
68 other site.
69
70 Briefly, our privacy formula can be
71 summed up as the fact that we use non-personally
72 identifiable online profiling combined with a
73 requirement for notice and opt-out capability for
74 consumer choice and contractual enforcement with
75 our web sites that requires that they post
76 privacy statements and a link explicitly to our
77 web site privacy page at Engage.
78
79 We also work with third parties like
80 TRUSTe for certification of our practices and FTC
81 oversight is invoked.
82
83 In summary, we believe that for other
84 businesses there are business models that may
85 give personally identifiable information and they
86 may be appropriate for other businesses that have
87 a direct consumer relationship and that follow
88 fair information practices. But at Engage we
89 believe that for us non-personally identifiable
90 information-based profiles balance consumer and
91 industry interests.
92
93 We also believe that as the industry
94 matures the business models and solutions will be
95 developed that will benefit both consumers and
96 marketers. For example, the work that is going
97 on with P3P as one potential innovative
98 technology, as well as other developments, will
99 cause rapid changes that we believe will help
100 everyone.
101
102 Thank you once again.
103 (Applause.)
104
105 REMARKS OF MARTIN SMITH, CHIEF TECHNOLOGY
106 OFFICER AND VICE PRESIDENT, MATCHLOGIC, INC.
107
108 MR. MARTIN SMITH: Good morning. I'm
109 Martin Smith from MatchLogic. Let me give you a
110 little bit of background. MatchLogic is a full-service
111 digital marketing services company based
112 in Colorado. We work with quite a number of the
113 leading advertisers in the Fortune 50 and also in
the commerce and marketing space. Our products and services have been developed to support multi-product large advertisers in delivering web service.

We were acquired in 1998 by the Excite organization and were subsequently acquired in 1999 by At Home and remain as a subsidiary.

MatchLogic's service offering breaks into a range of digital solutions, primarily memory management, database and direct marketing services working, as we mentioned, with multiple sites and with advertisers and their agencies.

With regard to the subject of today, on the online services, we deliver targeted advertisements based upon identification of demographic segments, so broad age, income, gender lines, geographic location, country, state; then variables peculiar to the industry that we work in, such as connection speed. We have a non-intrusive way of calculating the connection speed to provide the optimal experience for the user.

We also have segments that deliver advertisements pertinent to somebody's buying propensities. One of the earlier keynotes mentioned the fact that the right offer to the right person or to the right segment is something that is of value to the consumer.

The second part of our business is targeting e-mail messages. MatchLogic has invested significantly in media to acquire customers through sweepstakes and through registrations. These are all opted in and consumers on every communication have the opportunity to opt out, not to receive communications on specific subjects, and also to receive communications about subjects they are interested in.

Finally, and again a critical component to identifying whether and how this media can be used effectively, is the production of consolidated reporting. Dan mentioned the use of a cookie and the importance of the cookie in providing reporting that is ubiquitous across different web sites and providing consistency of measurements.

One of the largest issues that we have in terms of standardization and measurement is the fact that sites count differently, what do we have by using the cookie and what's called a "ping," which I'll come to? We're able to measure ubiquitously and anonymously across the sites and produce aggregated reporting that our advertisers can then evaluate the success or otherwise of the media, of the site.

Our business model breaks into four component areas, all requiring different elements of data. Campaign management requires highly aggregated information. E-mail services requires opted-in information and a delivery address through the e-mail address and also for prizes and so on a land-based address. Database management services is the computer production capability of managing large transactional databases. And then the optimization area, which is the area we're focused on today, which I will drill into.

Our optimization model delivers to four key areas: the first area being predictive modeling; the second area being media optimization; the third area being return on investment tracking; and the fourth area, customized reporting. I deal with those quickly.

Predictive modeling is the ability to take segments that we train -- I'll step you through the model of how that works -- to be able to make a statistical likelihood that the characteristics that that browser has relate to a specific segment.

The second area of media optimization is, through the use of the cookie, how specifically and what specifically is served to that browser. One of the biggest problems from a media point of view is management of frequency of number of times an advertisement is seen by a browser. Management of frequency controls and the measurement of that is key for a successful and viable medium.

ROI tracking, to the keynote speech, is the ability to measure how successful an advertiser is being in a cause and effect. So as the browser comes to a particular site, do they actually complete the actions? Is the site navigating in the way that you intended to navigate? This is highly aggregated information.

A third area then is customer supporting, the ability to look comparatively at different media sites and make educated performance assessments to see whether the
advertising is truly working.

To the first point of the predictive modeling and the online profiling, why we're here today, MatchLogic's profiling system -- I'll provide you with a basic overview and then get into the data specifically that we're capturing within that, how then we generate the profiles, how we use those profiles, and the privacy issues that that creates.

What MatchLogic does is take variables from our known data set. This is not personally identifiable information. This is non-identifiable information, such as demographics, so age, income, gender. Because of the nature of the targeting, we then, before we put the segmentation in there, we actually do a preclassification. So at the point the data is entering into a profiling system it is already pre-aggregated and is non-identifiable. No identifiable data is brought across into the process.

From the segments, we're then able to look at what specifically the patterns of information from the unknown or the web surfing behavior is. From that we then train or build a model, using a combination of latent semantic analysis, linear regression, and neural network modeling.

The output of that model is then tested against the unknown segments and reapplied. From that, we are then able to statistically predict the area and the geography. So within the system, Martin Smith living in Colorado does not exist within the system, nor can it be tracked back through the system. The fact that I am a male living in Colorado is about as far as we go.

Third party ad serving is one of our primary data sources. We also capture in addition page, channel, search terms in some cases, IP browser, operating system, date and time. That information is linked by cookie, which Dan identified and showed you what that is.

That as an input variable to the web surfing behavior is encoded into a token, rather like the one you saw from the Engage model. Simply, that is a statistical value allocated to that variable. So again, we're not passing through into the modeling the specific nature of site, content of that site. It becomes a statistical algorithm.

We then take that and build our prediction model and apply that. How we use that information is in the serving of targeted advertisements. That can be segment-specific, so if an advertiser has specific geographic segments or their product or service breaks down into a number of brands or sub-brands they're able to fit, based upon the segments, the right message that is most appropriate to that segment.

That provides them with a very powerful tool to then provide optimization across the media. So if you think of the analogy, rather than buying an audience on television, where you have high potential wastage, you're able to buy an audience of the same magnitude, then segment it and optimize the inventory across a number of services or products.

The second area, second key area, is in site analysis, specifically what audience segments are producing the most significant or salient results. That provides key measurement to either customization of the site or presentation of the correct either navigation or dialogue within the site. This leads to significant improvements in performance and provides us the ability to really start to customize content that is appropriate to those specific segments.

As mentioned in the opening addresses, this then does throw up some very key issues from privacy. MatchLogic has been instrumental in a lot of the thinking from the industry point of view with regard to privacy, with regard to how we relate to our consumer.

The third party model does provide us with challenges. It is seamless to the consumer. Our focus is to deliver advertising in a totally clear way. Believe me, we would know if the adverts did not get to the page, from both the publisher and our advertisers. By that fact, we are in the background.

Our challenge is to provide notice and choice, which is part of what today is about and will be addressed this afternoon. It is also beholden to us to make sure we prohibit the linkage of personally identifiable information into the process, which is how we have architected our systems. We have also architected them to be able to preclude people...
<table>
<thead>
<tr>
<th>Page 42</th>
<th>Page 44</th>
</tr>
</thead>
</table>
| 1 that do not wish to receive targeted advertisements or to have any of their information tracked across. The next area is also to provide education. As a founding member of TRUSTe, we take that role very seriously and have invested significant dollars in supporting that, and to provide choice to the consumer. Thank you. (Applause.)  
MS. BURR: Just give us a moment while we rearrange here. (Pause.)  
PANEL DISCUSSION I  
MS. BURR: Thank you. Those were very interesting presentations and I think they'll help us as we move through the day. Let me just introduce the people who are sitting up on this panel who will help us discuss the technology issues this morning. To my right is Lori Feena, who is the Chairman of the Board of the Electronic Frontier Foundation. Lori has worked for years to focus the organization with respect to participation in legislation, court proceedings, and a number of other areas in order to promote the protection of civil rights and ethics online.  
Jason Catlett is the founder and President of Junkbusters Corporation, an authority on privacy and marketing, and a frequent participant in our conversations here. I introduced Dan and Martin earlier. To my immediate left is David Medine, a familiar face to all of you from the Federal Trade Commission and somebody I've worked with for years on this issue. Next to David is Kunwar Chandrajeet Singh, or K.C., I believe, the founder of both Hyperportals and Cyberknowhow. K.C. has been involved in communications technology issues since 1979, when he was responsible for the first electronic interactive stocks and shares information and trading system. Richard Smith is an independent Internet security consultant based in Brookline, Massachusetts, and prior to that he was the President of Farlap Software for 13 years. You guys are outboarded here. Eric Wenger is the Assistant Attorney General in Attorney General Elliott Spitzer of New York's newly formed Internet Bureau. Eric also serves as the Chair of the Internet Privacy Working Group of the National Association of Attorneys General, and Eric has also been active with David and with me in a number of these panels for years. Finally, on the end is Danny Weitzner, the Technology and Society Domain Leader for the World Wide Web Consortium. I love these titles. He is responsible for developing Internet technology standards addressing many issues, including user privacy. Before joining W3C, Mr. Weitzner was co-founder and Deputy Director of the Center for Democracy and Technology, and after a two-year stay in Boston we're very happy to have Danny located back in Washington. He's been very important to us in all of these. The way that we will proceed is familiar to those of you who've come to these workshops before. This is a slightly more formal setting than we've had, but obviously needed to accommodate the interest that we have in it. But generally, we've asked the panelists not to make prepared statements. We really intend to have a conversation, and we will proceed on that basis. David, do you have anything you want to say?  
MR. MEDINE: No.  
MS. BURR: Okay. And just to remind you all, as we have said before, there are cards on the sides of the auditorium and your questions will be brought up to us.  
MR. MEDINE: I just wanted to mention that the opportunity for people to submit comments in writing to us, which started with the publication of a Federal Register notice, will continue until after this workshop, until November 30th. So if there are issues that arise today during the discussion that people would like to comment on in writing, please submit those comments pursuant to the procedure outlined in the Federal Register any time up until and including November 30th.  
MS. BURR: Thanks.  
OKay, we've heard about MatchLogic's technology and Engage's technology. Before we get down to the policy issues, I'm curious about other technologies that are used by online profiling companies to collect information about... |
consumers. Can either Martin or Dan or both of you talk just briefly about other, or Jason or anybody else at the table, briefly about other technologies that are out there and perhaps differences significant for privacy purposes?

MR. MARTIN SMITH: I'll take that one as I don't have to speak ill of any competitor. Dan in his talk today said that Engage's profiles are not personally identifiable. His company's made a commitment to not personally identifying these profiles. However, obviously these profiles could be by some other company that had not made such a commitment become personally identified.

The dangerous thing about these profiles is that they amass a huge amount of information. Dan gave you three examples, banking and a couple of other examples. But the interest vectors are typically several hundred fields wide. That represents an enormous profile, which can be collected over a period of years and then subsequently identified. That is where they become so unfair.

There are many companies out there who will gladly identify a profile for you based on a cookie. Two leading companies in this area are Navient.com and Cogent.com, and I don't believe that they're represented here. So I just came from Adtech last week, the leading conference in this field, and the explosion of technologies for adding identity of the offline world to online data is really one of the hottest issues in that industry.

So really, we're not seeing the entire picture. If we think this is 100 percent ethical and this has been identified, that is where the money is and that is where the industry is going.

MS. BURR: K.C.?

MR. SINGH: I'll take that. Basically, we are only talking about containing the loss of privacy here. There is going to be some loss of privacy. Each wave of technology brings with it the inevitable dilution of privacy. When the written word was invented, so was the possibility of somebody actually taking your letter and intercepting it. So I am sure that all the companies that are involved in profiling realize that profiling is also vital for the growth of the Internet and will take appropriate measures. The problem, as my colleague just mentioned, is that there are companies who would not, and especially companies outside the country. One of the main concerns that I have is that if the control of Internet were to go out of these shores, then most of what you are talking about here would be hypothetical.

MS. BURR: Lori.

MS. FEENA: I think actually that is a very good segue. First, the delineation between online profiling and offline profiling is a false one. We really can't assume that the bricks and mortar world is no longer part of this discussion. The bricks and mortar world of real life stores and situations where you aren't actually touching a keyboard also collect data that goes into this profile.

As you drive through the easy-pass or whatever, the toll booth convenience payment systems are, they collect data. You don't have to be online to do that. As you shop in the grocery stores, you are building a profile. They're not just simply trying to figure out an easy way for you to clip coupons. You're building a profile.

So the discussion of online versus offline is really where the technology is going. We are all connected on a network, whether it's a bricks and mortar store or whether you're at your keyboard at your desktop. I think the profiling demonstrations that were given here talking about the online world are also -- very appropriately can be applied to the offline situation as well.

MS. BURR: Danny.

MR. WEITZNER: Thanks, Becky. I think Lori just explained to us why President Bush avoided those supermarket scanners. While we are sort of pushing on some of the distinctions here --

VOICE: We can't hear back here.

MR. WEITZNER: Can you hear now?

VOICE: No.

MR. WEITZNER: Is the microphone on?

VOICE: No.

MR. WEITZNER: Can you hear me now?

Yes, you can hear me.

While we're discussing some of the
On-Line Profiling Workshop

Washington, DC

On-Line Profiling Workshop

November 8, 1999

1111 14th Street, NW, Suite 400  800-FOR-DEPO Washington, DC  20005

Alderson Reporting Company

14 (Pages 50 to 53)

1 distinctions here, I just wanted to also suggest
2 that we should think about what we're really
3 talking about with profiling. Clearly, we've
4 heard a lot about profiling for the purpose of
5 delivering advertisements. Certainly in the
6 direction that we see the World Wide Web
7 technology evolving, we're going to be having
8 profiling for many other purposes, in many cases
9 not really intended to be disguised from the
10 user, but profiles that will be largely hidden
11 from the user, profiles that will help web
12 servers recognize that a user is accessing the
13 web site from a cellular telephone with a little
14 four by four screen instead of from a desktop
15 computer, profiles that indicate where the user
16 is physically located in order to deliver the
17 appropriate information, and I think all of these
18 are very exciting services with potential for
19 great benefit for users all around the world.
20
21 But we should certainly recognize
22 that there's going to be an explosion of profile-based
23 information, both provided by users and
24 created by a whole variety of services, with
25 advertising profiling really probably only the
26 tip of the iceberg.

I would just add also that the
27 gentlemen at the end of the table have been very
28 clever at working with really what is widely
29 recognized as entirely inadequate technology,
30 namely cookies, to do all the profiling and in
31 some cases to provide a level of security and
32 privacy, which is even harder in some ways. I
33 think that we're going to certainly see on the
34 web the rise of much more structured information,
35 information that carries with it much more
36 meaning, that identifies certain information as
37 credit card numbers or as a name, etcetera.
38
39 So the good news and the bad news is
40 that this technology for profiling purposes is
41 going to become far more capable than it is
42 today.
43
44 MS. BURR: Does the use of this
45 technology depend on a persistent IP address? In
46 other words, people coming through AOL get a
47 differently generated IP address whenever they go
48 out on the web. Are you able to use this
49 technology for that segment of the web users?
50 And if so, could you explain how?
51
52 MR. JAYE: This microphone is
53 working? Good.

Briefly, with regard to IP addresses,
1 the technology doesn't really care very much
2 about IP addresses. It is important that between
3 one page request and the reply to a page request
4 by the server that the network is able to return
5 the page from the server to the correct browser.
6 But over time persistent or static IP addresses
7 are by no means acquired and in fact are not the
8 norm on the Internet at this time.
9
10 Static or persistent IP addresses
11 generally are very rare and becoming rarer,
12 simply because of the exigencies of managing the
13 assignment of IP addresses between different
14 computers.
15
16 MS. FEENA: Just to further note on
17 that, the IP address is simply one way to create
18 a global user ID. This is a new term that I
19 think we are all going to become much more
20 familiar with. Some people call them GUID's.
21 Essentially, there needs to be some identifier to
22 create a profile to continue to aggregate
23 information about the identity or the person
24 profied. So there's generally a global user ID,
25 in some cases -- well, it's true. You can create
26 many different ways to put walls between the ID
27 and who the person is, but the reality is there's
28 a central identifier.
29
30 In many cases, databases are not
31 always aggregated according to one ID. There are
32 many different technologies, as we have seen
33 today, used in the offline world to aggregate
34 information and create a profile about a person
35 from many diverse databases, and frequently they
36 aren't joined together with perfect knowledge.
37
38 A lot of information, as you have
39 seen -- how many of you have gotten -- I happen
40 to be somebody who's divorced and I still get
41 information connected to me about my ex-husband,
42 although I've been divorced for many years.
43 Sometimes they take databases and they realize,
44 well, these two people used to be married, they
45 must still be married, and this address change
46 must be applied globally to this person.
47 Well, it isn't because I told them
48 so. It's because they had one database here and
49 one database there and they decided to link this
50 and put that in my profile, too.
51
52 So one of the things that we have to
53 worry about are some of the data movement and
54 data management tools that are used to better
On-Line Profiling Workshop November 8, 1999
Washington, DC

Page 54
1 connect diverse pieces of data and databases
2 together under a unique ID, whether it be
3 attached to, in the online world, your IP address
4 or your masked address or identifier that's been
5 created for you, this unknown person.
6 Regardless, we have a great deal of
7 technology and background in technology that
8 connects databases of information about you. So
9 frequently in history we've talked about this as
10 far as the social security number has frequently
11 been used as your global user ID, and many
12 different databases get linked together under
13 that.
14 So as we move forward, we have to
15 figure out how is this going to translate in the
16 new complete network world where everybody has a
17 database about your transactions and they start
18 to get aggregated.
19 MS. BURR: I can tell that Dan has
20 something he wants to say and I will let you have
21 your response. But I just want to add to it.
22 Are you using external databases with
23 personally identifiable information and how would
24 you link that up to the non-personally
25 identifiable profiles?

Page 55
1 MR. WEITZNER: Thank you. That
2 actually goes back think to the very first
3 question. Lori brings up a very important point,
4 which is the risks of globally unique
5 identifiers. This has received a lot of press in
6 the past year regarding a couple of major
7 technology companies that use globally unique
8 identifying technology, not in our space, but a
9 noted operating system vendor and another
10 computer chip vendor.
11 Globally unique identifiers are a big
12 concern because they are potentially personally
13 identifiable information, because once a globally
14 unique identifier has been associated with a name
15 and address then effectively it's contaminated.
16 The point we would make is that
17 cookies, which is the technique that companies
18 are using, as opposed to IP addresses, are not
19 globally unique. By definition, they are domain
20 specific. So by definition, they are domain
21 unique, not globally unique, and that's
22 inherently -- it's a very, very important
23 distinction.
24 The second distinction is that IP
25 addresses, because they're not persistent, are

Page 56
1 also not -- because they're dynamic and
2 constantly change, also are not relevant globally
3 unique identifiers in their current form under
4 the current IP address standards. So those two
5 points.
6 Then on the marrying of the different
7 databases, I think, focusing a little bit on some
8 of our businesses that are here today talking
9 about online profiling, it's true there's an
10 awful lot that's happening in the industry
11 offline as well as online. But when we talk
12 about online profiling, it is not possible to
13 link an online profile with an offline profile
14 unless at some point the consumer has filled out
15 a form and provided their name and address to
16 someone.
17 That is the linkage that's required.
18 Our position is very formally that any collection
19 of identifiable information needs to be done
20 using fair information practices with notice,
21 consent from the consumer, et cetera.
22 MS. BURR: Thank you.
23 We have a lot of requests on the
24 table here. Eric, I know you had something.
25 MR. WENGER: I'd like to thank the

Page 57
1 Department of Commerce and the Federal Trade
2 Commission for inviting me here. I also have to
3 start off with my standard disclaimer, which is
4 that my views don't necessarily represent those
5 of my office. I'm sure that the same goes for
6 many other people.
7 But I think one of the interesting
8 things that we've heard today over and over again
9 is that consumers don't necessarily realize that
10 they're dealing with third party companies that
11 are dealing ads to them and collecting
12 information.
13 But I think even more interesting or
14 perhaps more interesting is the idea that the
15 recent stories that have involved RealNetworks
16 and InfoB and Microsoft, while not strictly
17 relating to online profiling or not always
18 relating to it, but the use of GUID's and things
19 that Lori mentioned, demonstrate that many
20 companies don't necessarily know what they're
21 doing with the information that they're
22 collecting, and that they could stand to take a
23 closer look at the accuracy of the privacy
24 policies that they're posting on their web sites
25 before Richard Smith does it for them.
I think that it's also important to recognize that from a legal perspective, with the exception of the children's rules and the Children's Online Privacy Protection Act, there are not really requirements that companies tell consumers what they're doing with the information that they're collecting. Having said that, if a company does post a policy, then we know that the Federal Trade Commission and other law enforcement agencies, including my office, are going to be very interested in making sure that the policies that they post are accurate. I think that there is also some good news with regard to the stories that we've seen recently. The good news is that the marketplace clearly puts costs on those who fail to propose privacy policies. We've seen that in the increasing number of web sites that have posted privacy policies in the last year or two after the Federal Trade Commission and the Department of Commerce have thrown light on the past inadequacies in that area. We also see that companies who have bad privacy policies that are exposed quickly change them because they don't want to face a public that has concerns about dealing with those companies. The Attorney General along with the Federal Trade Commission and along with the Department of Commerce favors the continued development of self-regulatory mechanisms. But I have raised in the past at other workshops some concerns about whether in this marketplace, where there are a lot of small companies and low barriers to entry, self-regulation can reach all those companies. I want to add another concern here, and I think this is something that has been expressed, is the concern that if consumers don't realize the companies with whom they're dealing, then self-regulation may be a flawed model, because if they don't know that they're dealing with a particular company how can they be expected to opt out of the databases. That's the challenge that goes to this industry now. I read with great interest the proposals that they're putting forward about opting out and I think that's going to be the biggest challenge, is letting people know who you are and what you do so that they have the opportunity to exercise in a meaningful manner the opportunity to opt out. MS. BURR: Can I follow up, Eric. We've heard both from MatchLogic and Engage that they are not collecting personally identifiable information and not matching that information up with individuals and not triangulating to get that information. They also talked about a commitment to do that. In the absence of a relationship between the data gatherers and the data subject, how is that commitment enforced and are we comfortable that that is an enforceable commitment? Do you want to respond to that before we go on? MR. WENGER: I think that's the challenge for law enforcement and for consumers as well, for them to have some sort of faith in the idea that the promises that they're going to get from Engage and MatchLogic are going to be followed or that there aren't other companies that don't follow policies that are as privacy friendly as the ones we've heard about today. That's going to be a difficult thing. I think that the key for them if self-regulation is going to work is to provide as much transparency as possible to the consumers so that they know who they're dealing with and also for them to engage the services, I guess, of companies that can perform audits for them, so that they can certify that they are following the policies that they say that they're going to follow. MS. BURR: We have a lot of requests. Richard, then K.C., then Jason and Lori and then Danny, in that order. MR. RICHARD SMITH: Yes. My concern here with right now this talk of anonymous profiling is the fact that to identify somebody is very, very easy at some later date. Jason made this point a little earlier, but the fact is you collect all this data and you want to match it up to a cookie; well, all you do is you send out an e-mail message that sends back both the e-mail address and the cookie. So it's basically pretty trivial for them to do matching e-mail addresses. So you know, if they want to put it
in blood here that they'll never do these kinds
of matching, that's fine. But business realities
make me concerned here. I mean, DoubleClick is
looking, is moving in the direction of matching
up online profiles to people, and to expect the
competitors not to go down that route if they're
being beat up in the marketplace is a bit much.

Also, companies are being bought and
sold all the time and promises today don't really
necessarily have anything to do with two or three
years from now. So the collection of these
massive, of these very large online profiles is
eminently matchable up with personal information
down the road, and that's the real concern here.

MS. BURR: K.C.

MR. SINGH: Thank you.

Firstly, the triangulization is
inevitable. We have to assume that, because all
the business sits on thousands of geo-commercial
faults and there's upheavals going all the time,
and to say that one company is going to carry on
that policy is just impossible, because the
policy may not work with the new configuration
later.

But this has been all very, very
negative. Let me just add very, very quickly a
small positive point, and then we can go back to
the negative side.

(Laughter.)

Mr. SINGH: The positive thing, I
mean, we create vertical portals focused on a
single subject at a time. Just to give you an
example, if somebody is buying a book, say
"Catcher in the Rye," I'd like to make available
to him or her at the same time the information
that there are half a dozen chats going on about
"Catcher in the Rye" or related to that subject,
should he or she be interested in them. That's
very useful information and that's time-saving
and relevant.

The other thing is, a little googly,
as they say in cricket terms, is that the
consumer has with him that we don't realize yet,
we're in the early stages of computers. It's
like the time when there was just one TV in a
house. There is going to be a different computer
and thus a different hard drive in numerous
different places, workplaces, leisure places,
cars, in pockets, and so on.

All the companies what are sending
even called behavioral science. The icon for
that is the Skinner box, invented by a
psychologist called B.F. Skinner, where you have
a rat in a box and they flash a red light or a
green light and they give the rat an electric
shock or a piece of food or something.

Now, that is basically what is being
done now to consumers. Instead of the red light
and the green light, we have the choice of
tens of different ads to choose from based
on the models that have already been built, and
the response that the rat gives -- I'm sorry, the
consumer gives -- is whether to click or not.

So every time you see an ad, you are
being experimented on, and you see a lot of ads.

On average, a consumer sees about 5,000 ads per
year. Each bit of data that's collected with
that goes into your profile, building these huge
profiles, which are totally unacceptable. They
are unfair practices and they should be stopped
immediately.

Ms. BURR: Let me just follow that
up, because I think that's a little bit different
from what we heard this morning, unless I missed
something. Certainly it's true that information
is being collected about what users want, like, and I think we'll hear a little bit later on that in fact users really want that personalization and value it. But every time I see an ad it's not clear to me that anybody actually knows anything about me at this point, because my computer at home is used by my husband, who likes motorcycles, and my 14 year old son, who likes God knows what. So anybody who's using information about the cookies on my hard drive at home is getting a pretty confused picture of what the world looks like.

MR. JAYE: Just two real quick points. On that specific issue, the issue of multiple users sharing the same computer, in certain cases, depending on what browser you're using, people are more and more personalizing their browser because they have their favorite home pages, they like to see their news a certain way. When you use those types of techniques to personalize your computer, generally the computer manages cookies separately, so the profiles are separate. But in the case where it's one where that isn't happening, then what you end up with is what we would term a household profile, which, from a positive standpoint, it might be somewhat confused, but at least you know that somebody in the household might be a golf fan and perhaps a spouse wants to buy a present for their spouse, etcetera. So it may not necessarily be ineffective.

I did want to just point out one thing. The comment was made about easy to match a person's name and a cookie and the comment about easy to match, you just send an e-mail address and it sets a cookie. The whole point is that e-mail addresses are personally identifiable information. When we say we're non-personally identifiable, we've already assumed and said we don't have the e-mail address.

MR. RICHARD SMITH: You can buy the e-mail address from a mailing house.

MR. JAYE: No, we have no way to match it. The example I'm going to --

MR. MARTIN SMITH: The company who buys you will.

MR. JAYE: The standard is not that we won't violate privacy or we won't figure out who the consumer is; our standard is that we can't. Literally, if you go through our database, we can't figure out who you are, not that we won't.

MR. CATLETT: That's because your company has gone to a tremendous effort in that respect. It's actually easier to take, and cheaper, to take the route of going directly to the identity of the consumer, don't you agree?

MR. JAYE: Actually I don't, because I think that the amount of effort and time that would be spent to try to wade through all the noise of changing computers and IP addresses and networks and directories and then trying to deal with -- there is a requirement, I believe, at some point for the consumer to disclose an e-mail address or some piece of information to create linkage, and many studies show that upwards of 70 percent of the information that's disclosed is either deliberately or accidentally misleading or inaccurate.

So once again, we believe there are significant challenges to companies that try to match online and offline data. And we believe that we can deliver just as effective, if not more effective, advertising through the use of non-personally identifiable techniques.

MS. BURR: We're going to go to Lori and Danny, but I have a question from the audience for Lori and Danny, which is: How do offline data collection practices compare with non-PII profiling in terms of the privacy impact?

So in whatever you were going to say, if you could address that as well.

MS. FEENA: Actually, I think that I'll start with that. What we've seen in the online world is, because of the great deal of awareness that a consumer has that they are actually on a network when they're on the computer, there's been a higher degree of concern, and I think the programs that we've put in place -- I should also for clarity disclose that I'm also a co-founder of TRUSTe, so I'm wearing both hats, EFF and TRUSTe, when I say this. We took a higher standard of going after notice and consent in the online world, probably a higher standard than in the offline world.
of what Dan is saying and what Mike has also
done, is that architecture -- we have a saying at
EFF that architecture is policy. Architecture
begets policy. And Danny can probably touch on
this with the WC3. You've got many policy
standards that are being set right now that would
predict many technical standards, that would
predict how policies get implemented.

Things like SDMI, which is a standard
for music listening and music players, actually a
portion of their standard deals with how
information is reported back from the player to
the server about a person's listening standard.

Some people may think that that actually is just
a technology standard and how nothing to do with
policy. But it does get into the whole area of
how do you give the consumer notice.

The same thing with profiling: How
do you make sure that technology that happens in
the background actually has a way for a consumer
to control this? So what we have here is sort of
a battle of the desktop or a battle on the
telephone or a battle on the little handheld
device for the goal of consumer control with
consumer convenience and consumer customization.

MS. BURR: Danny, you're on. I think
that one may be working now.
MR. WEITZNER: Is it working now?
No.
MS. BURR: Hopefully we'll get these
fixed at the break.
MR. WEITZNER: Thanks.
I want to come back to this question
about, I want to come back to the question about
the extent to which it's possible to re-identify
previously unidentified information. I guess I
think that we really shouldn't rely on the web
not being able to do things to get us to the
right policy outcome.

I think that companies, organizations
that make commitments to only follow certain
kinds of profiling practices, are to be
commended. But I frankly don't think that you
all aren't smart enough to do this if you want
to, and I think the underlying technology really
makes possible quite a lot of profiling.

I think that's only going to become
more and more true, for the simple reason that
people do want a personalized web experience.
They don't want to have, as Dan I think was
pointing out, they don't want to have to share
their browser preferences with their kids or
their parents. They want to have an experience
when browsing from some computer in a hotel
similar to their experience at their office or at
home.

For this reason, people want profiles
to work well for them and to serve them. I think
that what people don't want is to be surprised by
profiles. This is really a lot, and I think
we'll see this even more in the electronic
commerce arena with wallets.

People will want to carry their
electronic wallets around with them, be able to
make purchases easily, and certainly all of those
of you with commercial in this room want people
to make purchases easily and seamlessly, without
having to fumble around for their credit card
number and mistype the expiration date, etcetera.

At W3C we've developed the P3P,
platform privacy preferences, in order to help
users have more control over the various profiles
that are created of them, created about them, and
we think that's going to be an important part of
all these services. That's not going to solve
the problem all by itself, but it will help users
to manage the increasingly complex relationships
that they have, whether with services that are
really way in the background and they don't
necessarily know much about or services that they
have a more direct relationship with.

So I think the key is going to be to
give users the ability to have control over these
various profiles, to know they're there, and not,
as I think Eric pointed out correctly, have to
opt out from a profile that they don't even know
existed.

MR. MEDINE: Following up on that
point, to what extent do users today have control
over the technology that ad networks are using?
Are there ways that consumers can empower
themselves with current technological fixes, from
deleting files or setting browsers, to address
some of these concerns?

Obviously, later in the day we'll
hear about some industry efforts, but what can
the technology empower consumers to do today?
Dan?

MR. WEITZNER: As I mentioned in my
presentation, Engage has offered on our web site
an ability to opt out of our non-personally
identifiable profiling for several years now.
But it does -- a major question we deal with is
how do we get that capability and information out
to the users.

The way that we've done this to date
unilaterally has been through contractually
requiring our web sites to have a prominent
policy statement that discloses what's happening
and has a direct link to our privacy policy
statement at Engage.

You'll hear later on today some
discussions we've been having in the industry
about trying to make that a more uniform
practice. I think the point to be made is that
Danny is absolutely right on the fact that there
is not only a technology solution here. As one
of the original members of the P3P working team
and one of the original co-authors of the syntax
specification technical work on P3P, it is a
great technology that will yield benefits to
consumers and to marketers. However, it has to
be within an umbrella, a framework.

We believe that that framework should
be based on self-regulatory principles because
the Internet evolves so quickly. Four years ago
there weren't ad networks. The models change
very quickly, and one of the concerns I think
that consumers should have is whether
legislation, hard and fast legislation, could
possibly keep up with the new nuances in
technologies that have come up.

MS. BURR: Mike, do you have anything
to add?

MR. CATLETT: I'd just add to David's
question about what consumers can do. The
simplest thing you can do is just turn off
cookies. Unfortunately, many sites export
cookies from you by not allowing you to use their
services, such as free web-based e-mail. Late
model browsers have a feature where you can turn
off cookies for all other than the site that
you're visiting, and that gets around this
invisible monitoring aspect of cookies.

The other thing that you can do is
use a product to filter out banner ads and that
removes the opportunity for surveillance
completely. My company, Junkbusters.com, has
been publishing a free banner-out filter for more
than two years.

But I find this a completely
unacceptable solution to the problem because it
shifts the burden onto the consumer to defend
themselves against a practice of which they're
completely unaware and that's grossly unfair.

MS. BURR: Eric is next and then you.

MR. WENGER: I wanted to add one more
problem to the mix here with the idea of
transparency. That is, if I like MatchLogic's or
Engage's privacy policies, I don't really have
the opportunity to select which ad networks are
going to be giving me ads from the web sites I go
to. That I think is another fact that's going to
make the attempts at self-regulation difficult
here.

One other question I wanted to raise
is, we sort of glossed over the idea that
somebody put out the idea that static IP
addresses are becoming less common. I'm not sure
that that's true. I'd like to see the data on
it, because the cable industry is growing very
rapidly as far as Internet service is concerned.
My understanding is that they use static IP
addresses because you're permanently on the
network. And I imagine that most other broadband

The other thing is that the
percentage of people who get their Internet
service through work when they're on a network
that has a static IP address I think is fairly
high as well. So I wouldn't necessarily just
accept the idea that static IP addresses are
something in the past.

MS. BURR: I'm going to go to
Richard, but there's a question for you about
going back to the sorts of technologies that are
used in tracking, like GIF's and one by one web
bugs.

The other question that's come up is
that we often hear that the protocols as they're
written are not supposed to enable anybody other
than the site that set the cookie to read it, but
we've lately been hearing more about cookie
synchronization, and I'm wondering how prevalent
that is and how that works.

1 that is and how that works.
2 MR. WENGER: Cookie synchronization
3 is extremely common. The gentleman from Engage,
4 I was surprised when he said cookies could not go
5 across domains, because any time you have a
6 banner ad it's being served up by the ad server.
7 So that cookie, whether you go -- in the case of
8 DoubleClick you go to AltaVista or Inforoll, are
9 two sites that I know that use it. They have the
10 same cookie on the banner ads there.
11 So cookie synchronization happens all
12 the time, and that's the real danger. What's bad
13 about cookies is they do become universal ID's
14 when you have something like 800,000 pages on the
15 web, at least with DoubleClick, of different
16 sites that they have things at. So cookies, you
17 know, were intended to be domain specific, but
18 they're clearly not.
19 Another quick issue here, too, on
20 this issue of controlling cookies, back on the
21 question before here, of being able to opt out,
22 I've certainly been offered that option at
23 DoubleClick, but only after badgering them with
24 questions. They wanted me to go away by saying:
25 Oh, just turn off your cookies, our cookie.

Indeed, we have an opt-out option for that, but
that's after weeks of asking questions. That's
not really offered as an option.

Another quick thing here, cookie
synchronization gets even more sort of -- I won't
use the word "sinister," but interesting, let's
say, with the use of one by one GIF's. As an
example, prepping for this discussion here I was
looking at Procter and Gamble. They have
approximately 40 sites that are product specific,
1 one for Bounty, one for Metamucil, one for
12 Pampers, and so on, and they're all bugged with
13 one by one GIF's so you can't see them.
14 These are used for basically
15 gathering demographic information. You know, in
16 terms of opting out of those cookies, well,
17 there's no way to know how to do it. Number one,
18 you can't see them. A one by one GIF is like --
19 four pixels make a period, so you can't see them.
20 They're white on a white background, so you can't
21 see them.
22 They go to a company called
23 Preferences.com, which happens to be actually
24 MatchLogic. So there's no way for a consumer to
25 know that they need to opt out in this situation.

So the transparency is extreme, and it's an
intentional one also.

MS. BURR: Mike.

MR. MARTIN SMITH: On the cookie
synchronization issue, what we really mean by
cookie synchronization is the matching of cookie
across the domain. What you're highlighting
there is the request to the server within a site
that somebody or the browser has actually
appeared on the site.

That is used for measurement across
the site rather than gathering any specific
demographic information. What it brings back is
the cookie, the IP, the operating system, and the
date and time. What it's saying is, if it's
associated to advertising data, how effective has
my advertising been, what pages within the site
has the navigation been.

There isn't any intention to
synchronize between the domains.

MR. RICHARD SMITH: Well, maybe not,
but what I did notice here is your slide talked
about demographic information like sex and age,
and what I was seeing in the Procter and Gamble
case is those one by one GIF's were very
strategically placed to identify demographic
information. It was done also in the case of
some stuff for children and so on.

It's all hidden. That's what I'm
wondering about here, why is it hidden?

MR. MARTIN SMITH: The reason it's
hidden is for essentially page load. So we're
like a guest on that particular site. All we
need is a call to our servers. The reason we
need that call is if the page gets cached behind
a proxy server and you have high volumes of pages
cached, then there will be no counting across
those pages, so your actual media analysis, your
ROI analysis if it's a destination activity,
would absolutely be hosed. You would not get
consistent measurement.

We actually ran studies with Ernst
and Young two to three years ago in this area and
found that the percentage of pages that were
being served from behind proxy servers and
therefore not visible were actually on average
about 70 percent and on highly trafficked web
sites to the order of 700 percent, which in terms
of an order of magnitude from a measurement point
of view completely disrupts it.
So that's why it's there. The reason, it's very clear, is that it's a very lightweight request.

MR. JAYE: I just want to add to that for a second because I just want to clarify one issue. The examples you're giving, none of those are cookie synchronization. It's a very important point you're bringing up. Cookie synchronization is taking cookies, which are inherently as part of the protocol domain specific, and trying to match them across different domains.

So cookies are not inherently multi-domain. Cookie synchronization is what takes them across domains. In the case of, say, an ad network serving onto another page, that is not cookie synchronization -- so you gave the DoubleClick example -- because the site that DoubleClick is serving onto never sees DoubleClick's ID.

So there is no passing of information between the domains. There is no cookie synchronization.

MR. RICHARD SMITH: AltaVista gives your search string off to DoubleClick. That's no passing of information?

MR. JAYE: No, there isn't. If you would look at my architecture slide you would see that the third party ad network doesn't have a connection to the web server. It has a connection to the browser.

MS. BURR: Excuse me one second. We have just gotten a helpful technical message and, since this is the technical panel, I want to pass that on. The best way to keep the feedback off the mikes is to tilt them down and bring them closer, since all of us have them up.

Lori, you had a comment?

MS. FEENA: Yes. On the area of how do you create this transparency for these third party technologies -- can you hear now?

VOICE: Can you get closer to your mike?

MS. FEENA: Okay, I will get closer.

How's that? Any better? I see heads shaking.

MS. BURR: Here's a mike.

MS. FEENA: This one's very much on.

In the area of trying to create transparency for third party data in the background, one of the things that we are investigating and we'll be announcing later today with TRUSTe is that we do intend to extend the same principles and practices that we've been pioneering with many of the people in this room, that we have pioneered on the web sites, to actually apply to software and third party services.

I think it's very important to realize that this is not a simple solution. It's a very complex problem and it's going to require technology, P3P technology and other technologies, to bridge this gap. It's going to require programs like TRUSTe and BBB and certification programs, as well as -- I'll even bring this up -- I think it will also require certain laws, because we do have a great deal of this gap is being filled by the market forces, by technology, by programs, and by very voluntary high watermarks by industry leaders, but it doesn't address many of the things that have been brought up, which are the companies that haven't participated, the companies that aren't disclosing to consumers.

So when we look at this issue of transparency to the consumer and consumer control, I think it's really important that we look at this as not a self-regulation or law.

It's going to take informed consumers, because if you give a consumer a choice but they don't know what choice they're making it doesn't really help.

What we have in the Internet is a situation where huge decentralization is happening, and we can't create a magic policy or a magic law or a magic technology that can figure out what the right amount of information is to disclose in any particular transaction. It's very contextual.

MS. BURR: I want to go to Danny and Richard. I have a question from the audience that one or both of you might take up, which is: Why isn't the answer just cookie-killer software?

If you can't place cookies or they don't stay on, you can't serve up these ads.

MR. WEITZNER: I think that certainly the answer with respect to cookies is a better specified technology, which is work under way at the Internet Engineering Task Force, and that we're certainly looking forward to seeing move forward and implemented, because indeed cookies...
are a pretty blunt instrument at this point.
But getting rid of cookies, as Jason pointed out, maybe the problem there is not quite extortion, but sites actually have good reason for using cookies which have nothing to do with invading anyone's privacy or surreptitiously collecting information.
But I really want to just underscore Lori's point because I think it's critical. I don't know how many of you could follow the interplay about this kind of cookie versus that kind of cookie, but I can guarantee you that 99 percent of people who use the web can't follow that kind of discussion, have no interest in following that kind of discussion.
So certainly what we really need is the commitment across the board from people who are building services and building technologies to put real tools in the hands of users that make this experience less threatening, more accessible, gives users more control. I think the successful services in this area try to do that.
I can tell you it's not easy and we are still a ways away. I tried to install one of the services that's going to be discussed on a panel later today and erased most of my Windows registry. So I had a sort of unpleasant weekend.
MS. BURR: Eric and then Richard.
MR. WENGER: On the way to passing the microphone I'll just through in one last comment. I don't think it can be overemphasized, the point that Danny's making, which is that if consumers don't feel comfortable using this technology and that their privacy is going to be protected and that they're going to be protected from fraud, then they're going to shy away from it. That means that the continued growth of e-commerce may be stunted. So the topic that we're discussing here is extremely important.
MR. WEITZNER: Could I just intercept this on the way in that direction? There are good models for addressing this sort of problem and probably the best one that we can think of is a technology called SSL. Most people don't know what SSL is, but they do know what the little locker key at the bottom of their browser is.
That one tiny piece of real estate on web browsers has gone so far to close the confidence gap that users have in purchasing items over the web with their credit cards. We need to get to that level of accessibility for users, so that users see on their browsers tools that they know how to use, that help them manage their privacy relationships with all the entities that are out there.
MR. RICHARD SMITH: Real quickly on the question of the cookie buster software, the big problem really is that there are sites that require them. For example, I use my Yahoo for customization and I need cookies for that site so I don't have to keep logging in each time, and the controls on the browsers are kind of all or nothing. That's a problem.
Maybe if there were some level of who you'd accept cookies from, maybe like only from the web site that you explicitly go to, rather than an embedded image, that might be an interesting solution.
MS. BURR: K.C.
MR. SINGH: First of all, if you see us trembling it's because it's cold, no other reason.
MS. BURR: It is very cold.
MR. SINGH: The important thing is the e-commerce part of it, and the moment you give your credit card there goes the triangulation.
MS. BURR: Let's hear from the e-commerce folks over there.
MR. JAYE: Consumer confidence is an absolutely critical issue that we are very concerned about, and that's one of the reasons why we do want to find solutions that deal with the transparency issue. We do think that there is a middle ground here that benefits the consumer and the companies that, candidly, pay for all the free services and the free stuff on the Internet, which are the advertisers, and that
through the appropriate fair information practices and non-personally identifiable information techniques that balance could be found.

Some of the solution is technology. The cookie problems are definitely there. There are potential holes where cookies can be exploited to cause security and privacy risks. In fact, I'm the author of a draft of the IATF called "Trust Labels," which was an attempt a couple of years ago that I demonstrated at a session here in Washington a couple of years ago, which actually tried to make cookies intelligible by labeling them with their P3P vocabulary, the P3P practices and uses and data types, so that it would be more than just a number and a date.

Unfortunately, these initiatives don't always get off the ground, don't always find widespread technical implementation. Part of that is because the industry moves so quickly, and once again I think that's a reason why we have to work hard at this to come up with the right framework and the right types of policies so we can address the legitimate concerns about implementation, for example, that's non-personally identifiable today. People want to know, what happens in the future, and we have to make sure that we have a framework that addresses those legitimate concerns.

But I don't think that saying let's just make the web unusable for consumers, which would be what turning cookies off, is necessarily the right answer, nor is shutting off, making the web unprofitable for advertisers.

Furthermore, privacy advocates are not asking for the ads to be removed. You can still have the ads. You can still target them the old-fashioned way, like the newspapers do, which is putting the relevant ads in the relevant segments next to the relevant editorial. So the idea that consumers value targeting of ads is wrong. The idea that the e-commerce economy is dependent on it is wrong.

The number of companies that are making money -- well, actually losing money, but hoping to make money in the future -- about this targeting is relatively small and not a large part of the commerce market.

MS. BURR: Lori.

MS. FEENA: I think one note -- we've been focusing a great deal on advertising and targeting, and it's really important to understand that -- it's really information to understand that we've been focusing on advertising and targeting, but the same technology that's developed for advertising and targeting can be used for things like stalking and for red-lining.

So as we develop these technologies, we really have to understand the political and societal impacts of them. So it's nice to talk about advertising, it's nice to talk about ads and mail, but there's actually more sinister things that occur as well. So as we move forward I think we need to address these issues additionally.

MS. BURR: Mike, you're going to have the final word. If you could just give us also along with that a sense or your sense of what this advertising is contributing in terms of economic value to the Internet, that would be very useful.

MR. MARTIN SMITH: In terms of value from measurement and management of advertising, we have seen clients identify the capability to really optimize fully over 50 percent of their media buy through the use of effective frequency, through the effective rotation of advertisements. We have also seen 3 to 6 percent or 3 to 6X lifts in responsiveness from the use of targeting.

Now, the use of targeting to the segment allows the capability to deliver advertising that is relevant and that also creates resonance. The old adage, good
advertising and bad advertising costs the same,
but the results are immeasurably different, holds
very true. Used correctly, targeting to segments
is producing significant results.

MS. BURR: I think we're going to go
to a break now. When we come back at 11:00,
we're going to hear some more information about
this from the consumer perspective.
I'd just like to point out that your
coffee break is brought to you by the Center for
Media Education, and we'd like to thank them very
much for their generous help in this.

(Ms. Burr's statement is interrupted by applause.)

RECESS.

MR. MEDINE: Thank you very much.
First a few announcements. If
someone from the Law Offices of Allen Schlaefer
has left a Daytimer, we have it and feel free to
come up and get it.

Second, again the comment period for
this workshop will be left open until November
30th.

Third, Dr. Westin will be taking a
few questions and so, as with the prior panel, if
you do have questions, there are cards down on

the side of the auditorium and if you'd like to
pose a question to Dr. Westin, please fill out
the cards and they will be brought up to us.

It's my real pleasure to introduce
Dr. Alan Westin, who has been a regular
participant at all of the FTC and Commerce
Department privacy workshops. Dr. Westin has
been the Professor of Public Law and Government
at Columbia University since 1959 and he's
considered the nation's leading expert on
information privacy.

He's been a member of a number of
federal and state government privacy commissions,
an expert witness before state and federal
legislative committees and regulatory agencies,
and the academic adviser to Louis Harris and
Associates for 15 national and public opinion and
leadership surveys on privacy.

It's my pleasure to introduce Dr.
Westin to hear his latest survey results. Thank
you.

(RECESS.)

(REMARKS OF DR. ALAN A. WESTIN, PROFESSOR
OF LAW AND GOVERNMENT, COLUMBIA UNIVERSITY)

DR. WESTIN: Are we up?

I think that we can gain some
insights from survey research in general, which I
want to talk about first, and then a particular
survey that has been done dealing with the issue
of collecting personal information for banner ad
presentations.

Actually, it's 40 national surveys, I
hasten to say, that I've been involved with since
1978, either with Louis Harris and Associates,
now called Harris Interactive, or Opinion
Research Corporation in Princeton, New Jersey. I
think the central theme in every one of these
surveys which we've tracked and I think has been
extraordinarily useful for the public policy
process is to trace the rising, steady concern of
American consumers, citizens, employees, about
personal information and privacy.

When we asked our first set of
questions right after Watergate in 1978, 68
percent of the American public said they were
concerned about threats to privacy. I think it
was something like 30 or 35 percent chose "very
concerned." Now we have 94 percent of
respondents saying in survey after survey, 92, 94
percent, that they are concerned about threats to
personal privacy, and 77 percent, 3 out of 4, choose "very concerned."
On the other hand, these 40 surveys all document very carefully that people differ in how they want to balance their concern and interest in privacy with other social interests that they consider important -- consumer opportunities, protection of society against crime, and threats to security, the balance between the employee's interests and the employer's interest in the way in which communication tools are used in the workplace. So I think to understand how to use survey research one has to understand that there is no one position or one size fits all. People differ and the important thing is to see how they differ and what these differences mean.

Over the 21 years we've found a continuing pattern that divides the American public. When you take all kinds of privacy issues, consumer issues, citizen issues, employee issues, into account, we find that about 25 percent of the public are what we call privacy fundamentalists. Privacy is for them an extraordinarily central and important value. Generally, speaking, no consumer benefit or no claim that law enforcement needs this information to do its job will persuade them that the threat to their privacy should be put aside. So they will take the strongest positions on behalf of privacy, and when it comes to the business community the privacy fundamentalists generally favor legal interventions and regulatory enforcement of the consumer's interest in privacy.

At the opposite end you have what we call the privacy unconcerned. That's about 25 percent of the public and they don't know what the privacy issue is all about. They couldn't care less. For 5 cents off they'll give you their family genealogy and all their lifestyle choices, and it simply is not an issue that is on their radar scope.

In between you have what we call the privacy pragmatists, about 55 percent of the public. For them the clear answer is it depends. They go through what I think is an extraordinarily rational process, as our survey research shows. First they say: What's the benefit to me or to society if I give you or you collect my personal information?
Secondly they say: What privacy risk do I run that you will misuse my information or that I don't see that giving the information is really needed, it's not relevant, it's not essential?
Third they ask: What privacy safeguards or policies will you put in place that will give me some feeling that I get the benefit and you've taken care of the risks in a way that I am comfortable with?
Fourth and most important, they ask: Do I trust you? Do I trust your industry? Do I trust you as a company or do I think that there needs to be law and regulation in order to give me a feeling that if I give my information for this purpose that I am going to be adequately protected?

So the dynamic of consumer policy really is where the privacy pragmatists will come out on any given situation where personal information is sought to be collected and used for various kinds of consumer opportunities, benefits, choices, etcetera.

Now, even though this general picture that I have given is of the numbers 25, 20, and 55, when you focus on any particular consumer privacy issue, such as medical and health records, it will not surprise anybody in the room that the category of privacy fundamentalists expands enormously. So when we ask a series of health and medical privacy questions, you can go up to 48 or even 55 percent of people who fall into the fundamentalist category.

In general, both online and offline, the general pattern that we have breaks into these three categories and it gives you at least a kind of quick snapshot of the way in which people differ as to how they want to set these boundaries of privacy.

In the next two slides I want to report on some data from an IBM multinational consumer privacy study that I'll be reporting in full at the Privacy and American Business Conference in two days. I think it's extraordinarily important for today and in general because what it shows is that within the last year or two the American public has become...
extraordinarily privacy-asserting and active in a
day that was not true in the data in the early
nineties or the middle 1990's.

Just look at these numbers. 78
percent of the public, representing 152 million
adult Americans, say that they have refused to
give information to a business because they felt
it was too personal or wasn't needed. 58
percent, representing 113 million, asked a
company they patronize not to market additional
products to them. And 54 percent, over 100
million, 105 million, decided not to use a
company or buy because they weren't sure how
their information would be used. That's the new
privacy veto at work.

Some other figures: 53 percent asked
a company they were using not to give their name
to another company for marketing, 103 million
adults. And in smaller numbers, but very
significant in terms of what I think will be a
rising trend, 21 percent looked to see whether a
business had a privacy policy -- that's 41
million adults -- and 35 million, 18 percent,
asked to see the contents of their own record.

So I think that what we're seeing is
an extraordinarily active consumer population in
the United States, concerned about privacy, but
not just concerned in the abstract, ready to take
actions to patronize or not patronize, to
exercise opt-out or not exercise opt-out, based
upon their sense of the way in which they want to
see their privacy balances set.

Right away in terms of understanding
the picture fully and therefore framing my
presentation today, we want to recognize that the
American public still represents extraordinarily
active and avid consumers. 110 million people
bought last year from direct mail that was sent
to their residence, and 48 percent of the public,
93 million adults, say they're interested in
getting information from companies about new
products and services.

60 percent, representing 117 million
people, say that it doesn't bother them at all,
it's acceptable, for companies to look at their
profiles in their records in order to customize
communications to them about other products and
services that the company thinks might be of
interest to them.

Then when we add a statement to
people, would you be willing to do this if the
company gave you notice of how they would be
using your information and an opportunity to opt
out of uses that you did not approve of, we then
pick up 25 or 30 percent of people who were
initially negative and we wind up with 75 or 85
percent of the adult American public saying that
kind of customization is acceptable with notice
and opt-out.

With that as background, let me turn
to the survey that I'm reporting on today, which
we call "Personalization and Privacy on the Net."
Questions were developed by me, put onto the ORC
weekly Caravan survey. This is a representative
national survey of roughly a thousand
respondents. What we got was 474 of those 1,000
who said they use the Internet, and that
represents about 92 million adults self-reporting
that they use the Internet once a week or more.
In survey jargon, that leads to a
confidence factor of about plus or minus 4
percent, which is not what you want if it was
electoral statistics, but is perfectly acceptable
if what you're looking at is broad public
attitudes in an area such as privacy.
they went to. So you have roughly one-quarter of
people who click on banner ads saying they buy
something after they've gone to view what the
banner ad presents.

One of the things that I always try
to do in a survey is to make sure that the
attitudes about privacy of our sample track what
we know to be the national figures from many
other surveys, and we confirmed here that, as far
as Net users are concerned, 92 percent said they
were concerned about possible misuse of personal
data when they were on the Internet and 67
percent said they were very concerned.

So we have a kind of clear
confirmation that our Net sample paralleled the
general privacy concerns and attitudes of the
adult population of the United States in general.

So we turn to banner ads and
personalization. Our key question asked: When
banner ads are presented to you as you use the
Internet, how positive would you be in having
some of these ads tailored to your interests
rather than seeing only random ads that are aimed
at all Net users? 61 percent chose positive,

divided up into 18 percent very and 42 percent
somewhat, and that represents, as you see, about
56 million users of the Internet.

Having done that, we then wanted to
see what kind of information Net users say they
would be willing to give or to have collected and
under what conditions. The way we did this is in
a two-stage process that we've used in many
surveys in offline as well as online contexts.

First we asked in general: To tailor ads to
individual Net users, companies need information
about the user. How positive would you be for
companies to obtain such information in the
following ways?

First we asked about people supplying
their own information, and so we put the
question: By asking you to describe your
interests to them and you supplying whatever
information you wanted to have used for that
purpose. 56 percent of Net users said that they
would be willing to do this, representing 52
million users.

Then we asked the people who were not
willing if they would be willing: "If the
company providing tailored ads spelled out how
notice and opt-out, we get a total of 58 percent
that said that they would be willing to have
their web site visits collected.

Third, we asked about allowing
information about purchases on the Internet to be
used to tailor banner ads. You can see that it
dropped to 38 percent willing. But then when you
add those who would be willing if there was
notice and opt-out, it brings it back up to 51
percent or 47 million Net users.

By asking you to allow information
about your purchases from catalogues and stores
not on the Internet to be used to tailor Internet
banner ads to you, for you; 41 percent willing
and, after providing notice and opt-out, brings
it up to 52 percent or 49 million net users.

The fifth test was by asking you to
allow information about your purchases from
catalogues and stores not on the Internet to be
combined with information about your purchases on
the Internet, to be used to tailor Internet
banner ads to you. 45 percent were initially
willing; with notice and opt-out, it brings it up
to 52 percent or 48 million Net users.

Finally, and what obviously is the
most integrative of all, we asked: "Many companies on the Internet would like to combine information about your purchases, your visits to web sites, and the personal information you furnish to them into a profile that they use to present banner ads reflecting your interests as you use the Internet."

44 percent said this was initially acceptable; and then when you add those with notice and opt-out, it comes to 53 percent.

So when you draw back and look at all 6 of the examples that we tested, you see that a majority of Net users, ranging from a low of 51 percent to a high of 68 percent, feel comfortable, say that they would be comfortable, in supplying or having their data used to tailor banner ads to their interests, and it's the provision of notice and opt-out that increases acceptability by approximately 10, 15 percent depending on the particular issue.

The survey is also very clear in indicating that a solid minority of Net users, ranging from 32 to 49 percent, would not be willing to give or to have their personal information collected for various types of banner ad personalization.

In my judgment this is quite consistent with all of the other survey research that I summarized at the beginning. Approximately one-third to one-half of Net users are privacy fundamentalists, and the more you combine data sources from different activities on the Internet the higher their sense that their privacy would be invaded and the more they would want to have a privacy veto on any such collection and use.

On the other hand, when you put together the privacy unconcerned and the privacy pragmatists you get between 51 and 68 percent saying that they're willing, especially with notice and opt-out, to have various sources of information used for tailoring banner ads.

We didn't feel that it was appropriate just to leave it there with a broad statement about notice and opt-out, but rather to test some of the key fair information practices concepts that have always been at the heart of the way in which the consumer privacy relationship has been dealt with in the United States.

So we tested three central policies, indicating that: "These are policies that could be adopted by companies that were collecting online and offline profile information in order to present tailored ads. How important would each of these policies be if you were to participate in tailored ad profiles?"

First we said: "The information given by users or collected from their actions on the Internet would be used only for presenting tailored ads and other communications to them and users would always be able to opt out of communications they did not want to receive."

Not surprisingly, 71 percent rated that as important and 51 percent chose "absolutely vital or very important."

Second: "A user's interest information would be used only by the banner ad company and would not be sold or given to other companies." This rose to 79 percent rated as important and two-thirds, 66 percent, said it was either absolutely vital or very important.

Finally, we said: "A user participating in a tailored banner ad program could ask to see his or her profile and remove any items that the user did not want in the profile." This drew the highest importance rating, 83 percent, and 70 percent calling this absolutely vital or very important.

I draw the following conclusions from my results and from my thinking about how this fits into the larger picture of consumer privacy dynamics that I've sketched. First of all, we have a clear division of the Net user population into a majority that says it would be comfortable with banner ads tailored and personalized in this way and a strong minority that is clearly opposed.

Secondly, the scope of the information combination and integration is a key factor in how many people will be comfortable and how many people would walk away from a particular combination.

Third, the privacy policies or fair information practices we tested drew overwhelming support from Net respondents: limited use with opt-out, no sharing beyond the provision of tailored ads of communications, and user access.
<table>
<thead>
<tr>
<th>Page 114</th>
<th>Page 116</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to and control of the profile.</td>
<td>1 there was no position of neutrality. Do you</td>
</tr>
<tr>
<td>2 My fourth conclusion relates back to</td>
<td>2 think that affected the results of your survey?</td>
</tr>
<tr>
<td>3 what I presented as the new privacy-asserting</td>
<td>3 DR. WESTIN: Let me say right away,</td>
</tr>
<tr>
<td>4 behavior by consumers off and online. It seems</td>
<td>4 I'm not a survey methodology expert. I've done a</td>
</tr>
<tr>
<td>5 to me clear from our data that Net advertisers</td>
<td>5 lot of surveys, but I'm not the statistical</td>
</tr>
<tr>
<td>6 who want to get personal information must embrace</td>
<td>6 expert.</td>
</tr>
<tr>
<td>7 the privacy or fair information practices</td>
<td>7 My understanding is that you can use</td>
</tr>
<tr>
<td>8 policies that I describe or they're going to face</td>
<td>8 a five-point response in which you have a middle</td>
</tr>
<tr>
<td>9 a consumer privacy veto.</td>
<td>9 or neutral answer and that gives you one kind of</td>
</tr>
<tr>
<td>10 I see no signs that there are passive</td>
<td>10 spread. Or if you choose four points, two</td>
</tr>
<tr>
<td>11 consumers on the net, slaves to whoever wants to</td>
<td>11 positive and two negative, you have a tendency to</td>
</tr>
<tr>
<td>12 bounce something at them, incompetent to decide</td>
<td>12 push people a little bit to commit themselves.</td>
</tr>
<tr>
<td>13 whether to surf or not. I think the data about</td>
<td>13 My sense over the years is that by</td>
</tr>
<tr>
<td>14 privacy-asserting actions cuts two ways. It</td>
<td>14 using the four-point -- agree completely, agree</td>
</tr>
<tr>
<td>15 tells net advertisers that's the price of</td>
<td>15 somewhat, disagree somewhat, disagree completely -- you</td>
</tr>
<tr>
<td>16 admission for this new relationship with the</td>
<td>16 give people a range that they</td>
</tr>
<tr>
<td>17 consumer and, secondly, that consumers in fact,</td>
<td>17 can locate themselves on. In every question,</td>
</tr>
<tr>
<td>18 through a lot of media and privacy advocacy and</td>
<td>18 don't know and no response is always recorded, so</td>
</tr>
<tr>
<td>19 business activity, are in fact paying significant</td>
<td>19 if somebody says &quot;I don't know&quot; they're put into</td>
</tr>
<tr>
<td>20 attention to this issue and will not be supine or</td>
<td>20 the don't know or no response.</td>
</tr>
<tr>
<td>21 lifeless when it comes to it.</td>
<td>21 So I'm really not myself able to say</td>
</tr>
<tr>
<td>22 Finally, I would think that Net</td>
<td>22 that the five-point scale with the neutral is</td>
</tr>
<tr>
<td>23 industry associations need to adopt these</td>
<td>23 preeminently better than the four-point. I just</td>
</tr>
<tr>
<td>24 policies and to work on them, that privacy</td>
<td>24 note that both Harris and ORC in the work I've</td>
</tr>
<tr>
<td>25 advocates do an excellent job if they expose non-</td>
<td>25 done with them use that as the response</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page 115</th>
<th>Page 117</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 adopters or deviations from promises or</td>
<td>1 categories.</td>
</tr>
<tr>
<td>2 misleading privacy policies, and that I continue</td>
<td>2 MR. MEDINE: What are the</td>
</tr>
<tr>
<td>3 to applaud the role of the Federal Trade</td>
<td>3 demographics of your Net user sample? How were</td>
</tr>
<tr>
<td>4 Commission to hold privacy workshops such as this</td>
<td>4 they selected? How were they polled?</td>
</tr>
<tr>
<td>5 to oversee the issue, support these processes,</td>
<td>5 DR. WESTIN: This was a</td>
</tr>
<tr>
<td>6 and always to be ready, if there is not a</td>
<td>6 representative national sample, as I indicated.</td>
</tr>
<tr>
<td>7 significant adherence to these by the</td>
<td>7 A thousand respondents were questioned by</td>
</tr>
<tr>
<td>8 overwhelming majority in the Net advertiser and</td>
<td>8 telephone using the automated call system that</td>
</tr>
<tr>
<td>9 Net business community to recommend, if</td>
<td>9 most of the major survey firms use today, and</td>
</tr>
<tr>
<td>10 necessary, regulations to see that that is</td>
<td>10 people were asked: &quot;Do you use the Internet, I</td>
</tr>
<tr>
<td>11 followed.</td>
<td>11 think it read, 'once a week or more?' If people</td>
</tr>
<tr>
<td>12 Thank you very much.</td>
<td>12 said yes, then they were in the sample, which</td>
</tr>
<tr>
<td>13 (Applause.)</td>
<td>13 gave us a randomized, nationally representative</td>
</tr>
<tr>
<td>14 MR. MEDINE: Thank you, Dr. Westin.</td>
<td>14 sample of 474 respondents.</td>
</tr>
<tr>
<td>15 Dr. Westin actually has his own</td>
<td>15 In the material that has been passed</td>
</tr>
<tr>
<td>16 conference going on right now on privacy, but he</td>
<td>16 out, you'll find a box that describes for that</td>
</tr>
<tr>
<td>17 has graciously agreed to stay for a few more</td>
<td>17 sample gender, race, age, education, etcetera.</td>
</tr>
<tr>
<td>18 minutes to answer some questions. So you stay up</td>
<td>18 So if you want to see what the components of the</td>
</tr>
<tr>
<td>19 here and I'll pose some questions to you.</td>
<td>19 sample were, you'll find them there.</td>
</tr>
<tr>
<td>20 Is this working? Hello, hello? No.</td>
<td>20 But I think it's an accurate</td>
</tr>
<tr>
<td>21 One question from the audience is:</td>
<td>21 statement to say that this is a representative</td>
</tr>
<tr>
<td>22 Do you think the absence of a neutral position</td>
<td>22 sample of the people who say that they are using</td>
</tr>
<tr>
<td>23 affected the results of your survey? Neutral</td>
<td>23 the Internet in a larger, nationally</td>
</tr>
<tr>
<td>24 position, that is your survey called for people</td>
<td>24 representative sample of American adults 18 years</td>
</tr>
<tr>
<td>25 to express positive, very positive, somewhat, but</td>
<td>25 of age and older.</td>
</tr>
</tbody>
</table>
MR. MEDINE: Your survey results did not ask the question, how would consumers feel about providing this information assuming there was no notice and out-opt. Can you essentially take the converse of the percentages and say, since 75 to 85 percent were comfortable were comfortable with notice and opt-out, that only 15 to 25 percent would be comfortable without notice and opt-out?

DR. WESTIN: I don't think you can say that, because we first asked it without notice and opt-out. We said how willing would you be to, for example, number one, give your personal information that you wanted to see used for personalizing banner ads?

We didn't say with or without notice or opt-out. But for the people who said they would be willing, obviously in their mind I think there was not a requirement that they would have had to have heard notice and opt-out in order to participate.

Then by asking those who said they weren't initially willing whether notice and opt-out would lead them to participate, I think we picked up the people who had that in their mind when they said they would not otherwise participate.

MR. MEDINE: I guess the follow-up here is that, along the same lines, the first group you didn't tell one way or the other whether there was an opt-out.

DR. WESTIN: That's correct.

MR. MEDINE: Did you consider telling that group, by the way, would it make a difference to you if there were no notice and opt-out, essentially to highlight the privacy consequences that you did for the second group?

DR. WESTIN: It's an interesting point. I guess my experience in other surveys that I have done is that if you ask the question, how important is it to you that there be notice and opt-out before you give your personal information for this or that purpose, we always draw 70, 80 percent that say that's important.

So you have sort of two results to put together. As a matter of general outlook, it's absolutely clear that three out of four or more of Americans, when asked how important notice and opt-out is, will say it's important.

But if you try it the other way and say, is a particular collection of information for this benefit acceptable to you, you'll get the numbers that we did at the front end, and then putting the notice and opt-out brings them up.

But I wouldn't for a minute quarrel with anybody -- my data produce it all the time -- that notice and opt-out is perceived as the bargain on the part of consumers if they're going to be comfortable in giving their personal information for marketing and for other kinds of consumer purposes.

MR. MEDINE: Are there surveys of a like nature being conducted in Europe? If so, by whom? Are their findings similar?

DR. WESTIN: I'm happy to tell you that if you go to the IBM web site -- I don't happen to have the citation at the moment -- we did a national survey with identical questions testing American consumers, U.K. consumers, and German consumers. And you'll find there some fascinating material, because you'll find, first of all, that American consumers are by very large differences -- 20, 30, 40 percentage points -

more privacy-asserting today than individual consumers in the U.K. and in Germany.

Area by area, if you're interested in attitudes toward getting information, concern about Internet privacy, what U.K., German, and U.S. consumers are doing at financial service web sites, health web sites, retail web sites, and insurance web sites, our data show how the activities of consumers in all three countries compare with one another. So we now have some very good data with identical questions in three different countries comparing consumer behavior, attitudes, experiences, and so on.

MR. MEDINE: That's it. Thank you very much again for being with us today.

DR. WESTIN: Thanks very much.

(Applause.)

MR. MEDINE: If those on the second panel could please come up. Thank you.

(Pause.)

SESSION II. IMPLICATIONS OF ONLINE PROFILING TECHNOLOGY FOR USER PRIVACY

MR. MEDINE: Can people hear me?

Yes? Okay.

Thank you for joining us for our second panel, in which we're going to explore the benefits to consumers and to business of the
technology we have been hearing about, as well as
the privacy and consumer concerns about the
technology as well.

I am pleased that we have a
distinguished panel, some of whom have been here
before and some of whom are newcomers to our
privacy workshop. Starting to my right, we have:
Bradley Aronson, who serves as the President of
i-frontier, which is an Internet advertising
agency focusing on achieving client goals. i-frontier's
objective is building brands,
generating leads, selling products, and
increasing page views to measure success.

Next to him is Fred Cate, who's a
Professor of Law and Director, Information Law
and Commerce Institute at the Indiana University
School of Law at Bloomington. I guess I should
disclose that I was formerly a professor at that
same institution. He's also a senior counsel
for information law at the Indianapolis law firm
of Isemiller, DiNadio, and Ryan, specializing in
information and privacy law.

Next is Jason Catlett, who was on our
prior panel, who's already been introduced.

Jeff Chester, who we can thank for
the refreshments during the break, in addition to
being the Executive Director of the Center for
Media Education, one of the country's leading
consumer organizations working on electronic
media issues affecting children and youth.

Austin Hill serves as President of
Zero-Knowledge Systems, an Internet privacy firm
that develops end user-controlled privacy
solutions to enhance the privacy of Internet
users.

Deirdre Mulligan is Staff Counsel at
the Center for Democracy and Technology. One of
CDT's concerns involves the privacy issues
surrounding the deployment of the Intel Pentium
III processor serial number.

Dan Jaffe serves as Executive Vice
President of the Association of National
Advertisers and is dedicated to serving the
interests of companies that market regionally and
nationally, many of whom engage in electronic
commerce.

To my left is Megan Hurley. She
serves as Associate General Counsel at 24/7 Media
and oversees database development issues. 24/7
is a third party ad network and e-mail marketer

which currently delivers ads based on location or
context to suit the advertiser's needs.

Jonathan Shapiro, to her left, is the
Senior Vice President of Business Development at
DoubleClick, Inc. DoubleClick is a global
Internet advertising solutions company
specializing in developing the solutions which
make advertising work on the Internet for web
publishers and web advertisers.

Solveig Singleton is a
telecommunications lawyer and the Director of
Information Studies at the Cato Institute, a
public policy research foundation.

Robert Ellis Smith is a journalist
who uses his training as an attorney to report on
the individual's right to privacy. Since 1974 he
has published "Privacy Journal," a monthly
newsletter on privacy in the computer age.

Lastly, Shari Steele is an attorney
with the Electronic Frontier Foundation. She
works primarily on civil liberties issues for
people communicating online and on issues
involving access to government information.

Jonathan Shapiro, to her left, is the
Senior Vice President of Business Development at
DoubleClick, Inc. DoubleClick is a global
Internet advertising solutions company
specializing in developing the solutions which
make advertising work on the Internet for web
publishers and web advertisers.

Solveig Singleton is a
telecommunications lawyer and the Director of
Information Studies at the Cato Institute, a
public policy research foundation.

Robert Ellis Smith is a journalist
who uses his training as an attorney to report on
the individual's right to privacy. Since 1974 he
has published "Privacy Journal," a monthly
newsletter on privacy in the computer age.

Lastly, Shari Steele is an attorney
with the Electronic Frontier Foundation. She
works primarily on civil liberties issues for
people communicating online and on issues
involving access to government information.
visiting him and where they're going, it's natural that he would want to seek out some kind of information and collect it. Once that information is collected -- and here's a difference -- he'd have additional opportunities to use that information because, it's actually preserved in electronic form, to develop new products or to move things around or to improve security and so on.

MR. CHESTER: I'd like to respond because I think it's entirely different. The Center for Media Education has been tracking online advertising and online profiling since 1996, when we handed the FTC our report "Web of Deception," which led to the Children's Online Privacy Protection Act. Indeed, microtargeting of children was our early concern.

But I want to underscore from our observations at the Center that online profiling threatens the privacy of all Americans, and we're especially concerned about children and teens. An unprecedented technological apparatus has been put into place over the last few years to track and identify behaviors, values, psychological characteristics of individuals. This information is being collected online. It's being added to offline material. I know that we have a big panel, but I'll just give you an example of one of the many ads that appear in all of the ad trade journals. This happens to be in the current issue of Red Herring. There's a guy on a motorcycle, a motorcycle helmet -- I'm sorry you can't see it -- and the big copy says: "Has a nose for rare bordeaux, calls mom every weekend, grows award-winning roses. His name is Axel." This is from the Navient Company: "New precision web targeting from Navient combines physical world data with online behavior for the very first time, so you can deliver customized banner ads without the waste of scattershot messaging. With the acquiring of IQ2Net, we're taking data integrity to a level that's never been reached before, that includes name, address, demographics, psychographics, and click stream behavior."

I want to finish by underscoring, the psychographic scales, the technology that relates to identifying you as an individual, your interests, and strategies behind that information to get you to buy over a long period of time. The consumer in this country has no idea and they would have responded to Dr. Westin's study in a totally different way if they knew that in fact we are creating a psychological profile of you: We want to know your vulnerabilities and your interests.

So we think that this is a very critical issue here that the Federal Trade Commission must grapple with now.

MS. BURR: Shari.

MS. STEELE: I don't think the analogy of the shopkeeper really works. It would be a shopkeeper who is watching you as you were browsing through their store. They're following you down the aisles, peering at everything you pick up and look at.

It's also the shopkeeper who, you've walked in and you've got stamped on your forehead all of the purchases that you've made the previous stores that you've gone to. It's also the shopkeeper that you might choose to pay cash because you don't want information about what personal kinds of purchases.

And that information, you're not being given a choice as to whether or not that's collected about you or whether or not advertising is being directed at you based on those purchases.

So I just think that, while there are a couple of really basic similarities to a shopkeeper, it's really so much more intrusive with online communications because of the magnitude of information that's being collected and the amount of information that's being shared among shopkeepers.

MR. MEDINE: Deirdre.

MS. MULLIGAN: I wanted to build on some of what Shari just said, that I think, unlike an online service provider or a web site, where an individual actually has some role in initiating the relationship, I think one of the most troubling aspects of the advertising networks that we're discussing today is that they don't directly serve consumers. Consumers are unaware of their existence. They have no knowledge that someone else is reaching through your shopkeeper's store and extracting data about you.
<table>
<thead>
<tr>
<th>Page 130</th>
<th>Page 131</th>
<th>Page 132</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. about is all of the unintended consequences and</td>
<td>1. actually think about what goes on the</td>
<td>1. our ad.</td>
</tr>
<tr>
<td>2. all of the ways this data can be used.</td>
<td>2. Internet. The whole birth of e-commerce, the</td>
<td>2. MR. MEDINE: Just to briefly</td>
</tr>
<tr>
<td>3. the things I also think we need to address is the</td>
<td>3. whole birth of malls, and the incredible</td>
<td>3. interrupt the discussion, if Clark Rector is</td>
</tr>
<tr>
<td>4. use of cookies and the use of profiling is just</td>
<td>4. valuations that we're seeing in the Internet age</td>
<td>4. here, please call your office as soon as</td>
</tr>
<tr>
<td>5. milliseconds into the Internet age</td>
<td>5. is a recently new phenomenon.</td>
<td>5. possible.</td>
</tr>
<tr>
<td>6. starting to realize how some of these techniques</td>
<td>6. This is a communication medium.</td>
<td>6. Jonathan.</td>
</tr>
<tr>
<td>7. can be used.</td>
<td>7. that's the same medium that we're being asked to put</td>
<td>7. MR. SHAPIRO: The most important</td>
</tr>
<tr>
<td>8. Now, we can disagree as to whether or</td>
<td>8. our medical records on. This is the same medium</td>
<td>8. thing here is that the research that we've seen</td>
</tr>
<tr>
<td>9. not it's a benefit to consumers to have</td>
<td>9. that people are reaching out to talk about</td>
<td>9. suggests that users, a majority of users,</td>
</tr>
<tr>
<td>10. information tailored or not. But I don't think</td>
<td>10. support groups, get advice about cancer. Every</td>
<td>10. actually like the notion of having advertising</td>
</tr>
<tr>
<td>11. anyone here would disagree that individuals</td>
<td>11. single aspect of our lives is being pushed onto</td>
<td>11. and content personalized for them. Now, we</td>
</tr>
<tr>
<td>12. should have knowledge and that their consent</td>
<td>12. this online form.</td>
<td>12. recognize that the majority doesn't mean</td>
</tr>
<tr>
<td>13. should be given when we're talking about a</td>
<td>13. So it's not just a mall where</td>
<td>13. everyone. So what we want to do is provide users</td>
</tr>
<tr>
<td>14. secondary use of data, that no consumer is</td>
<td>14. shopping goes on.</td>
<td>14. notice and choice, as Deirdre mentioned, so that</td>
</tr>
<tr>
<td>15. visiting a web site in order to enable ad</td>
<td>15. The same profiling and the</td>
<td>15. the user gets to decide whether they're</td>
</tr>
<tr>
<td>16. serving. This is all about a secondary use.</td>
<td>16. same techniques are being used to help an</td>
<td>16. participating in this profiling.</td>
</tr>
<tr>
<td>17. MR. MEDINE: Austin.</td>
<td>17. insurance provider make a decision on whether or</td>
<td>17. DoubleClick for the last two and a</td>
</tr>
<tr>
<td>18. A couple points.</td>
<td>18. not someone's a viable prospect for insurance.</td>
<td>18. half years has provided users that choice. We've</td>
</tr>
<tr>
<td>19. the analogies that I think Shari has kind of</td>
<td>19. Did they visit a risky web site? Did they go to</td>
<td>19. had a selective opt-out that allows you to opt</td>
</tr>
<tr>
<td>20. touched on breaking down is the Internet as a</td>
<td>20. a web site that was unpopular?</td>
<td>20. out of the DoubleClick cookie and basically de-link, take</td>
</tr>
<tr>
<td>21. mall. I think it further breaks down when you</td>
<td>21. An employer who's doing a background</td>
<td>21. away our technical ability to profile</td>
</tr>
<tr>
<td>22. MR. HILL:</td>
<td>22. search can now go into Dejanews and look at</td>
<td>22. you.</td>
</tr>
<tr>
<td>23. one of the things we need to think</td>
<td>23. someone's opinions, religious beliefs,</td>
<td>23. MS. MULLIGAN: Can I just respond?</td>
</tr>
<tr>
<td>24. And the employer who's doing a background</td>
<td>24. discussions that went on eight years ago that are</td>
<td>24. Actually, I agree with you that notice and</td>
</tr>
<tr>
<td>25. archived in there forever.</td>
<td>25. So one of the things we need to think</td>
<td>25. consent are critical. But notice, when you talk</td>
</tr>
</tbody>
</table>

34 (Pages 130 to 133)
1 about notice, it's supposed to occur prior to the
2 collection of information. It is not supposed to
3 be something that individuals can later on, if
4 they happen to realize that they've interacted
5 with an entity with whom they didn't initiate an
6 interaction, has to go back, track them down, and
7 then say: No, I want you to stop collecting
8 data.
9          In fact, particularly when you're
10 talking about a secondary purpose, its notice to
11 the individual and a consent.
12          MR. CHESTER: And it's meaningful
13 notice. For example, DoubleClick says on its web
14 site that you use psychographic targeting in
15 order to help bias ads toward users most likely
16 to respond. I suppose when you give them an opt-out, do
17 you tell them that you're doing
18 psychographic targeting?
19          MR. SHAPIRO: Well, clearly our web
20 site is a public forum and everything available
21 on the web site is available.
22          To Deirdre's point, wherever we are
23 going to aggregate or collect personally
24 identifiable information, it'll be at that point
25 where the user is volunteering their name and

---

1 address or their e-mail address that they are
2 provided notice. So before in fact someone gives
3 to DoubleClick or a partner of DoubleClick their
4 personally identifiable information, we will be
5 providing them notice and at that point they'll
6 have the choice. That notice will include the
7 choice to participate or not.
8          MR. MEDINE: Dan.
9          MR. JAFFE: I think it's very
10 important to put this in a real economic context.
11 I think it's common sense that if you get
12 information that is useful to you, that means
13 something to you, that's more likely to create an
14 efficient, competitive, and innovative low-cost
15 marketplace.
16          Now, the question is in getting to
17 that marketplace if you have to give up key
18 privacy values it may not be worth it, that
19 you're going to have to balance it. So the
20 challenge for the business community is to see
21 that people get the ads that they want when they
22 want them, at the cost that they want them --
23 that's a tremendous value for everybody -- and
24 then how can we do this in a way that is privacy
25 protective.

---

1 this medium are going to be effective unless
2 there's a very major industry backup of the
3 system, and you're never going to have an
4 efficient Internet unless you can get ads to
5 people that they want. If I get an ad for a
6 product I have no interest in, it's a waste of
7 money for the company and it's a waste of my
8 time, and that's true over and over and over
9 again, and when you multiple that over the
10 hundreds of millions of consumers throughout this
11 world, maybe even billions of consumers
12 eventually, then you're talking about enormous
13 economic waste that can be affected.
14          So we have to find a way to make this
15 work while protecting privacy. Our association,
16 the American Association of Advertising Agencies,
17 direct marketers, others, have all come forward
18 to say -- and this is just a short list; there's
19 many other groups -- saying that we're going to
20 see the consumers get this privacy protection.
21          So it's not a question of pro-privacy
22 or anti-privacy. Our members are not interested
23 in knowing some dossier about somebody just to
24 know something about them, to have that
25 information that they can hold close to their
vests. They want to know something that will allow them to provide ads to people so that they can make choices that are more likely to be meaningful to them and therefore create an economic benefit both to the consumer and for business.

MR. MEDINE: It would be helpful on the comments on profiling, where is value added at networks and web sites, as well as the benefits to consumers. Then I'll turn to Megan to address what you wanted and possibly that as well.

MS. HURLEY: Before getting to the benefits, I just wanted to address the transparency issue of the ad networks. We realize that consumers don't know who we are and that we have to get to them. Consumers are our business. If they're unhappy, we're not going to have happy advertisers and we're out of business.

So some of the ad networks, like 24/7, require all of the web sites that are in our network to post a privacy policy that is in adherence with the highest industry standards, such as TRUSTe or DMA. So that is one way, not the only way, that is one way that the ad networks recognize this problem and that we're addressing it. You'll hear much more on panel three, when the advertisers talk about the new initiative that they're putting in. But the benefits economically to the web sites and to the advertisers and to the consumers are obvious. You see from the various studies that consumers want to see ads that are targeted to them. Their fear is of the unknown, how is this information used? So I think our struggle here is to start with reaching consumers and educating them to the fullest.

So I think that, before we talk about benefits, is a key issue.

MR. CHESTER: David, I'd like to just -- I'm glad to hear that the industry will address it and I know you're saying it sincerely. But I think we have to look beyond the notion that this is really about giving consumers what they want or choice.

I suggest that we have to look behind the technology and see if there are other motivations and really have a debate about the proper use. Let me just share with you some of the phrases used with the online ad targeting networks to describe what they do: predictive databases, targeting algorithms, flow states. Recently one of the heads of Excite talked about neural imputation.

Clearly there are other motives here, in some sense to direct consumer choice without consumers fully understanding why. Those choices are linked in fact to editorial content also made available, which raises other public interest issues.

But it's not just about giving people what they want. It's about steering them and having long-term strategies to steer them, and none of this is understood by the consumer and the citizen. I do think it has implications far beyond advertising and marketing, including for political speech. But it's very important we deal with this issue now, early on, to develop the safeguards.

MR. MEDINE: Jason, Bradley, Fred, and Deirdre.

MR. CATLETT: Thanks, David.

I'd like to give people some specific cases of URL's that they can go to to see this technology and this kind of proposal in action.

The first one is Netdeals.com, which is related to DoubleClick. It's a sweepstakes where you enter your name for a contest, and there's a privacy policy down at the bottom that says that the company will protect your privacy, and you actually have to scrawl down to see some of the details there that they are going to link that. So that is a first point of call.

The second one is a popular finance site called Quicken.com, and there are ads on this served actually, I believe, by MatchLogic. There are also these web bugs, as Richard Smith calls them, or pixels, clear GIF's, transparent GIF's -- they have a number of names -- which basically tells the advertising network that you are going to that page.

This can be tremendously valuable to the advertising network. For example, the Quicken site has areas on mortgages, on insurance, and finance, and it's very valuable for the advertisers to know what you're shopping around for. But it's also highly intrusive.

Let me give you a final URL, which has a poetic irony to it. It's Mentalwellness.com/mask, Mentalwellness.com/mask.
Now, if you go to this page you will read a touching story of people who in history, great figures, have overcome mental illness and gone on to greatness.

What is not -- there are no ads on this page and it's not clear to anybody who doesn't know to view source and look at the URL to see that there is one of these web bugs pointing, telling the advertiser when you are visiting this page, and I find that very offensive.

MR. MEDINE: Bradley.

MR. ARONSON: I wanted to address a few issues. The first is Austin had brought up how it's kind of we're only milliseconds into what's going on, and that's really important because no one really knows what's next. The risk of coming up with some sort of set regulations is that we could be stunting the growth of something we don't know.

To address the economic issues, most of the web sites out there are supported by advertising. That's why the content is free. And advertisers need to see results and targeting delivers results.

Consumers should definitely have notice. They should definitely have choice. But we need to be able to target, because if it's not effective how are web site publishers going to support what they're doing? It's going to be kind of difficult.

I think advertisers will support self-regulation. Look at the bigger picture. For most advertisers the Net is a very, very small portion of their budget and they're not going to try to upset consumers by violating their privacy through doing things that are outrageous on the Internet. In fact, a lot of the large advertisers say, we're only going to advertise on sites that have clear privacy policies.

By coming up with a set of guidelines and saying, hey, here's what self-regulation, what we're going to do to make it safe for consumers, I think advertisers can really, with the privacy of a machine or an IP address at issue. I'm concerned. What is the nature of this harm? Now, in reading the comments filed before this proceeding, without exception they talked about the harm of being marketed to, the harm that somebody might actually advertise things to you that you would want. I'm again concerned about the nature of this harm. If it is a fraudulent or deceptive trade practice, you've already got jurisdiction, I assume. If we are talking about marketing in terms of sending people the types of ads or type of information, type of opportunities that they're interested in, again it's unclear to me what the privacy, what the privacy harm is. 

On the benefits side, although you asked earlier about the economics within the industry, something which I'm not in a position to comment on, but the benefits as a user, as a consumer, would seem to be not paying for a great deal of that content that we access on the web.

I thought earlier during the panel this morning of Encyclopedia Britannica. When it networks to track what's going on. It's for the advertiser to track whether or not they're having success. For example, on a lot of our sites we run different ads. We need a way to track after someone clicks on the ad, what do they do on the site, because it's not really -- we can't say we had a successful ad campaign if someone clicks on the ad and just comes to the web site. I want to know did they go to the right section of the web site and which ads drove the people who delivered orders or leads.

MR. MEDINE: Fred.

MR. CATE: Thanks, David.

I just want to turn, I guess, to the question asked right at the outset, which is the question of harms and benefits, because, to be perfectly frank, I'm confused and this may come more in the guise of a question than a statement. In terms of harms, what we heard about so far this morning is non-personally identifiable information, is collections of information that may be linked to an IP address or a cookie, but not linked to a person. And this is certainly one of the first times that I've heard an extensive privacy discussion about information that isn't linked to an individual, that isn't the privacy of an individual, but is rather the privacy of a machine or an IP address at issue.
1 went from a pay per use to a non-pay per use, a
2 "free" system, I assume that advertising is the
3 difference there. So that's one benefit that to
4 me is very clear.
5 The other benefit -- I am one of the
6 75 percent in Alan's sample who don't click on
7 banner ads typically. On the other hand, you
8 know, I have to say I prefer seeing banner ads
9 that relate to what I'm interested in or what I'm
10 looking at, as opposed to ads that are either
11 randomly generated or, better yet, generated to
12 be something which I have no interest in.
13 So this is the question I would
14 leave, which is what are these harms that we're
15 really, that we're really talking about here.
16 MR. MEDINE: We haven't heard from
17 Robert Ellis Smith. A question came from the
18 audience, and I'll give folks here a chance to
19 jump in as well, that amplifies on that, which
20 is: Online profiling blurs the line between
21 personally identifiable information and non-personally
22 identifiable. It is the collection of
23 detailed information about an individual that can
24 be later joined to a name-address. Should
25 information with such privacy implications notify
consumers and require their consent?
1 I don't know, Robert, if you want to
2 speak to that or other issues.
3 MR. ROBERT SMITH: Well, I think Fred
4 Cate might well be confused because we have not
5 in a session on privacy even talked about
6 privacy. In order to know whether something like
7 this violates privacy, we should define privacy
8 and know what it is.
9 Privacy is not just the keeping of
10 secrets. The concern about privacy goes far
11 beyond breaches of confidentiality. Even if no
12 individually identifiable information is kept in
13 a marketing scheme like this, it would violate
14 privacy.
15 What Jeff Chester describes is a
16 scenario that violates privacy in two aspects.
17 One, the right to privacy includes the right of
18 personal autonomy. To the extent that I am
19 manipulated in the marketplace, especially
20 without my knowledge and especially if I'm a
21 vulnerable individual, it is a violation of a
22 diminution of my autonomy and therefore a
23 violation of privacy.
24 The scenario that he described as
25 well has been described as an invasion of privacy
26 as a tort matter by the U.S. Supreme Court. In
27 1995 they said that target marketing aimed at a
28 vulnerable population is an invasion of privacy.
29 And that's, even though we haven't used the word
30 yet, on two points this is an invasion of
31 privacy.
32 I'd like to give you a scenario of
33 about 20 years ago, when movie theater owners
34 discovered that they could flash up instantaneous
35 messages on the screen for just a portion of a
36 second and get people to buy products, whether it
37 said "You're thirsty" or "You like popcorn."
38 They could do that immediately on the screen.
39 That involved no collection of
40 personal identifying information at all. Is it
41 an invasion of privacy? Of course it is. It's a
42 diminution of our autonomy. It's commercial
43 manipulation in an unfair way, simply because the
44 individual in the theater doesn't have the same
45 resources to respond in a meaningful way.
46 The Federal Trade Commission, by the
47 way, acted immediately to say that that sort of
48 technology ought to be suspended until we knew
49 more about it. It then gravitated towards
information, which I believe at least some of the services, the companies that are engaged in these services, are moving to making this information that is identifiable with an individual in both their online capacity through a unique identifier and their offline capacity?

Now, I have a question that I think might help illustrate this. Have any of -- I guess we have Bradley, Austin, Michael -- no, Megan, and Jonathan -- have any of you been served with either a civil or a criminal subpoena for access to information contained in your databases? And if you were, would you be able to, either retrospectively or prospectively, attach the profiles that you have to an individual? And if yes, what would it entail?

MR. MEDINE: Jonathan.

MR. SHAPIRO: Let me address that. We have not been served a subpoena, and if we were we would not today be able to attach any of the information we have to a unique individual.

But let's be clear. The ad networks are not the best source if someone wants -- if a legal agent wants to get information on someone. The ISP has a view of everything that the ISP's members do, and if someone wants a picture of someone's transactions, you know, Visa and American Express have a much more complete picture than anything that any of the ad networks would ever have.

MS. MULLIGAN: So you're saying technically you cannot?

MR. SHAPIRO: Technically, today we cannot associate the name and address or personally identifiable information with the profile that we have.

MS. MULLIGAN: No, an IP address or a unique ID? If I --

MR. SHAPIRO: Well, let me clarify. If someone's volunteered their information, if someone has volunteered their name and address somewhere on the web where we were, we could technically at that point, we could give them notice and choice and then we could associate it. So for example, the Netdeals site that Jason cited earlier -- by the way, I encourage all of you to go and visit because you can win a million dollars -- at that site we clearly state that we are going to take personally identifiable information from you when you register, so your name and your address and your e-mail address.

We are going to link that information to both online information and offline information, and then we're going to use that information. Now, what are we going to use that information for, because it gets to some of the other questions earlier and Fred's comments on harm. We are going to use that information to target advertising to you. That's it. We're going to send you marketing messages. We want to get -- DoubleClick and all the ad networks are in the same business. We serve advertisers. We want to help advertisers get the right message to the right user at the right time. We want to put information in front of consumers that's relevant to them, and that's what we're going to use all the information we're collecting to do going forward.

Can I, just one more comment, David. You know, to Robert's comment on this is personal autonomy being a key component of privacy, we agree. Again, Dr. Westin's research suggests that Americans are very active about managing their privacy. We are providing notice and choice, and that gives them the tool to exercise their autonomy.

Moreover, we have made business decisions where we think that, even though we can aggregate certain information, it's inappropriate for targeting. So a vulnerable population like children, we will not gather or link information on children's activities to a profile or ever use that information for targeting purposes, because we think that's inappropriate.

Detailed financial information we think is inappropriate, and clearly health, mental health or health-related information is inappropriate. So there are classes of information that we at DoubleClick, and I'm sure the other ad networks would echo, are inappropriate for targeting.

MR. MEDINE: Thanks.

Austin, then Jason.

MR. HILL: Just addressing two points, one Fred's and then Bradley's point. One of the comments was who was being harmed? We're receiving advertising, advertising is an acceptable form of reaching consumers in this culture. One of the things I don't think has
been honestly talked about today -- we've heard a lot from ad tracking networks, you know, advertising networks, advertisers -- is some of the surreptitious activities that do go on.

There is very, very active efforts on the part of advertising networks to collect information without informing customers about how that will be used. One of the companies that presented today very quickly in their presentation talked about how, we allow customers to opt in and voluntarily give data. What they didn't mention is that their sweepstakes sites, if you go to their sweepstakes site where you can win a trip or a bunch of information and you go through and you go to register for this trip, there is the little TRUSTe logo that says, we have a privacy policy, you can give this information.

Nowhere on that site does it identify that they are part of one of the largest search engines in the world. Nowhere does it identify that the information you're volunteering for this one sweepstake is also setting a cookie that works on an entire ad tracking network.

So customers don't know this. You can look through the entire site and nowhere does it say that this is a subsidiary of Excite At Home. It's not there. So there is a surreptitious activity. Customers are delivering data without full information or understanding of how that will be used.

The next point to Bradley's comment, which I think is a very, very important one, is the economic benefit and the fact that there is a lot of content for free. Advertising and the delivery of ads represents a significant part of our economy, and we can't just say tomorrow we're going to shut it off. I don't think it's realistic and I don't think it's right. There is an economic interest.

What's not being talked about is the entire basis, if we look at this honestly, is Internet advertising was sold on the idea that we can charge more for advertising because we can get more targeting, we can get you better response rates. So they started charging $50 CPM's. A number of companies started going public and received market caps, valuations of their companies. Combined, if you associate all the big ad tracking networks, it's around $10 billion.

So there is a $10 billion investment in the fact that we can charge more and get more return because we can do better at understanding customers, when the actual facts haven't proven so. Click-through rates and response rates for advertising has gone down. In the last two and a half years since DoubleClick implemented DARTS, their Dynamic Ad Targeting System, their banner ads and click-through rates have gone down. It's now less than one percent.

The alternative is not to throw out advertising. The alternative are things like opt-in permission-based marketing, where you have 18 to 24 percent response rates. It's more economical for advertisers, it's more economical for the amount of money you spend, to only reach the customers who want to see the ad. It's permission-based, it's more economical, and it makes sense. There are early entrants into this.

So what we're doing is we're saying we're going to throw off privacy rights to protect one segment of the market that wants to profile as opposed to another segment of the market who wants to do it with informed consent and permission-based.

MR. MEDINE: Austin, before we go on to Jason could you just briefly explain what you mean, what CPM's are, just so people understand how that works?

MR. HILL: "CPM" is cost per thousand impressions. To give an example, average advertising, whether it's TV, radio, print, usually has an average cost per thousand impressions somewhere in the area of 5 to 8.

Obviously, the Superbowl is more expensive. Different places you advertise have different costs per thousand impressions.

A lot of the early banner ads were charging and still attempt to charge rates as high as $40 or $50 per thousand impressions, incredibly high. The basis of this was: Our response rates will be more targeted; because we're only talking to the customers who have an interest based on our profiles, we can justify this.

If you go through and read the S-1 documents, which is the IPO filings of most of the public ad tracking networks, you can find details where they talk about how: We're a
better company, we're worth more to the public, because we profile better, and that will lead to better response rates.

MR. ROBERT SMITH: David, can I ask a quick question along that line?

MR. MEDINE: You're jumping on Jason's time.

MR. ROBERT SMITH: I'm told it's an open secret that the meters that are used on web sites to show how many people visit a site can be manipulated and altered as the site operator wishes. Is that correct?

MR. HILL: Those actually, the counters, the site counters, don't have a lot of relevance when it comes to the ad tracking networks because they don't base it solely on how many times was this page loaded. They base it on how many times did this person with this cookie come back to this site.

So they can detect refresh rates, they can detect if someone is just visiting for a first time in a day. They have a lot more valuable information because they do attach a cookie to it, as opposed to solely how many times was this site loaded.

MR. ROBERT SMITH: But they can be reset with ease, isn't that correct?

MR. HILL: The site counters?

MR. ROBERT SMITH: Yes.

MR. HILL: The site counters can be reset.

MR. ROBERT SMITH: So they're deceptive inherently.

MR. HILL: Well, it depends how they're being represented.

MR. MEDINE: Jason.

MR. CATLETT: Let me pick up on Austin's comment about the economic effect, how the flood of money from Wall Street is causing these technologies to be developed. Wall Street hasn't found a way to value Internet companies.

Their usual method of seeing how much money they make doesn't work because they all lose money. So they started looking at traffic, and the trouble with traffic and measuring the number of eyeballs that a site gets is the bank doesn't take eyeballs. So they dismissed that one, and now sites say: Well, we've got registrations. So that's the current way. Really, when you think about it, the bank doesn't really want to take the registrations, either. They think that people are going to buy once they've registered.

So Wall Street has this perverse incentive to give companies the motive to collect absolutely excessive amounts of information and to get it in ways that are really scrambling. So the result of all this technology and money is a single terrifying fact: If you give your name to a single web site, then every other web site on the Internet may know who you are the moment you walk into their front door.

Now, once that message goes to consumers around the country they will realize that the Internet is a very unfriendly place and that e-commerce will be damaged far more than any measure of limiting targeting could possibly do.

MR. MEDINE: Jason.

MR. SHAPIRO: Just because -- you know, one of the things we've talked about here today which we believe the ad networks I know all share is very important is education. So it's important that when we say things in a public forum we say them accurately, and it's just not accurate to say that once you've given your name to one web site every other web site can know who you are. That's just not accurate.

Dan Jaye described this morning, cookies are domain-specific. They are only associated with the domain that is putting the cookie. So that means if you're at Amazon.com, Amazon can place an Amazon cookie, but Amazon can only read the Amazon cookie and they can only place an Amazon cookie on you when you visit Amazon. DoubleClick can only place a DoubleClick cookie and we can only place it on a site that's a member of our network.

MR. HILL: Sorry, Jonathan; that includes AltaVista. So if I go to AltaVista, I'm not going to DoubleClick, I'm not asking for DoubleClick to send a cookie. I'm going to AltaVista and I received, totally unbeknownst to me, I never requested that, I never typed it into my browser --

MR. SHAPIRO: Austin's right. When you visit any member of the DoubleClick network, DoubleClick will place a cookie on your browser. And what we use that cookie for is to identify that browser as a unique user. Today we do...
things like we ask the question: Well, how many
times has this unique browser seen this
particular ad? We use it because we know that if
you've seen an ad three times and you haven't
responded, then it's unlikely that you're going
to respond in the future, so we will frequency
cap the delivery of that ad to you.

So yes, if you visit a site in the
DoubleClick network we will put a DoubleClick
cookie on your browser, that's absolutely true.
But onlyDoubleClick sites and sites that are
participating in the DoubleClick network through
us can know or recognize that cookie. So it's
not fair to say that if you've given your name to
DoubleClick through Netdeals, as an example, that
every other site can know who you are.

MR. HILL: No, but it's also not
specific or accurate to say that only Amazon when
I visit Amazon can set or read a cookie, because
clearly if Amazon were to join the DoubleClick
network they now benefit from all.

MR. SHAPIRO: That's a great example.
That's a great example because even when, let's
say Amazon did join the DoubleClick network, even
if they were a member of the network, and I go to Amazon

and I buy a book, my personally
identifiable information is not passed to
DoubleClick. It's not given to us.
So yes, there's a DoubleClick cookie
there, but it's not associated with the
personally identifiable information that was
given to Amazon. So it is, again, it's just not
accurate to say that once you've given your name
to somebody on the web that everyone has it.
It's just not accurate.

MR. HILL: Speaking to Jonathan's
point --
MR. MEDINE: Jason.
MR. CATLETT: I think I said that
anyone could technically do it. I didn't say
everyone can do it now. If you want to see the
details --
MR. SHAPIRO: Well, technically, you
know, the phone company could give everybody
everybody's name and address.
MR. CATLETT: And some people are
doing it, such as Navient.com.
MR. MEDINE: Dan has been waiting and
he yielded a moment of his time, but not all of
his time.

MR. JAFFE: Thank you.
I think it's an interesting
discussion here, where people are trying to say
that they're going to decide how this should come
out economically, where I think really the
consumers should decide how it's going to come
out economically. If they don't want to click on
these ads, believe me, these ads are going to
disappear.

People are not just going to be
carrying on these practices for fun and for
economic waste. People are trying to use these
various means to sell products and to move the
economy forward. We are seeing all sorts of
companies that are taking on people who've been
around for a hundred years. Amazon.com is
clearly an example of that. One of the reasons
that people think that this can happen is that
they are going to be able to personalize, to have
one to one selling, to make selling more
relevant.
If that's not going to be the case,
by the way, I think that you're going to find the
Internet is going to not meet -- that all of
these great IPO's and others are going to be found to be

much less effective.
I would like to finish.
Second of all, the problem is not
whether people are giving information away. The
problem is do people know about it. As I said
earlier, the industry, the advertisers, want
their customers to be happy. They want their
customers to feel secure. They want their
customers to use these mechanisms.
The data says that some of them are
not using this mechanism, and not an
insignificant number, because they are concerned
and frightened, and therefore it is a tremendous
interest of business to help the consumer feel
secure. That's why we are pushing within our own
membership, many other groups are doing it to
get the privacy policies up on the advertiser's
site, up on the web page.
Now a point has been made, but there
are other players that people don't know about.
But who are these other players? They're not
free riders. They're working for somebody.
They're working for people who are known.
They're working for the Fortune 500 companies who
have a reputation and a brand to protect. Therefore,
<table>
<thead>
<tr>
<th>Page 166</th>
<th>Page 168</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 those companies are going to push to</td>
<td>1 marketing companies' advantage to help</td>
</tr>
<tr>
<td>2 see that these people become known and that</td>
<td>2 consumers, they're going to do it. But if it's</td>
</tr>
<tr>
<td>3 consumers are going to be able to protect</td>
<td>3 not to their advantage, if they can get advantage</td>
</tr>
<tr>
<td>4 themselves, because if they don't it's going to</td>
<td>4 from not helping consumers, they're going to do</td>
</tr>
<tr>
<td>5 undermine the economic model.</td>
<td>5 that, too.</td>
</tr>
<tr>
<td>6 I can't believe that anybody in this room can honestly say -- you know, there's all</td>
<td>6 Even if we've got on this panel a</td>
</tr>
<tr>
<td>7 this discussion, and I did take experimental</td>
<td>7 whole bunch of good actors, and even if the first</td>
</tr>
<tr>
<td>8 psychology, about Skinner boxes. I just don't</td>
<td>8 marketing groups that we're seeing online are all</td>
</tr>
<tr>
<td>9 think most consumers see themselves in a little</td>
<td>9 good actors, which they aren't, but even if we</td>
</tr>
<tr>
<td>10 box being shocked and stimulated. The consumer</td>
<td>10 say that they are, that doesn't mean that self-</td>
</tr>
<tr>
<td>11 thinks that he can make choice when he knows what</td>
<td>11 regulation is ever going to be the answer to</td>
</tr>
<tr>
<td>12 his choices are.</td>
<td>12 truly protect consumers.</td>
</tr>
<tr>
<td>13 So what we're trying to do is allow</td>
<td>13 There have been lots of cases in the past where it's to a marketing advantage to hurt</td>
</tr>
<tr>
<td>14 the consumers to have a fair shot and to make</td>
<td>14 consumers. Making the system transparent is</td>
</tr>
<tr>
<td>15 this process more transparent. Everybody in this room agrees that there needs to be more transparency. That is going to come because it's in the businessman's interest, it is in the consumer's interest. And if we don't do it, the government is going to step in, and many of us believe if they do in a fast-moving target they're going to miss the target, they're going to injure the whole process. So we know that if we don't self-regulate until you buy, and it's about writing the TV show show</td>
<td></td>
</tr>
<tr>
<td>16 so that people have a fair shot and to make</td>
<td>16 clearly going to be the answer, but we can't kid</td>
</tr>
<tr>
<td>17 transparency. That is going to come because it's in the</td>
<td>17 ourselves into thinking that marketing concerns</td>
</tr>
<tr>
<td>18 in the businessman's interest, it is in the</td>
<td>18 or businesses in general are going to be doing</td>
</tr>
<tr>
<td>19 consumer's interest. And if we don't do it, the</td>
<td>19 things that are against their own best interests.</td>
</tr>
<tr>
<td>20 government is going to step in, and many of us</td>
<td>20 It's only when the consumers' best interests and</td>
</tr>
<tr>
<td>21 believe if they do in a fast-moving target</td>
<td>21 the marketing companies' best interests intersect</td>
</tr>
<tr>
<td>22 they're going to miss the target, they're going</td>
<td>22 that they're going to act on behalf of consumers.</td>
</tr>
<tr>
<td>23 to injure the whole process.</td>
<td>23 Otherwise, there are going to have to</td>
</tr>
<tr>
<td>24 So we know that if we don't self-regulate until you buy, and it's</td>
<td>24 be other groups that are going to have to step in</td>
</tr>
<tr>
<td>25</td>
<td>25 on behalf of consumers in order to protect them.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page 167</th>
<th>Page 169</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 there will be regulation. And I'm</td>
<td>1 MR. MEDINE: Jeff.</td>
</tr>
<tr>
<td>2 telling you that even if there is regulation, you</td>
<td>2 MR. CHESTER: Millions and millions,</td>
</tr>
<tr>
<td>3 should be clamoring for our self-regulation,</td>
<td>3 tens of millions, of online profiles of you and</td>
</tr>
<tr>
<td>4 because the FTC doesn't have enough people,</td>
<td>4 me have been created, and they don't need to know</td>
</tr>
<tr>
<td>5 neither does the DOC, neither do the other</td>
<td>5 your name, they don't need to know your address,</td>
</tr>
<tr>
<td>6 governments around this world have enough people</td>
<td>6 but they know you. The technology has grown</td>
</tr>
<tr>
<td>7 to track this Net to protect the consumers.</td>
<td>7 dramatically in the last few years. It is now</td>
</tr>
<tr>
<td>8 So it's only self-regulation that is</td>
<td>8 part of the foundation of the next generation of</td>
</tr>
<tr>
<td>9 going to finally give the protection that you</td>
<td>9 the Internet.</td>
</tr>
<tr>
<td>10 need and that you want and that consumers demand.</td>
<td>10 That's why we think the Federal Trade</td>
</tr>
<tr>
<td>11 MR. MEDINE: Shari is next. Let me</td>
<td>11 Commission, a number of privacy groups including</td>
</tr>
<tr>
<td>12 just put on the table a comment that was brought</td>
<td>12 EPIC and Junkbusters and Center for Media</td>
</tr>
<tr>
<td>13 up in the written comments that were submitted to</td>
<td>13 Education and Privacy Times and Privacy Journal</td>
</tr>
<tr>
<td>14 the Commerce Department and the FTC, which is:</td>
<td>14 believe, that the Federal Trade Commission has to</td>
</tr>
<tr>
<td>15 We've heard about the beneficial uses of this</td>
<td>15 launch an immediate 90-day investigation into</td>
</tr>
<tr>
<td>16 technology in targeting consumers with ads that</td>
<td>16 these technologies. The information is there.</td>
</tr>
<tr>
<td>17 they might be interested in. Is there the</td>
<td>17 It's on the web site, it's in the SEC. It's</td>
</tr>
<tr>
<td>18 opposite risk, that there could be what's called</td>
<td>18 there about what this technology can do and the</td>
</tr>
<tr>
<td>19 electronic redlining or price discrimination,</td>
<td>19 attempt to change behavior.</td>
</tr>
<tr>
<td>20 where the same targeting process could result in</td>
<td>20 This really deserves an independent</td>
</tr>
<tr>
<td>21 some consumers not getting offers they would</td>
<td>21 and serious discussion. It's not just about</td>
</tr>
<tr>
<td>22 otherwise get or being charged higher prices for</td>
<td>22 giving people what they want. That's fine, but</td>
</tr>
<tr>
<td>23 the same merchandise based on their profiles?</td>
<td>23 if you read the literature it's very clear. It's</td>
</tr>
<tr>
<td>24 MS. STEELE: Yes, and that's exactly the point that I was going to</td>
<td>24 about changing the color and changing the song</td>
</tr>
<tr>
<td>25 get to. When it is to</td>
<td>25 until you buy, and it's about writing the TV show show</td>
</tr>
</tbody>
</table>

43 (Pages 166 to 169)
to have the e-commerce opportunity embedded.

Go to Veon.com, V-e-o-n, to link the psychological aspects of the individual with the emotional intensity of the editorial content.

Now, with broadband and the new system emerging, this system is always going to be on. One to one marketing and data collection and profiling and targeting are at the heart of what will be America's new media system in the twenty first century.

The technologies are there, they're off the shelf, and we're asking the Federal Trade Commission to get off the plate, investigate these technologies, and give a report to Congress right away about what the policy protection should be.

MR. MEDINE: Deirdre.

MS. MULLIGAN: Well, first, as an organization that both works on First Amendment issues, including commercial free speech, this is not about limiting people's speech. It is about limiting the collection of data without individuals' knowledge and consent, and that you can separate those things out and I think it's important.

I want to welcome Dan's call that industry wants to step forward and address this issue. I agree that self-regulation is part of the puzzle here. I think one of the things that is important to reflect on is that if each one of us at this table operated an independent web site and we wanted to create the kind of profile that DoubleClick or 24/7 creates, we would both have to collect information that was personally identifiable and we would have to disclose it, right, in order for us to do that independently.

So in that area I think the industry players who have stepped up to the table said that we need notice, which means clear and conspicuous notice prior to the collection of data; we need consent, at the very minimum the ability to limit the use of data, particularly the disclosure of data, for secondary purposes, which is clearly what targeted advertising of the type that you're talking about is about.

Now, I think just on those two points, it is very, very difficult to figure out how a consumer looks at this medium and finds that, even by this minimal standard that we're talking about, notice and consent, is going to feel like their interest is being addressed here.

I think most consumers -- as we said, this is not transparent. They have no knowledge of who they're dealing with or that data's being collected. They certainly don't understand the extent of the profiles that are being created and they certainly haven't given their permission by any stretch of the imagination.

So I think I welcome the effort and the goodwill that you bring to the table. But I'm saying this is an enormous area, and I don't think that an after the fact opt-out is going to address this problem. So I welcome other people's thoughts.

MR. MEDINE: Solveig.

MS. SINGLETON: I'd like to begin by going back to Fred Cate's question and just say briefly that, having heard now arguments about some of the harms, that it still seems to me that most of them are of sort of a vague philosophical nature and, especially insofar as we're hearing from consumers on this issue, it does seem that those fears of the technology may be simply stemming from ignorance rather than an understanding of any real harm that might arise from people collecting information on you and wanting to sell you something.

The second point I'd like to make goes back to some of the discussion of the benefits. It seemed to me that sort of implicit in that discussion was the idea that the benefits are primarily benefits to business or to industry or to companies that want to market things. I think there's a certain important area of benefits that are being overlooked here, and that is benefits to consumers.

One of the things that used to be believed about advertising, for example, back in the 1930's and the 1950's was that this was essentially wasteful information, it simply made people buy things that they didn't want to buy, that it was manipulative and so on. But empirical studies of advertising that economists have done since then have shown that advertising plays a big role in terms of market results in delivering information to consumers, that is at a lower price, delivering goods that are of better quality, and giving them more choices.

So when you compare markets where advertising is restricted to similar markets
where it is not, consumers benefit a tremendous amount from getting the kind of information they're getting through advertising.

A final point about the sort of self-regulation, regulation, consent issue. I take a somewhat, I guess, a broader view of free speech than necessarily everybody on this panel does, but I think that essentially there is a free speech issue here, because what you have businesses doing is collecting facts and information about real events that were involved in. It's unclear to me why they should be restricted, in a sense, in this use of this information.

With respect to the consent and notice point, the market is definitely moving in that direction, particularly where the uses of information that are going to be made are controversial or fairly extensive. But nevertheless there would remain areas where that model doesn't necessarily work very well.

An example might be credit reporting. It's difficult to see how a service like that could exist if people were opting out of it every time they had a bad loan payment, that kind of thing. That's a very simple example, but there are many kinds of services, many kinds of business models, where it would be simply legitimate for companies to make use of information about real people and real events without necessarily getting consent.

So I think it's really important, whatever model is ultimately adopted here, to retain flexibility for new business models to spring up, so goods and services continue to come into existence which might otherwise not even be possible to be created.

MR. CHESTER: Can I respond to something she said?

MR. MEDINE: There's a question from the audience and I want to give people a chance. One is actually a credit reporting-related question, which I want to ask either Jonathan or Jason to respond to, which is: Consumers have rights to access copies of their credit reports and examine them for accuracy. Can or should consumers do the same with regard to their online profiles?

MS. HURLEY: The answer to that is an easy yes. If you read the privacy policy on most network advertisers and on 24/7, you have access to the information collected about you. If you volunteer personally identifiable information, you can review it, you can have it retracted, edited, at any time that you like. So that's an easy answer for that.

I'm glad that Solveig pointed out that we're overlooking -- the purpose of this panel here was what are the benefits, and it's not only to advertisers and web sites --

MR. ROBERT SMITH: Could I ask for a point of order: The purpose of the panel was what?

MS. HURLEY: Okay. Back on the point, the benefits are also overwhelmingly to the consumer. The point that we're at now is the advertising industry is growing as well as all technology industries and, going back to when people were captive audiences in the movie theater, people said: Hey, let's talk about it; why is this good, why is this bad? It eventually came to a consensus that people can handle that; they're informed; it works.

So we're at that point now where we have to get the message out to consumers what we're doing, what we're doing with your information, how we collect it, and how they have a choice in the matter at all times.

MR. CHESTER: I want to respond to that.

MR. MEDINE: Time is at a premium. Let me ask one more question and then we'll have a response. This is for Jonathan from the audience: What is the purpose of merging DoubleClick and Abacus if you are not merging online and offline data on the individual, in other words collecting non-personally identifiable information online and merging it with personally identifiable information offline?

MR. SHAPIRO: Okay. Let me be clear. We today do not have personally identifiable information associated with cookies. However, in the future we do intend to link offline information with online information. Again, what we are trying to do is deliver on the promise of
1 putting the right ad in front of the right user
2 at the right time.
3 We think that's what's going to work
4 for the user. Now, we are only ever going to
5 capture that personally identifiable information
6 in places where the user is given notice, and as
7 part of that notice they will be given the choice
8 to participate or not. If they choose not to
9 participate, if they opt out of the DoubleClick
10 cookie, then there's no way for me to link that
11 personally identifiable information with their
12 online behavior. I can't technically do it.
13 That's really the crux here.
14 Dan said it. I think Deirdre was
15 getting to it. This is about the consumer and
16 giving the consumer enough information, enough
17 notice, and then the tools to make the choice
18 that's most appropriate for them. It's not about
19 us deciding what's appropriate for the consumer.
20 MR. HILL: Just a quick question for
21 Jonathan on that. Your privacy policy on
22 DoubleClick's network did state that these were
23 anonymous profiles being created and was
24 certified by TRUSTe and talked about how there
25 was no personally identifiable information. Are

1 you going back to consumers now and telling them
2 that they can now opt out of that with the merger
3 of Abacus personal information?
4 MR. SHAPIRO: When we associate
5 personal information with that cookie, we
6 absolutely are going to provide the user the
7 notice that we're doing it and the choice. I
8 mean, I can read from the Netdeals site if you
9 like, but it says very clearly we are going to
10 link, we're going to capture your name and your
11 address, your e-mail address, we're going to link
12 that with online and offline information, and
13 we're going to use it to target advertising to
14 you.
15 MR. HILL: Just a follow-up question.
16 Being that most consumers on the Internet don't
17 know who DoubleClick is, they have no idea who
18 you are, and they know you only through your
19 partner site, how much money is DoubleClick going
20 to be allocating to reaching consumers, letting
21 them know that there is this profile, we just
22 merged with Abacus and you have an opportunity
23 now to opt out? Have you set a budget for that?
24 MR. SHAPIRO: Let's get back up and
25 get very specific on the technicalities. I can't

1 just take Abacus data and link it to all the
2 DoubleClick cookies. It's not technically
3 possible. The only way to technically link any
4 of the Abacus data with a cookie profile is after
5 I've captured the person's name and address, and
6 the only way -- I've said it and I'll say it
7 again -- the only way we're going to capture the
8 name and the address is when the user volunteers
9 it.
10 When they volunteer it, either
11 because they are registering or they're
12 purchasing, it's at that point that they will
13 have full notice and choice. They'll have the
14 choice right then to say, you know, I really
15 don't want to participate in this, or the choice
16 to say, fine, let's go forward.
17 But before we can actually link any
18 of that data up, the user technically has to be
19 given notice and choice. I have to do it in a
20 place where I give them notice and choice.
21 MR. HILL: Then you haven't dedicated
22 any money to informing customers about who you
23 are?
24 MR. SHAPIRO: We have spent lots of
25 money putting up on our web site our privacy

1 policies. We've got a web site called Adchoices
2 that we've developed, we've invested in
3 developing, that describes privacy policies, that
4 describes cookies, that describes the choices
5 that users have.
6 So we've made adequate investments to
7 date and we'll make more going forward.
8 MR. MEDINE: Deirdre and then Dan.
9 MS. MULLIGAN: A while ago, an online
10 service provider which had said that they were
11 not going to engage in a certain activity, in
12 this case telemarketing, decided that they were
13 going to change their terms of service and
14 provide an opt-out. I think they heard pretty
15 clearly from both the public and from advocates
16 that that was what we call kind of a fundamental
17 change in the terms of service, kind of like
18 somebody gives you a 5.5 percent mortgage and
19 then later on sends you a notice and says: Well,
20 we've changed it to 7.5; let us know if you don't
21 like it.
22 I think what you're talking about
23 here is you've collected information from
24 individuals with a very specific statement that
25 you were not going to attach it to their
1 identity, and I think if you want to then after
2 the fact engage in a business practice that's
3 based on attaching it to identities that you have
4 to get their consent, they have to opt in. I
don't think an opt-out is going to pass the smell
test.
5 MR. SHAPIRO: Deirdre, we haven't,
6 again --
7 MS. MULLIGAN: I'm saying if.
8 MR. SHAPIRO: But we can't. The only
9 way -- I agree with you. Here's what DoubleClick
10 is committing to --
11 MS. MULLIGAN: I understand what
12 you're saying. It's when I go to register there
13 will be a little thing saying: If you don't want
14 this to become part of your DoubleClick,
15 opt out.
16 MR. SHAPIRO: Yes.
17 MS. MULLIGAN: And I'm saying it
18 should say: We would like to give this to
19 DoubleClick; can you please opt in? It's a
20 fundamental change that has enormous -- the
21 extent to which all the businesses in this
22 discussion of gone to strip out personally
23 identifiable information from aggregate data
24 about a specific individual highlights what a
25 fundamental issue this is. I think a fundamental
3 term like that changing is something that really
4 merits an explicit consent.
5 MR. SHAPIRO: We think that there is
6 a difference. But again, the only people for
7 whom this is going to be a relevant difference is
8 anybody who has volunteered their name and
9 address. If they volunteered their name and
10 address, it's at that point that they're going to
11 get notice and choice.
12 So for everyone for whom this has
13 really changed, they will be fully notified and
14 they will have the opportunity to opt out. We
15 agree with you, we think that's crucial, that
16 it's important to give the users the notice and
17 choice.
18 MR. MEDINE: Dan.
19 MR. JAFFE: I just hope that when
20 people leave this workshop that they not forget
21 that what we are dealing with is probably, as the
22 Secretary said, a historic development, a
23 development -- he talked about the trillion
24 dollar economy, the future, as I understand it,
25 of United States economic health, that you're
26 really talking about something that can have
27 profound economic competition, innovation values.
28 If you're in a small town, you
29 suddenly are having options that you never had.
30 Up until then you had that one store or two
31 stores or three stores to choose from. Now you
32 have the whole of the world and it's suddenly
33 competing with those two or three stores.
34 When we talk about redlining,
35 redlining is a real problem. We're not talking
36 about setting up a situation where online or
37 offline you're going to have an absolutely safe
38 world.
39 My concern when the whole Internet
40 got developed was that we were going to really
41 have an information-stratified society. I
42 thought that was the real danger, because it
43 looked like we were going to a subscription
44 approach. What does a subscription approach mean
45 if you depend on it? It means those with money
46 get the information and those people without
47 money don't.
48 What's happening is that the Internet
49 is opening up incredible information to our kids,
50 to ourselves, to all that will come after us, and
51 at very low prices.
52 MR. CHESTER: I do have to say,
53 though, being a children's group, we have real
54 concerns about the industry, not this particular
55 part of the industry, but tyeing access into
56 having the child and having the family watch the
57 ads and giving computers to schools, school
58 libraries, forcing the kids to watch the ads.
59 We're not against advertising. I
60 want to make that clear. But advertising has
61 taken a fundamental shift over the last few years
62 with the development of these personalization
63 technologies that allow this unprecedented
64 individual tracking and profiling and potentially
65 behavior modification.
66 You have to link the technologies
67 with the online advertising campaigns designed to
68 get consumers to change behavior and to use
69 various psychological and other kinds of
70 psychographic and demographic approaches to
71 change behavior, and you need to make all of
72 these extremely transparent.
73 In terms of the First Amendment, I'm
74 not so sure that this in fact amounts to unfair
75 and deceptive practices, because when they know
On-Line Profiling Workshop

Washington, DC

November 8, 1999

Page 186

1. that you really like the color red -- and I was
2. at Digital Commerce '99, at a conference. It was
3. two days about how to embed e-commerce in the
4. narrative. You should go to Silicon Valley
5. Reporter and look up the transcript if you want
6. to see what's coming.
7. But in fact the strategies are there
8. to do the profiling, to steer you, to give you
9. the prizes, to give you the incentives, to
10. provide the information without necessarily
11. knowing that it's going to be linked, and these
12. little profiles are being built one by one into a
13. digital Kafka-esque nightmare.
14. MR. MEDINE: Dan and then Brad.
15. MR. JAFFE: I just would like to say
16. that, remember that the laws of this country have
17. not suddenly been stopped by the creation of the
18. Internet. If there are unfair acts or practices,
19. if people have statements of privacy policies,
20. they will then be held to false or deceptive
21. requirements. It's not like we just have a free
22. fire zone here.
23. I also want to say that the consumer
24. is not quite as helpless as is being described
25. here. The consumer can make his choices when he

Page 187

1. knows what choices he's been given to make.
2. I really don't care if people know a
3. tremendous amount about me. I don't care if they
4. know what kind of Rice Krispies I have or what
5. kinds of clothes I wear. I just don't think that
6. they can psychographically from all of that just
7. manipulate me like putty in their hands. But if
8. they can, more power to them, because people are
9. going to find this information out about you.
10. In the real world privacy is not the
11. same thing as invisibility, and that's what we're
12. going to really start demanding so that people
13. can't target effectively. You're going to always
14. have an inefficient market.
15. What I find amazing, because I
16. usually happen to be talking about the mass
17. media, and what you hear is everybody
18. complaining: Oh, there's so many of these ads
19. and they're so irrelevant and they go on for so
20. long; isn't that terrible. Now we say: Oh,
21. we're going to start giving you ads that are
22. relevant, that are meaningful, that actually have
23. something to do with your real life and your real
24. choices; and everybody says: Oh, but those are
25. going to be so powerful that you're going to be

Page 188

1. helpless and they're going to psychographically
2. manipulate you.
3. MR. CHESTER: But consumers deserve --
4. MR. JAFFE: You've got to start
5. deciding what you want.
6. MR. CHESTER: No, it's not an either-or
7. choice, Dan, for consumers. What the industry
8. has to do is to have opt-in and you have to make
9. all these practices transparent, and there needs
10. to be a serious investigation that looks at these
11. technologies very closely and determines which
12. ones are unfair and deceptive, particularly when
13. it comes to children and teens.
14. MR. MEDINE: We have time for two or
15. three more comments. Brad.
16. MR. ARONSON: A couple things. First
17. off, I don't think anyone's forced to look at
18. ads. Just like in magazines and TV, the ads are
19. there and you look at them or you ignore them.
20. And as you put down, response rates aren't always
21. that great, so a lot of people ignore them.
22. We're not manipulating them like that.
23. Then also everyone's talking about
24. these in-depth profiles. The reality is that
25. right now on the Net I can say I want to make

Page 189

1. sure this ad goes to people and they'll only see
2. it three times, and my clients love it because we
3. know that we're getting a certain frequency. I
4. can also say I want to target my ad for ESPN to
5. someone that's looked at sports content. That's
6. very good profiling. We know that it's someone
7. who's going to be interested in an ad for ESPN.
8. The types of things you're talking
9. about, everyone's saying that they're here. It's
10. not really possible to do all that yet, and
11. that's kind of why it's a good thing that we're
12. talking about it now, because there is the
13. opportunity to shape how we're going to move
14. forward.
15. But again, I want to stress, we don't
16. know what's next. So having dialogue and coming
17. out with self-regulation as far as how we want to
18. control what happens gives the advertisers and
19. the consumers what they need.
20. MR. CHESTER: Yes, but Engage's
21. profile includes over 800 attributes, 800 to
22. accurately get a picture of a visitor, in all
23. kinds of categories -- huge amounts of
24. information, updated daily, cross-referenced.
25. The Internet has developed the same
kind of business advertising model of television, syndicated across the entire web. None of these are transparent to the individual.

MR. ARONSON: I agree there definitely needs to be transparency. But what you're looking at for targeting is that you want to target to someone who has shown interest. It's not the type of psychological targeting that people think that we're doing right now.

MR. CHESTER: But it is psychographic, right?

MR. MEDINE: Okay, our time is up. Two more comments. Jonathan and then we'll close on an academic note with Fred.

MR. SHAPIRO: I just wanted to bring this back. This is about the user and the consumer. The research suggests that the majority of users do want to receive tailored information, targeted advertising. We recognize again that the majority doesn't mean everybody, so that the important point here is that the users get notice. This is a transparency issue. We agree we as an industry have to do a very good job about educating the user about what's really going on and then giving them the choice, providing them real notice and real choice around whether they participate.

MR. MEDINE: A final remark.

MR. CATE: I have to say I'm left at the end of this with something of a feeling of so what, that the harms that we have discussed, the little discussion we've had of harms, have tended to focus primarily on this: I'll respond to advertising if you show me these ads; if you give me the color I like, then I'm more likely to respond. That's what we've been doing forever. There's nothing new about that. That's what universities do. That's what people in grocery stores do. There's nothing new about that.

We've asked one question and that is it manipulation? Subliminal advertising, as Robert said, clearly manipulation. The FTC has said you can't do it. The FTC has said you can't do it.

In this case, we're asking about collecting information for uses that so far, which is not to suggest that there may be no harms, but rather that so far we haven't targeted the sort of harm that would justify, particularly an opt-in requirement, something that you can only think of maybe three examples of in all of U.S. law, that this would be the fourth example, this with children's privacy. The FTC is going to come to my home, protect me on the web. Maybe you can set my VCR as well while you're there.

MS. BURR: Just the clock part.

MR. ROBERT SMITH: I've got a whole list of problems with this profiling and the question was never asked. The question was asked today, what are the benefits of this technology.

So we've got them if anybody wants to hear them.

MR. MEDINE: Thank you very much, all of you, for the discussion. The record does remain open until November 30th.

For those who have not passed out for lack of lunch, there are flyers outside about local lunch places. Thank you. We'll resume at 2:30.

(Whereupon, at 1:02 p.m., the workshop was recessed, to reconvene the same day.)
As we were designing Freedom, the idea was to come up with a couple different solutions to the problem of privacy on the Internet. One of the big things with Internet privacy is the idea that the actual infrastructure, the underlying TCICP protocol, this is something that was designed 25 years ago and kind of got out of the lab. It wasn't something that people said, we're going to put medical records online, we're going to do commerce and shopping. Everything after that has just been layered on top.

We employ a bunch of really bright cryptographers who look at how do we design networks so that the network privacy is built into the infrastructure, so it's not something that afterwards you try and layer on top of, but you can actually build it into the protocols.

So one of the key parts of this is something we call the Freedom Network. Now, the Freedom Network builds on the idea of separating out information about a user from where they're going online. Just because you're using a public network doesn't mean you want everyone in the public to know what you're doing.

So one of the things we do is, a consumer goes to browser the Net, if they have our Freedom software installed we relay all their packets with different layers of encryption through a series of servers around the world. What this ends up doing is making sure that no one, not even Zero-Knowledge, knows the identity of the customer as they go online.

That's the start. That's the infrastructure. So this is an example of how a packet would transfer or be formatted. There are multiple layers of encryption, and as the packet leaves the computer we have wrapped it with a different layer of encryption for each one of the servers.

So it leaves the client's PC and it goes to one of the first servers. That first server only knows the identity of the client PC. It then sends it on to another server. That server then passes it on to the final server, which would connect to the end web site. So now the client is browsing and he appears to be coming from the final server. So there's no linkage to the client's actual IP.

This becomes real important as we look at things like static IP addresses, IP Version 6 that has unique identifiers, because it allows the user to separate out the identity at an infrastructure and a technical layer so that the network itself doesn't reveal or compromise our identity, the same way walking around on the street does not compromise our identity. We may choose when we walk into an establishment to identify ourselves with a loyalty card or a credit card if we want to pay that way, but simply by walking down the street we're not giving up any privacy.

So the goal of the Freedom Network is to establish that first basis. Then on top of that we talk about separating out identity and building an identity management system. Now, the goal behind our identity management system is something we refer to as "Nyms," "Pseudonyms."

Now, the goal behind Pseudonyms is to be able to establish online personas that are separate and unique from your real identity.

The idea that we're going to establish in the future a single identity system that acts as a national passport is very against privacy.

But at the same time, for transactions like commerce, applying for health information online, insurance applications, we need better forms of identity. We need a way that we can certify who we're talking to. A lot of those situations, it's a true identity certification. For instance, we're not going to ask our doctor for X-ray information under our handle "Looking for a Date at Hoffman's." You want a true identity if you're going to be asking for health care information. But a lot of uses, let's say for instance talking about health care concerns or you're taking part in a support group online, you don't want it associated with an insurance application. You don't want it associated with all your activities.

So Zero-Knowledge promotes the idea of being able to separate out your identity so that you have a unique identity for each one of your online activities. Now, Zero-Knowledge does that by establishing these Pseudonyms, and I'll give you a quick example of how these Pseudonyms work.
I just have a web page. I think that's Richard Smith's work. (Pause.) We're waiting for the demo. There we go. Okay, so this is Freedom. You'll see that it's sitting in a toolbar just beside my browser. I have the ability with a pulldown menu to select one of my identities. Each of my identities is completely unique. It has its own e-mail address, its own cookie file. It is completely separated from any of my other identities, the goal being I can create an ID, "Cancer Support at Freedom.net," and that's separate from anything I do with e-commerce, and I know that my activities cannot be profiled across ID's. Part of how we do that is we maintain and separate out information. This is an identity called "Half-Finger," so you have an icon representing it. So there is the e-mail address. You can define your security settings for how much encryption you want, so you can trade off speed versus performance. We can also look in the cookie folder, and if you look into the cookie folders with this Pseudonym you can see all the cookies and you can selectively block per site or you can block all cookies. So under one of my identities where I have a higher concern for privacy, let's say health care activities, I might choose to block all cookies, where under another one of my identities I might choose to only block cookies from ad-serving networks, but accept a cookie from Yahoo.

So it allows the user to selectively choose which cookie they want to receive. At the same time, if we go into another one, another identity, and we look at the cookies, the cookies are completely separate for that different identity. So what we're allowing users to do is gain the benefits of technologies like cookies, digital certificates -- each identity has a digital certificate and can authenticate itself -- but not have to compromise their true identity, which is a really important innovation, because the idea on the Internet is not for everyone to be anonymous.

Total anonymity fights back against community. We want to establish relationships. We want people to know who we are. We want to maintain loyalty with a brand. If we're buying or frequenting the same establishment over a long period of time, that organization might want to give us discounts, loyalty reward programs. But by using a pseudonym-based relationship that is separate from your true identity, it stops the abuse of that site exchanging your data with another, because every partner and every person you interact with you can manage your identity set, so you don't have to compromise more than you are planning to.

MR. MEDINE: Thanks very much, Austin, for an example of how the technology can address some of the concerns that we've heard about throughout the day. I want to turn now to Jerry Cerasale from the Direct Marketing Association. Jerry's certainly a veteran of the FTC and Commerce Department workshops. He's the Senior Vice President for Government Affairs of the Direct Marketing Association, which seeks to raise the bar for privacy practices by assuring that its members adhere to certain privacy practices.

REMARKS OF JERRY CERASALE, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, DIRECT MARKETING ASSOCIATION

I'm in the process here of just setting up my computer. Let me talk to you very briefly before I show you this very simple, this very simple demonstration. One, why DMA has placed this? As you can see, I'm not technologically literate here, so this is going to be a very non-technical operation.

What's coming up is a panel on self-regulation and the DMA is very much a proponent of self-regulation. In July we required a privacy promise to be a member of the DMA and any member of DMA in any form, any medium that collects information, personally identifiable information, and transfers it to third parties must let the consumer know and must give them opportunity to opt out. I think that's the situation as we look at what we're talking about here today, is ad servers, and we don't think it's very different for them, either, in a situation where you go to a web site and then turn onto, click onto a banner ad. You're really in a situation
<table>
<thead>
<tr>
<th>Page 202</th>
<th>Page 204</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 where there are three parties at play. There is 1 relationship between the consumer and the third 2 the web site that you're visiting, probably the 2 party ad server. So that's the real important 3 publisher. 3 thing that we're trying to push here. 4 I don't know if this is going to work 4 The DMA in 1997, in trying to help 5 here. 5 people put privacy policies on their own web 6 (Screen.) 6 site, created a privacy policy generator at our 7 Yes, it does. 7 web site. You just answer a few questions and it 8 The web site that you're on is the 8 will print out what your privacy policy is. 9 publisher and you have the advertisement, the 9 Well, 1997 is a long time back in Internet time, 10 advertiser whose ad you click on, and then you 10 so we've decided it needed to be updated, and ad 11 have an ad server that's between that. Clearly, 11 servers is clearly one of the areas where we want 12 you know the web site you're on and they would 12 to update. 13 have a privacy policy. You know the advertiser 13 So we've added a few things to it: 14 you clicked to and hopefully they have a privacy 14 whether or not you use cookies and things on ad 15 policy. 15 servers; if you decide to change your policy on 16 But it's likely that you don't have 16 how you're going to use information; access and 17 the foggiest idea who the ad server is. So we 17 correction; and security and some form of 18 took a look at that and said, how do we get 18 reinforcement -- of enforcement, excuse me. 19 notice and choice, which is the key to the DMA's 19 What I'd like to do is take you, if 20 privacy promise? We believe the place to give 20 this thing will move me there, to the DMA privacy 21 notice in the first instance falls on the 21 policy generator that is on our web site. 22 publisher, the web site that you originally go 22 (Screen.) 23 to. They already have the obligation, if they're 23 This is it. These actual forms will 24 DMA members, or they should have the obligation 24 not be up. The web site is up, but item number 4 25 if they collect personally identifiable 25 -- excuse me -- item number 5 will not be up</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Page 203</th>
<th>Page 205</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 information themselves and give it to third 1 until later this week, whether or not you collect 2 parties, including the ad server; they must 2 cookies. We didn't have anything on it before in 3 disclose it and give you an opportunity to opt 3 1997. We think it is important to let people 4 out. 4 know whether or not you place a cookie, not 5 We think that they should also 5 collect cookies, excuse me; and if you do place a 6 disclose to you whether or not they have any 6 cookie, what use you put it to. 7 relationship with a third party ad server and to 7 So you can see the checklist. I 8 let you know that the third party ad server may 8 don't know if you can read it. You just click on 9 be independently collecting information on them, 9 &quot;Yes, I collect cookies&quot; -- &quot;I set cookies,&quot; or 10 and to give you a hot link to the privacy policy 10 &quot;No, I don't,&quot; and then what uses you put it to. 11 of their contractual third party ad server. 11 Then there's an &quot;Other&quot; policy there where you 12 From the ad server's point of view, 12 can add it in. So we would hope everyone would 13 we think that they have the obligations that any 13 answer that. 14 DMA member would have, that they provide notice 14 Then we go down to these other 15 to the types of information they collect, what 15 privacy policy statements here, like name, 16 they do with the information, and if their 16 address, e-mail addresses, phone numbers, 17 navigational data is to be used in an 17 etcetera. Those were all on our 1997 web site. 18 identifiable manner by the ad server that should 18 We've added this other one, &quot;Ad servers,&quot; whether 19 be disclosed. And there should be an opportunity 19 or not you partner with someone, and if you do to 20 of choice for the consumer. 20 make a statement that in fact you do partner and 21 It's that simple: Let the consumers 21 that they may collect information on you. 22 know and give them a choice. The point of view 22 I've typed in, not to dump on any 23 here is what's different with this situation is 23 company, &quot;www.jerry.com&quot; in order to show you in 24 when do you give them notice and who should give 24 a later slide what the privacy policy said. But 25 them notice, because you don't have a 25 that would be there, and we'll try and make a hot</td>
<td></td>
</tr>
</tbody>
</table>
We also added item number 12, which has to do with dual uses. I think that was something that came up in the panel this morning, that we suddenly have a privacy policy, I've seen it and I've given some information out, and you decide to change that privacy policy. You decide to change the uses, how you're going to let people know, etcetera, and this is a series of questions telling you what you will do and how to notify the web site.

Another question that constantly comes up is access, whether or not you allow access, what information you can see. You can see down at the bottom the last click there is "No information that we have collected and that we maintain about them," so that you do have the negative option, you do not allow access. But these are things that you can check off, and it's not one or the other; it's all that apply, in the hope that we can make it easy for not just larger companies, but all companies who have a web site, to go someplace, answer a few questions, get a privacy policy that's fairly comprehensive about what they do, and give it to their attorneys to switch things around, but then can quickly get it up on their web site so that we can get information to customers and consumers so they know what's happening and have some choices, because we want e-commerce to continually grow, and the only way it's going to grow is if there's consumer confidence and consumer confidence comes from knowing what the web site is doing with information.

Besides, if you sell something you've got to deliver the product and it has to have good quality. But really, the idea is we want people to go searching on the web and taking a look at our privacy policies.

Finally, we put out what kind of security we have on the web site. We have some additional questions in there about financial and medical information that you can see, and you'll be able to go to that web site and take a look at it if you'd like.

Then on enforcement, if you have a complaint where do you go. We put the DMA on there. We added the FTC. I didn't put David Medine's phone number on there, just a general phone number. I was tempted to put David's on there, but we didn't do that. You're quite welcome.

So that's pretty much where it is.

As you can see, way down at the bottom you can generate this web page in HTML, you can e-mail it, you can make it in hard copy, and so forth. We do ask people to e-mail a copy to the DMA so we know how many people use it. I'm not sure how many people do that for us, but we do get a few of those and know people have done it.

That's pretty much what we have done to try and make it so that customers have an opportunity to know if information is being collected, to have an opportunity to say, no, don't do it. And hopefully, with this understanding we can make the web experience rewarding, that people will not be afraid to go surfing on the web, that they will not be afraid of data that's not personally identifiable, that helps them enjoy and get to places without re-registering, don't see repeat ads, etcetera, and not be afraid of it.

Thank you very much for your time and thank you, David, for having me.

(Applause.)
1 TRUSTe.
2                MR. CERASALE: Jerry Cerasale, Senior Vice President, Government Affairs, with Direct Marketing Association.
3 MR. ROBERT SMITH: Robert Ellis Smith, Publisher of Privacy Journal.
4                MR. CATE: Fred Cate. Because I was confused, they invited me back.
5 MR. HENDRICKS: Evan Hendricks, Editor and Publisher of Privacy Times.
6                MR. KAMP: John Kamp, Senior Vice President, the American Association of Advertising Agencies.
7 MR. LUCAS: Steve Lucas, Senior Vice President from Industry and Government Relations, PrivaSeek.
8                MR. LORDAN: Tim Lordan with the Online Privacy Alliance.
9 MR. SHEN: Andrew Shen, Policy Analyst, Electronic Privacy Information Center.
10 MS. BURR: I don't know if it's intentional or not, but we seem to have segregated the tables here. So I'm going to turn to the table on my right.
11                We've heard a lot of very interesting things today about this technology, about its benefits, about the concerns that it raises with Internet users. The topic of our panel this afternoon is how self-regulation can help in this area.
12                So I'd like to talk to the companies and ask, what do you think?
13 MR. JAYE: Thank you. On behalf of my colleagues in the Internet network advertising business, I'd like to thank the Federal Trade Commission and the Department of Commerce for the opportunity to participate in today's workshop. (Slide.) Earlier this year, a group of companies in the Internet advertising business began talking with government officials about issues surrounding advertising on the Internet. They included 24/7 Media, AdKnowledge, AdSmart, AdForce, DoubleClick, Engage, Flycast, MatchLogic, NetGravity, and RealMedia.
14                The first thing to know about our companies is that they are not mysterious entities taking profiling technologies to dizzying levels which threaten consumer privacy. Nor are they gathering data in a deliberately secretive way. Our companies are among the leading providers of advertising solutions to web publishers in advertisers, and the services we offer have substantial economic benefits for both consumers and companies.
15                According to Dr. Westin's most recent survey, we are providing services that most consumers want to receive using technology adapted to the Internet. For example, most smaller and medium sized web sites use our services or similar services, and it's very important to preserve the ability to deliver effective services via third party ad servers to allow these medium and smaller sites a chance against the larger portals and the larger, more established sites.
16                The goal of the group was to explore ways in which we could collectively address the types of consumer concerns and perceptions about profiling that we have heard this morning.
17                Although our companies do not deal directly with consumers on the Internet, we believe we can play an important role in increasing consumer confidence and contributing to the growth of electronic commerce.
18                To that end, we in the industry are announcing the launch of the Network Advertising Initiative, NAI. Our goal is to develop a framework for self-regulation of our industry. We believe our industry is distinctive because we have no easy way to communicate directly with consumers. Our business is not to make our own web sites known to consumers. Our business is to make our customers' web sites more useful to consumers.
19                To do that, we provide a wide range of advertising solutions to consumer-oriented web sites, to support their development and growth. Elizabeth Wang will talk in more detail about what we have been working on. MS. WANG: Thank you, Dan. As many of the commenters today have pointed out, there are significant benefits to Internet advertising for consumers and the industry. For consumers and web sites, it is the reason why content on the web is available for free or for nominal cost. For advertisers, Internet advertising takes advantage of a medium uniquely suited to delivering the right message to the right consumer at the right time.
<table>
<thead>
<tr>
<th>Line</th>
<th>Page 214</th>
<th>Line</th>
<th>Page 215</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Our companies use technology to help</td>
<td>1</td>
<td>We believe that education is the key</td>
</tr>
<tr>
<td>2</td>
<td>advertisers deliver tailored messages to</td>
<td>2</td>
<td>to developing consumer confidence on the</td>
</tr>
<tr>
<td>3</td>
<td>consumers. In fact, every consumer who uses the</td>
<td>3</td>
<td>Internet, and for that reason our companies are</td>
</tr>
<tr>
<td>4</td>
<td>Internet has likely seen the banners and other</td>
<td>4</td>
<td>committed to educating our business customers</td>
</tr>
<tr>
<td>5</td>
<td>advertising our companies deliver.</td>
<td>5</td>
<td>about the data collection and use issues</td>
</tr>
<tr>
<td>6</td>
<td>As Dan Jaye and Martin Smith discussed this morning, the NAI companies</td>
<td>6</td>
<td>associated with Internet advertising. This</td>
</tr>
<tr>
<td>7</td>
<td>collect information in order to make decisions on which</td>
<td>7</td>
<td>includes the benefits of both the responsible</td>
</tr>
<tr>
<td>8</td>
<td>ads to send to whom. Some NAI companies create</td>
<td>8</td>
<td>flow of information and fair information</td>
</tr>
<tr>
<td>9</td>
<td>profiles about consumers in order to tailor that</td>
<td>9</td>
<td>practices.</td>
</tr>
<tr>
<td>10</td>
<td>message. As Dr. Westin's survey demonstrates, most consumers want a</td>
<td>10</td>
<td>We are also committed to educating</td>
</tr>
<tr>
<td>11</td>
<td>more relevant message and</td>
<td>11</td>
<td>consumers about data collection and use issues</td>
</tr>
<tr>
<td>12</td>
<td>are willing to accept profiling, but they also</td>
<td>12</td>
<td>associated with Internet advertising. As Dr. Westin's survey clearly</td>
</tr>
<tr>
<td>13</td>
<td>want to be given notice about the information that</td>
<td>13</td>
<td>indicated, most consumers are</td>
</tr>
<tr>
<td>14</td>
<td>is collected and used and a choice not to</td>
<td>14</td>
<td>are willing to share information, even personal</td>
</tr>
<tr>
<td>15</td>
<td>participate in some uses of the collected</td>
<td>15</td>
<td>information, with companies like ours if they are</td>
</tr>
<tr>
<td>16</td>
<td>information.</td>
<td>16</td>
<td>provided with notice and choice.</td>
</tr>
<tr>
<td>17</td>
<td>Our companies understand consumer concerns. As Lynn and David will</td>
<td>17</td>
<td>As a first step toward meeting</td>
</tr>
<tr>
<td>18</td>
<td>explain, our companies are fully committed to the principles of</td>
<td>18</td>
<td>consumer expectations, NAI companies will be</td>
</tr>
<tr>
<td>19</td>
<td>notice and choice for consumers.</td>
<td>19</td>
<td>establishing an informational web site located at</td>
</tr>
<tr>
<td>20</td>
<td>Today we are announcing the key tenets of the Network Advertising</td>
<td>20</td>
<td><a href="http://www.networkadvertising.work">www.networkadvertising.work</a>, as pictured on the screen behind me.</td>
</tr>
<tr>
<td>21</td>
<td>Initiative: First, each NAI company will continue to provide</td>
<td>21</td>
<td>This web site has been developed to provide consumer awareness about</td>
</tr>
<tr>
<td>22</td>
<td>consumers with a clear explanation of the</td>
<td>22</td>
<td>our industry and provide an easily accessible and</td>
</tr>
<tr>
<td>23</td>
<td>information it collects, how that information is</td>
<td>23</td>
<td>convenient place for consumers to exercise choice</td>
</tr>
<tr>
<td>24</td>
<td>used, and the benefit to consumers of such use.</td>
<td>24</td>
<td>regarding the use of their data.</td>
</tr>
<tr>
<td>25</td>
<td>Second, for consumers who choose not to receive tailored messages,</td>
<td>25</td>
<td>Our companies also adhere to the fair information practices developed</td>
</tr>
<tr>
<td>26</td>
<td>either currently provides or will soon provide an easy to use method to</td>
<td>26</td>
<td>by the Online Privacy Alliance and other organizations</td>
</tr>
<tr>
<td>27</td>
<td>opt out from such tailoring.</td>
<td>27</td>
<td>interested in privacy. To that end, all the Internet advertising sites</td>
</tr>
<tr>
<td>28</td>
<td>Third, our companies are committed to consumer outreach and education</td>
<td>28</td>
<td>owned or controlled by one of our companies will disclose their data</td>
</tr>
<tr>
<td>29</td>
<td>to let consumers know about our companies and the role we play in</td>
<td>29</td>
<td>collection and use practices on their web sites in a clear, concise, and</td>
</tr>
<tr>
<td>30</td>
<td>delivery of tailored messages over the Internet.</td>
<td>30</td>
<td>conspicuous manner and in language that consumers can understand.</td>
</tr>
<tr>
<td>31</td>
<td>In other words, we have heard consumers' concerns and we are</td>
<td>31</td>
<td>These disclosures will include the following: what data are collected and</td>
</tr>
<tr>
<td>32</td>
<td>committing to addressing them.</td>
<td>32</td>
<td>what data are not collected; how the data are used, including whether</td>
</tr>
<tr>
<td>33</td>
<td>Now I'll turn the microphone over to Lynn Chitow Oakes from Flycast,</td>
<td>33</td>
<td>they will be combined with personally identifiable data from any other</td>
</tr>
<tr>
<td>34</td>
<td>who will explain more about our commitment to notice and choice.</td>
<td>34</td>
<td>source; what other data are collected and how they are used, including</td>
</tr>
<tr>
<td>35</td>
<td>MS. OAKES: Thanks, Elizabeth.</td>
<td>35</td>
<td>the use of data for ad management; and lastly, what opt-out procedure</td>
</tr>
<tr>
<td>36</td>
<td>NAI companies are committed to providing consumers with notice and</td>
<td>36</td>
<td>are available for consumers who decline to have data used to create a</td>
</tr>
<tr>
<td>37</td>
<td>choice about Internet advertising. We believe that adherence</td>
<td>37</td>
<td>profile.</td>
</tr>
<tr>
<td>38</td>
<td>to fair information practices and data management</td>
<td>38</td>
<td>In addition, our companies will at a minimum request that their</td>
</tr>
<tr>
<td>39</td>
<td>that we are going to describe today are in accordance with the</td>
<td>39</td>
<td>customers, whether they are publishers, e-commerce sites, or networks,</td>
</tr>
<tr>
<td>40</td>
<td>consumer expectations and desires as outlined in Dr. Westin's</td>
<td>40</td>
<td>disclose their own data collection and use practices, including posting</td>
</tr>
<tr>
<td>41</td>
<td>survey and in our own business experiences.</td>
<td>41</td>
<td>a link to either the NAI companies' web sites or the NAI gateway</td>
</tr>
</tbody>
</table>
1 educational web site. We will also ask them to
2 post a privacy policy that is consistent with
3 fair information practices.
4 I'd like now to turn this over to
5 David Zinman at AdKnowledge, who will talk to you
6 about data collection and use.
7 MR. ZINMAN: Thanks, Lynn. It's
definitely a pleasure to be here. I appreciate
9 the time.
10 First actually, I'm going to address
11 the commitments our companies are making with
12 personally identifiable information that's
13 collected. I want to be clear that not all of
14 our companies currently collect personally
15 identifiable information. However, all of us
16 have agreed to abide by these principles.
17 Second, I'm going to discuss the
18 commitments NAI companies are making regarding
19 the collection and use of ad management and
20 reporting data which is non-personally
21 identifiable. This is important because the
22 ability to collect information about consumers in
23 a non-personally identifiable way is unique to
24 the Internet.
25 Here's the commitment NAI companies

1 are making for personally identifiable data:
2 First, our companies that collect this data will
3 notify consumers about the collection and use of
4 their data. At a minimum, we will let consumers
5 opt out of unrelated or secondary uses at the
6 time this data is collected.
7 Second, if that data is linked to
8 other personally identifiable information, our
9 companies will give consumers the opportunity to
10 opt out.
11 Third, in accordance with fair
12 information practices, NAI companies that collect
13 personally identifiable information will make
14 reasonable efforts to provide timely and
15 appropriate access to that information under
16 policies that each of us will post on our web
17 sites.
18 As has been discussed, our companies
19 are able to collect information from browsers
20 that's not personally identifiable. We call this
21 data ad management and reporting data. It can
22 include type of browser, type of operating
23 system, IP address, date and time of visit, and
24 ad viewed. This kind of data is used by our
25 companies to transmit, to sequence, and to report

1 on ads shown to customers.
2 Let me emphasize again, this data is
3 associated with a browser which is not personally
4 identifiable. The commitment our companies are
5 making today is to provide consumers with the
6 ability to opt out of the use of this data for
7 profiling and thus opt out of the services
8 associated with profiling.
9 However, consumers will not be able
10 to opt out of the transmission of this data for
11 basic ad management and statistical reporting
12 purposes. These data are necessary to deliver
13 the ads and provide advertisers with information
14 about how many users saw the campaign. So for
15 example, today it would be almost impossible to
16 sell advertising space without being able to tell
17 the advertiser how many users will see their ads.
18 Our companies will post notice to
19 consumers about our data collection and use
20 practices on our web sites. We will also give
21 consumers an opportunity to opt out of the use of
22 this data for profiling purposes. Consumers can
23 opt out by going to a designated location on each
24 of our companies' web sites or through a gateway
25 educational site we described earlier, and it's

56 (Pages 218 to 221)
companies, what we do, how we do it, and how consumers can exercise choice. We will pursue activities to promote consumer confidence and trust.

We believe the measures we are implementing are the foundation of a self-regulatory framework for our industry that will protect privacy while allowing the effective advertising that makes the web free. We look forward to working with our colleagues across the industry to fulfill the commitments we have made today.

Thank you.

MS. BURR: Thank you very much. I'd like to turn to the rest of the panel to solicit questions about what we have just heard. And let me remind the audience that we do have question forms and that people will be going, picking them up and delivering them up to us.

Andrew.

MR. SHEN: I think it's fair to say everyone in this auditorium believes that consumers should have the right to control their information. However, I think there is really a distinction to be seen between what the companies are providing in terms of control and what consumers want.

Fair information practices have four different --

VOICE: A little louder, please. Speak into the mike.

MR. SHEN: Sorry. Is this loud enough?

MS. BURR: It's working. Just bring it closer.

MR. SHEN: Fair information practices consist of four different elements: notice, which is providing information to the consumer about how the information is being collected and how it's going to be used; consent, which means that the person gives affirmative permission for the companies to use that information; access, so the consumer has access to the information that's being collected on them, what is contained in the profile; and security, so that information is not distributed to other third parties.

The self-regulatory proposal done by the NAI does not meet all those requirements. Online advertising is something that happens without the knowledge of most consumers, so the opt-out option is not really a good way to approach the problem because most consumers don't know that this is occurring at all.

MR. JAYE: We believe that it's very important for us to address those consumer confidence issues. That's one of the reasons why we have stepped forward and said that we would like to provide choice to consumers even for non-personally identifiable information. Fair information practices literally to this date have generally been interpreted to apply to personal data, personally identifiable information.

We have taken a step forward and understood the sensitivity of the information and said that we are committed to providing an opt-out for the innocuous information that we use for non-personally identifiable profiling.

MR. MEDINE: I think it might be helpful to clarify what your intentions are with regard to the opt-out for non-personally identifiable information. I don't think it's immediately clear how it could be used for some forms of ad management but not for profiling. Could you maybe explain in a little more detail exactly what information is going to be captured through the use of the cookies and how it will or won't be used?

MR. JAYE: Certainly. One example that we talk about in terms of profiling is the use of a cookie to manage an identifier that then could be used to build a profile for that web site visitor. That type of information, we can provide an opt-out and some companies around the table have already done that by allowing that cookie to be set to an arbitrary value like opt-out that would be a signal to a web site to remember that this browser is one of a number of browsers that are not to be tracked.

However, it is also possible to have other cookies on the computer that are being used for application management or other purposes. The most prototypical example would be for counting unique visitors, being able to correlate an ad click with the ad that was displayed, being able to try to avoid duplication of ad displays. In other words, avoiding repetition of the same ad over and over again.

These uses are not targeting per se, but they are important to the operation of the ad
industry. And once again, this is an industry that is extremely important to nascent and entrepreneurial web sites, as well as many medium and fact very large web sites that don't have the infrastructure or manpower to staff these services internally.

MR. ZINMAN: I just want to follow up and say that one of the reasons that we're taking this significant step is because fundamentally we have a different relationship with the consumer than a web site, where a person sees it. Most consumers don't know we exist, so we need to go the extra mile to allow the consumer to have complete choice, even if it's only of information that isn't personally identifiable.

So related to your question, your question related to personally identifiable information, which there's no question that you have to be -- every company needs to adhere to fair information practices, but on information that's not even personally identifiable we're willing to go the step to give the consumers the choice as to whether we retain that information.

MR. MEDINE: So I understand, the limits are that you would know which ad I have seen so it's not delivered to me again, but you wouldn't know anything about me in order to decide which ad I should receive if I have opted out?

MS. OAKES: Absolutely.

MR. JAYE: That is what is provided in our initial step of the principles.

MR. MEDINE: Another question in assessing any self-regulatory system, one issue is how broad is it, how much of the industry does it cover? I know you're all fierce competitors, but I suspect not all the competitors are in the room today. Give me a sense of what percentage of the industry the people who are part of the NAI constitute?

MS. OAKES: The majority of folks that are in the third party ad surveying are at the table. There are ten companies involved that represent, an estimate that we put together today, actually about 85 percent of ads served on the Internet today.

MR. ZINMAN: It is very difficult to determine that, but if you look at just the companies that are involved with doing just the infrastructure work of delivering advertising, the vast majority of those ads that are served are served by companies that are part of this group. And I'd suspect that if there are a few remaining companies that contribute significantly to this, that they're going to be interested in joining this as well.

MR. HILL: First of all, I want to commend the Network Advertising Initiative. I certainly think that any attempt to make the process more transparent to users and get users involved should be commended. I don't think that there is one solution that fits all. Technology can't solve the problem in and of itself. I don't think regulation can solve the problem in and of itself. At the same time, industry efforts like this I think do a lot of good.

I have a couple of specific questions. I'm just going to lay them out, let you guys individually take it. You talked about how fair information practices, the difference between this and traditional fair information practices that Andrew touched on, is because it is not personally identifiable information, where there is opt-out versus opt-in.

The question I would have is, for the cases where members of your group do adopt personally identifiable information, would the group be requiring them to adopt an opt-in for that purpose that go the extra step? The next question I would have is, being that I think this group represents the good players in the industry, the players who are trying to make an initiative to protect consumers, how would this group feel about some sort of legal framework for redress and accountability for bad players, so that in situations where people aren't adhering there is a legal framework to hold that person accountable?

MS. WANG: Actually, in addressing your question, Austin, I want to characterize something, the way you characterized fair information practices. The principles are notice, choice, security, and access. Choice is not opt-in. Choice is really, it can include opt-out, and in the United States it's always been opt-out, hardly every opt-in, except in very sensitive situations like medical, financial, kids.

So that's actually -- so in fact
there's a very key thing in our principles today and that is we are following the fair information practices principles. We're not expanding them. We're not extending them. We're not saying that opt-in is the right answer for personally identifiable information. In fact, we believe opt-out with clear notice and an effective opt-out cookie and an easy method to opt out actually more than satisfies that requirement of the fair information practices.

There is something that our companies, the fact that we deliver ads and we're not apparent to some consumers, although I think we are quite apparent because certainly people, consumers, know who we are even though they're not in advertising or they're not web publishers. I think we're more apparent than most people give us credit for, and sometimes many of them are our investors as well.

But getting back to your point, the reason why in our situation the opt-out included some information that was acquired for ad targeting really went to the fact that it's a relationship issue. We don't have a direct relationship with the consumer. So it's an easier issue for web sites, web publishers, that deliver their own advertising on behalf of advertisers, because the consumer knows whom they're dealing with.

In our situation, we went the extra mile, as Dave put it, and allowed for the opt-out of non-personally identifiable information collected in the routine course of delivering an ad or even delivering content to a consumer because of the situation that we find ourselves in, that we are business to business companies and not direct to consumer companies. So I just wanted to clarify that one point, that we are in fact not saying that -- we're not at all consistent with other self-regulatory regimes, it is this third party auditing that will provide for the accountability.

MR. HILL: Just to follow up on that question, so in a situation like we have seen this week with RealAudio, where they had a TRUSTe privacy seal, there were activities, and TRUSTe hasn't come down with their result, but that some people would feel weren't disclosed or honest, so the enforcement level that you're talking about would be the withdrawal of some sort of seal?

MS. WANG: Well, I don't know any of the details of that RealJukebox situation other than what I read in the paper. But wouldn't you agree that it was very effective, the self-regulatory mechanism there? The market came down very hard and RealNetwork did the right thing right away. I think to me that's just evidence that it works extremely well, and that's just one of many instances.

MR. HILL: I'm not commenting on the benefits, the strengths and the weaknesses. I'm just asking for this organization if that's the desired enforcement mechanism, is the withdrawal of outside audit seals if someone is a bad player? So a bad player in the network would find themselves without an audit seal? There would be no accountability or redress?

MR. HILL: But could a consumer go and hold that company accountable, sue them? Do you guys advocate some sort of framework? If someone says, I don't want to be in NAI, I don't care, I'm going to profile, should there be a framework?

MR. ZINMAN: I think there's another method of control that we need to get out here, which came out in the second panel, and I'm not going to articulate it as well as Dan Jaffe, but I'm going to try, which is that the advertisers do not want to be associated with companies that abuse the trust of consumers, and all the companies in our industry, our lifeblood is the respect and responsibility that we hold with our consumers, the advertisers.

So every company that represents any significant advertising dollars is going to feel a lot of pressure to make sure that they are responsible to consumers. So I think companies are going to naturally be pushed into a self-regulatory environment with or without
MR. MEDINE: I just want to add, of course, the Federal Trade Commission's deception authority to bring cases against companies that don't honor their privacy promises, both to consumers and business partners. I also thought it might be useful at this point just to hear from Paula Bruening from TRUSTe.

MS. BRUENING: Thank you. I'd like to make two points, one that would speak directly to the RealNetwork issue and one that probably speaks more to the general issue of relationship that everyone's been talking about. First of all, without going into tremendous detail, RealNetworks is a TRUSTe licensee and I think the people in this room and definitely on this panel are aware of issues that were raised earlier last week about the collection and transmission of user data via the RealJukebox consumer software. As it turned out, after we made an initial inquiry it turned out that, as our license agreement and program is set up right, we were not able to act on that because our program governs information that is collected through a web site and that was not the kind of information that was being transmitted. It was not at issue in the RealNetworks instance. However, we have taken this as an opportunity to look very closely at the issue of information that's collected in this manner, and this is our opportunity to expand the program to include that kind of data collection and transmission.

We do believe that RealNetworks has done the right thing. They have taken a lot of steps on their own with TRUSTe to address the issue, and we have worked closely with them over the last week. We're going to be looking at some very specific things that we can work on with RealNetworks to assure that our relationship with them is good and we can continue to be sure that they're doing the right thing and that our program is acting optimally.

I think for the future what we will be looking at is a program that deals with this kind of consumer software transmitted data, and that's going to be our project in the coming months. So I just want to get some clarity on that as we're going forward. The other point that I wanted to make is that I think speaks to what everyone's been talking about, relationships with consumers and how that pertains to seal programs in general. I think one of the things that we work on on a daily basis and requires some of the hardest thinking that goes on at TRUSTe is looking at these relationships that are increasingly growing between companies on the Net and are becoming increasingly complex.

I think that our job is to as much as possible clarify what those relationships are and what their implications are for consumers as it pertains to collection and sharing of information. We know that companies want to have as much as possible seamless and hassle-free experiences for their consumers on the web, but at the same time we have to assure that there is consistent notice that is going on as a consumer is traveling through their web experience. And we know that they may be going to different URL's that may be governed by different privacy policies.

So what we're challenged with is making sure that the consumer is clear as their taking these travels on the web as to when they're in safe space, when they're not, and when their privacy policy has changed. So to the extent that that mirrors what we're seeing in online profiling and to the extent that Dr. Westin's findings are an indication of what the consumer is looking for is notice and choice, I think it's our challenge as we move forward -- and maybe this is the topic for the next workshop -- to figure out what is effective notice.

It's good to have principles. It's very important to have principles and it's a wonderful first step, but how do you go about implementing those in a very complex kind of environment where real estate is very valuable, a seamless experience is very valuable? So we have to really decide, whose responsibility is this? Is it the advertiser's? Is it the online business? Is it both? What's adequate and effective notice and how do you provide for opt-in and opt-out as you're making your way on the web?

MS. BURR: We're going to go to John Kamp, then Evan Hendricks.

MR. KAMP: I don't have anything to say.
MS. BURR: Thank you.
Evan Hendricks.
MR. HENDRICKS: Thank you, John.
As a matter of clarification, is it
my understanding we're only here to ask
questions?
MS. BURR: I wanted to see if there
were any questions about how the program worked.
MR. HENDRICKS: Yes, I have one,
because somebody sitting in this seat at a
Department of Commerce meeting on ratings, when
he was giving ratings one to ten, how good is the
privacy policy, I'd say this one might be up
to about a 2.5.
One of the issues of fair information
practices that everyone agrees on is access to
your own information, and I don't see that listed
here. So I wanted you to address the access to
information.
Second of all -- and I have a series
of questions, so you might want to jot them down
and I'll get them all out of the way so we can
move on. Second of all, DoubleClick right now,
clearly you're in the business of collecting
personally identifiable information. If you're
not, it certainly appears that you are,
considering that you've acquired Abacus.
So the question in all of our minds -- let
me finish the question.
It looks like you're in the business
of acquiring personally identifiable information.
So I wonder, what is your projection? How many
files on how many individuals do you expect to
gather information? The credit reporting
agencies are willing to disclose they have
records on 180 million Americans. So considering
that your opinion poll that you paid for shows
that you got a response that 52 percent of the
people support using personally identifiable
information for online and offline behavior the
tailor ads, so what are your projections on how
many individuals you expect to collect
information on?
MS. WANG: You want to answer the
first question?
MR. HENDRICKS: The last question is
on access to information.
MR. JAYE: I would prefer to address
the specific question about NAI principles and
then I'll hand the mike over.
In terms of access, right now we have
left it, because there are lots of different
business models and not all the companies in NAI
gather personally identifiable information. We
have not explicitly addressed access at the NAI
level. It's something that we're looking at.
With regard to non-personally
identifiable information, once again, it is not
strictly true that access needs to be provided to
non-personally identifiable information. That
being said, let me comment on why many of the
companies do not provide access to non-personally
identifiable information-based profiles. The
problem is authentication, because we don't know
who the consumer is. We have no way of
authenticating that a person who's asking for
access to a non-personally identifiable profile
is in fact the person associated with that
profile.
Because we've made a commitment to in
many cases keep that information secure and not
to share it with other people, because we can't
authenticate the consumer, we can't display that
information. We are very interested, however, in
looking at new technologies and new techniques to
solve this problem, because we would like to
provide it if we can find a way to solve the
Catch 22 between not knowing who the consumer is
and being able to prove that they are who they
say they are.
MR. MEDINE: Why not just use the
consumer's own cookie to give them access to
their information?
MR. JAYE: The concern is that, once
again, cookies are not a strong identification
technique. We don't provide typically the
profiles out to any third party who has a cookie.
So the issue is, if we allow somebody just to
enter a cookie and say, show me this profile,
there are situations, for example in an office
environment, where a co-worker might have easy
access to the cookie file of another co-worker.
So once again, it's an area that we
keep thinking about. We would like to provide it
if we can solve the security issues.
MS. WANG: To your second question,
which has to do with DoubleClick's impending
merger of Abacus -- and it's impending because it
hasn't happened yet -- we don't own the Abacus
database. And it's something that seems to be -- we
don't own the company, we don't have any new products.

But I will answer your question in good faith, which is you want to know, you want to know how many profiles we think we'll get after the merger and whether or not we currently collect personally identifiable information. The answer is we do collect personally identifiable information through our Netdeals site, where we sponsor a million dollar sweepstakes.

Do we link that information to anything? No. Will we link it after we acquire Abacus? The answer is yes, and that's clearly in the consent and notice, very easy to understand. So I don't really think that there's anything -- there's no question or no confusion there.

As to your question of how many people, how many profiles, do we think we'll get that are linked, well, it's always subject to clear notice. It's always subject to their not having opted out after they received the notice. I don't know what the projections are. I don't think we can project right now. But I sure hope it's a lot because, as Dr. Westin's survey and as you pointed out, we did sponsor their survey and as you pointed out, we wouldn't have to do that. I think it's the role of the FTC or the Commerce Department.

MS. WANG: So when is your survey going to come out?

MR. HENDRICKS: How many files does Abacus have? I mean, you're going to merge this company. Can you give me a ballpark figure on how many people they have files on?

VOICE: 99 million.

MR. HENDRICKS: How much?

VOICE: 99 million.

MR. KAMP: Thank you. I wanted to respond first to a bit of Austin's question about, what about the law in this area, and I wanted to really sort of clear the decks and come back to this discussion. This whole section is labeled "The Role of Self-Regulation" because it reminded me of 1992, when the Commerce Department first was working with the White House on the National Information Infrastructure Advisory Committee to the President. There was a thought in this building...

... and elsewhere that advertising would have no place in this medium at all. It just wouldn't be useful there. There were several of us who came to this building and made the argument that we had difficulty. They were nice to us, but they were very skeptical that advertising does have a place and in fact advertising may very well be the way in which this medium would be available to all people. Their concern about communication have's and have-not's and ensuring that all people in our society had this medium available to them, advertising was one of the responses to that. It was long after that that there was a group called CAIE created, Coalition for Advertising and Information and Entertainment, where we came and developed a set of self-regulatory guidelines and policies which, interestingly enough, have all of the elements that Andrew suggested there, and we continue to stand by them. With that, we applaud the ad-serving group coming forward this morning, this afternoon, and working on this and coming forward...
and saying we understand what we're up to, we plan and we intend to do right. And I suggest that we not worry about creating laws in this area until we have allowed this self-regulation to play itself out.

I being a former regulator at the Federal Communications Commission, can tell you that when in 1997 the Federal Trade Commission did its first sweep on privacy policy on sites none of us were particularly surprised to find that under 15 percent of the sites that they visited had privacy policies.

But I think more of us were even sort of taken back by how one year later, when there had been in place, fully in place for some time, that nearly 80 percent of the sites had privacy policies on them of some type. As a former regulator, I must say that that is something that could not have been achieved by the government. Government regulation mandates could not have sped, gotten the industry there any faster than that. In fact, I don't think it would have gone that fast.

So those who are very interested in developing laws should recognize that the Federal Trade Commission has taken the right stance in the past by encouraging us to continue to do the kinds of things that the people coming forward with this program have today.

MR. MEDINE: Andrew is next. I want to just make it clear to the panel that we're now open to the broad topic of self-regulation. People are free to direct questions, but they can also discuss unrelated issues to the NAI proposal. Andrew.

MR. SHEN: I'll go ahead and apologize. I'm going to ask another question about the self-regulatory proposal. VOICE: Move the mike closer.

MR. SHEN: I'm sorry. Can everyone hear me?

VOICE: No.

MR. SHEN: No?

MS. BURR: Just talk louder.

MR. SHEN: Anyway, a couple people, David and Elizabeth, have said you guys have gone the extra mile to include some partial implementation of fair information practices, even though this information is not necessarily personally identifiable. But you can't really deny that this information has a very high potential to be potentially identifiable.

People have debated back and forth over the course of the day that it may be difficult, maybe, to find the person that this information correlates to, but it can be done.

MR. JAYE: It can be done?

MR. SHEN: Right.

MR. JAYE: If you assume a set of circumstances, at which point we would no longer consider it non-personally identifiable information. In other words, talking about what might happen and what might not happen, there are lots of different possibilities. However, with regard to the information we gather, when we say we gather information and use it in a non-personally identifiable way, that is accurate, that is how we are going to use it.

Now, if our privacy policies change, if we should start to have different practices, there are different ways of interpreting that. But at Engage, at least, the way we would interpret it is the information we gathered under past privacy practices we would need to go out and get proactive consent from a consumer before we started to treat data that we gathered under an assumption that it was non-personally identifiable as personally identifiable.

So I take issue with a position that says that there is no such thing as non-personally identifiable, because I think that it holds out the possibility that consumers will not be able to get the advantages out of the Internet, the free services that are advertiser-supported, if we draw a broad brush and say, now anything could be personally identifiable in some circumstances, so let's not create that category for non-personally identifiable information at all.

MR. HILL: Just a clarification, Daniel. So are you saying that, does the NAI as a group have a policy on fundamental change of notice? So if you collect data under one practice and then change at a later date, you had mentioned that Engage believes you require consent and an opt-in for that change of practice. Otherwise you have to stay under the previously advertised policy.

Does the NAI as a group have a policy...
on how they approach change of practices, so if
they have a merger or an acquisition and it's now
in someone's business interest to make it
identifiable how would your group suggest dealing
with that?
MR. JAYE: Well, as David Medine
pointed out, when we make a public policy
statement his organization certainly has
enforcement capabilities if we violate that
privacy principle. Now, with regard to changes --
MR. HILL: Yes, I'm talking about
revision.
MR. JAYE: Yes. In terms of revision
with regard to prior data collection, that's an
area that we have not explicitly called out at
this time. What I will say is that this is a
process we have gone through over the last, I'd
say, about eight or nine months since the initial
meetings with the government.
There are a number of areas that we
will in the coming months as we look to expand
the group to include other industry members, we
will need to tackle certain issues and we welcome
input about particular issues that people think
might make a better self-regulatory framework.

MR. HILL: Thank you.
MS. WANG: I just want to -- you were
talking, you say that if notice has been given or
choice has been offered and the consumer had done
one thing and provided the information, if later
on the practice had changed, the answer is -- and
it's not an answer that's particular to NAI, it's
really an answer particular to fair information
collection practices generally -- you need to
look at the original notice and see whether or
not the new use was contemplated in the original
notice, because you had asked the consumer for
permission to do a certain thing and if you
change that thing or you add to it, then,
depending on what that thing is, it could be that
you need to go back and provide additional
notice.
MR. HILL: Just to follow up on that,
do most of your guys' privacy policies have the
right to change the policy practices without
consent or permission currently?
MS. WANG: I don't understand the
question.
MR. HILL: Well, a lot of privacy
policies I've seen include -- and I assume it's

legal speak that gets put in there by a lot of
lawyers, but it's: we reserve the right to
change this policy at any time without consent or
permission from the user. By agreeing to this
policy, you're agreeing to all future privacy
policies that this company may issue.
That's generally a clause that's in
most privacy policies. So I'm asking, is that
currently this group's practice, to include it?
MS. WANG: I think those members of
our group that are members of TRUSTe and other
organizations probably have restrictions on what
they can say along those lines. Again, I go back
to my initial answer, which is that everybody has
to comply with general fair information
collection practices in how they would view that,
and that's really the answer. I think I can't
without specifics --
MR. MEDINE: Tim has been waiting
patiently over here.
MS. BURR: And Steve seems to have
been pulling the microphone closer.
MR. LORDAN: On behalf of the Online
Privacy Alliance, I want to applaud the
advertising industry for this self-regulatory
1 party relationship involved and access to our privacy policies as individual companies and as a group.

MS. BURR: We're going to do Steve, Jerry, Evan, then Fred. David told me that was the right order.

MR. LUCAS: Thank you.

I think that no one on this panel would deny that today the practice of profiling has occurred without any real notice, any of the major factors -- notice, choice, access, or consent, or the knowledge of consumers for the most part. And I think that we too applaud the work of this organization.

But I have some concerns over the whole notion of not requiring an opt-in. To me an opt-out, if you start with an opt-out and information is collected and then later on a person decides they don't want that information used any more, especially when your privacy policy says that we share information with third parties, at that point I would argue that an opt-out, while it doesn't allow the company to use that data any further, you still have a proliferation of data.

MR. JAYE: Steve, could you just clarify. Are you talking about PII information?

MR. LUCAS: Yes.

MR. JAYE: Okay, but not non-personally identifiable information?

MR. LUCAS: Right. We can get into that in a second. But I think that not having the consumer opt in first -- I don't see why, if we're going to take a positive step, that we don't take the whole step and say, let's go to an affirmative opt-in at that point as opposed to an opt-out. If you take a look at what's happening in Europe, that's required as opposed to -- an affirmative action as opposed to an opt-out.

The other thing is, we do, we support a self-regulatory model. We believe that a self-regulatory model has the potential to be the way to go. We think that if the industry doesn't step up there may be a need for some legislative mandates to establish a framework which we can all work on.

Having said that, we also have decided that it's important both to provide consumer education as well as the opportunity for consumers to be able to go to a site and opt out of targeted advertising as well as profiling.

Today we actually announced the launch of a site called Myprivacy.org. The purpose of that site is again to provide consumer education, but also to provide an opportunity for consumers to specifically request not to be targeted, both through the use of personally identifiable information as well as to be tracked through the use of cookies.

Having said that, we think that all these efforts -- we applaud any effort that brings the industry closer to a fully permissioned model, because we hear all the time that the goal of the industry -- in fact, someone on the panel said it -- the goal is to send the right ad to the right person at the right time with the right offer. I think it's time that the term "right" is the right of the consumer to determine when, where, and how any information that's being used, being collected and used -- they have the ability to control that.

Having said that, I do have a couple of questions. That is, we're seeing a lot more companies out there on the web either acquiring companies that have an offline presence or we know that there are practices out there that sites collect data -- use data that's been collected offline. Does your organization plan on any disclosure that would require, outside of COPPA, which I believe does require some disclosure when data is being used from offline data sources -- do you plan on disclosing the fact that you're using data that's been collected from offline sources and that data has been added to that profile?

Without providing the consumer access, the consumer has no way of knowing that you've created a profile with data that has not been permissioned.

MS. WANG: I guess that's my question. Your first question, which had to do with consumer choice, and this would be DoubleClick specifically.

MS. BURR: Elizabeth, can you pull the mike up.

MS. WANG: Oh, yes. Thanks, Becky.

The NAI principle provides for consumers to have choice at the time of data collection, personally identifiable data.
collection, and the opportunity to opt out, and
you're asking why we would not offer to opt in.
Actually, I want to clarify our opt-out, because
if at some point a consumer gave me an address in
connection with the sweepstakes with the full
notice that, oh, we're going to connect offline
data to you -- and by the way, in answer to your
second question, the answer is yes, DoubleClick
would do that, would specify at the point of data
collection that that information would be
connected, linked with offline data, more data
from other sources. So that's the answer to your
second question.

But in answer to your first question,
if later, if I'm the consumer and I signed up, I
did not opt out at that point, and then two weeks
later it occurs to me, hey, I really didn't want
that to happen, you can always come to the
DoubleClick site or go back to the site where you
originally opted, where you originally provided
the information, the sweepstakes site, and get
linked to the DoubleClick site and opt out then,
and that opt-out would be effective for as long
as you have that browser or until you delete your
cookie file.

MR. MEDINE: Can I just ask a
clarifying question on that. It wasn't clear at
the beginning that the opt-out that applies to
personally identifiable information is as broad
as the opt-out for non-personally identifiable
information, because as I understand it for non-
personally identifiable information it's for use,
whereas, just to clarify, for personally
identifiable information, I thought you could
only have a choice over third party transfers but
not any control over internal use by your
companies.
Could you describe if that's the
correct interpretation?

MR. JAYE: No, that's not correct.
The opt-out on PII data, personally identifiable
information, is over all use. On non-personally
identifiable information there are two
categories. There's a category that's
effectively the infrastructure of the web. The
infrastructure of the web requires us to be able
to, for example, be able to report on reach,
frequency numbers, etcetera. So we cannot
provide an opt-out to that.

In that category or the second sub-
category of non-personally identifiable
information is the ad delivery data, and that's
the data that's used for profiling and targeting,
and that we're providing an opt-out for across
the network.

MR. MEDINE: So, using Elizabeth's
example, if I changed my mind and I want to go
back, I can opt out of any future use whatsoever
of personally identifiable information?

MS. WANG: That's correct, yes.

MS. BURR: Jerry.

MR. CERASALE: Thank you.

I wanted to commend NAI for their
efforts here. And Lynn, I really was pleased
with your statement and I want to make sure I
understand it, because I think it agrees with
where the DMA is: that the best place for notice
is right away and it's really at the initial web
site where you go. I guess it's, using a term
that's been used here, the publisher.
And do I take it that you're going to
make efforts, you the NAI are going to make
efforts, to ensure that your -- the web sites
with whom you work are going to have in their
privacy policies a statement that would say: I
have an agreement with XYZ company that can
collect information and have a hot link to your
privacy policy, so that the consumer would then
know what the web site's policy is and then what
your policy is, so you can then establish the
relationship there with the consumer to do the
opt-out?

MS. OAKES: Couldn't have said it
better myself, absolutely correct, and we look
forward to working with your organization to make
that happen.

MR. CERASALE: And then a comment on
Austin's question. It's my view if you get a
change, at least it's the view I think of the DMA
-- and I'll get a pink slip tomorrow if that's
not true -- the view of the DMA is if you change
your privacy policy, information that you
collected under the old privacy policy, and then
try and use that old information in your new
privacy policy, which has a very material
difference, I think that subjects you, that
company, to FTC review, because you collected
information under one pretense and then start to
use it under another pretense, and you have to
somehow give notice back to change that.
So I think that there is already a law that is out there that covers that right now.

MR. HILL: Most of the practices in this area right now under the original collection of that data, it usually comes with the right to change and revise the policy later. I'm not sure if the FTC would consider that in their mandate if the original data collected had the clause attached to it that as part of giving us this data we have the right to revise our policy. That was my question. If the FTC does have oversight that would be very useful to know.

MS. BRUENING: TRUSTe's name came up in the context of this discussion and I just wanted to say that our license agreement provides that if you do change your privacy policy you must inform consumers that you're doing it and then give them the opportunity to opt out. We're also moving toward setting up a situation that was precisely as was just mentioned here, where if you have collected information under a certain pretense of a certain policy you have to continue to treat that information in that manner even if you've ended your relationship with TRUSTe.

MR. MEDINE: I'm not sure this is the forum for us to give FTC advice, but clearly there are deception implications if there are misrepresentations about use, and obviously we'd have to examine on a case by case basis changes in use and what representations were made initially and then what steps were made to obtain consumers' consent for subsequent use.

MR. CERASALE: I just want to respond to what Austin said. My view on that, and I'm not going to put words in David's mouth here or any of the Commissioners' mouths, is that I can change price any time I want to change price, but once you sign up, you click on the web that you've purchased something for 10 dollars, and before I fulfill I change the price to 12, I can't charge you 12 dollars. That's deception. So I think that it doesn't -- the fact that I have the ability to change doesn't change the matter of a material fact, that you got information from. That would be my view. That's my view on that.

MS. BURR: We're in radical agreement on this: Evan and then Fred.

MR. HENDRICKS: Further, I agree with Jerry's analysis of the law in that situation. The one thing that's missing from the law is the right of the individual to enforce his own rights or have control over his own data, and that can only be -- that's one of the main reasons legislation is necessary, because a major part of fair information principles is a remedy when something goes wrong. Protecting privacy is at its zenith when something goes wrong.

Now, in Europe where they are protected by law, they actually marvel at the progress we've made in this country at getting notices on web sites and at the self-regulatory progress. So you can definitely put yourselves on the back because they look in admiration at us.

So privacy will only be protected when you have it covered by law and by self-regulation, if you define self-regulation by implementation. That's why I really congratulate the FTC on this workshop, because I think it shows the true determination to find a way to protect privacy, because this scenario that we have so far with this self-regulatory program will never work. It is too far removed from people. It puts too much of a burden. It doesn't include enough fair information principles.

If the FTC wasn't interested in protecting privacy, they wouldn't focus on this sector, which contradicts its policy that there should only be self-regulation for the Internet. So I congratulate the FTC for asking the hard questions.

This has been a familiar pattern. We've had FTC workshops. Different industries have come up with self-regulatory programs. Sometimes it's been like pulling a rabbit out of the hat. I don't know if anyone remembers the early years when Firefly was described as a way of protecting privacy and a reason self-regulation would work. Well, that's one program or one example of something that's vanished once we've moved on.

I think a real problem here is the threat to e-commerce and the shaky confidence that's being engendered here. You know, DoubleClick, you mentioned that you thought the RealAudio situation worked really good because...
1 there was a public outcry and TRUSTe kicked in
2 and said they were going to look at it. But the
3 problem is information on millions of people was
4 transferred in violation of a policy without
5 people's knowledge and consent, and virtually
6 nothing's going to be done about it. That is not
7 any way to guarantee confidence in the Internet.
8 If you look at the Jupiter study and
9 the Forrester study saying that we are lowering
10 our projections for how much e-commerce will
11 generate if privacy is not taken care of, I think
12 those are very real things to look at and I am
13 very concerned that the existence of -- the way
14 you're operating, if you're going to collect
15 personally identifiable information and use it in
16 the kind of schematic that you've described,
17 you're going to just do nothing more except
18 produce distrust about the Internet.
19 The final thing is the enforcement
20 program here is flawed because you're hanging
21 your hat on the Alan Westin survey, which I think
22 we can talk an hour about why that should be
23 challenged, but also on the issue of TRUSTe.
24 TRUSTe, when the first Microsoft example came up,
25 TRUSTe said they couldn't do anything about the

1 information being transferred because it wasn't
2 transferred from the web site. Well, consumers
3 don't care if the information's not transferred
4 from the web site. They just want to know that
5 privacy's protected in relation to that company.
6 The question I have for Paula is,
7 this latest thing with Hotmail where I think the
8 information on the e-mail of, what, 40 million
9 people was at risk because of the technical
10 glitch in Hotmail. You did an audit by a third
11 party auditor. Yet you had to keep the name of
12 the auditing company secret.
13 One of the things in privacy is you
14 have to have a certain amount of openness and
15 transparency so you can breed trust. Yet in this
16 situation you could not reveal the name of the
17 auditing company. I don't see how that squares
18 with engendering trust or fair information
19 practices.
20 MS. BURR: I'm going to let Paula
21 answer that question. We have two questions from
22 the audience directed to TRUSTe, so I'll just
23 read them to you: As a third party auditor for
24 NAI, how will companies like TRUSTe redress and-or
25 enforce violations of these NAI practices?

1 Similarly, if a TRUSTe web site initially told
2 consumers that they only used non-identifiable
3 information, but later wanted to change that
4 policy to one that tied information collected to
5 specific individuals, what would TRUSTe require
6 them to do?
7 MS. BRUENING: Let me start with
8 Evan. And what time are we finished?
9 Let's see. First of all, the Hotmail
10 situation involved a security breach that we
11 understood potentially placed the privacy of that
12 information at risk. We asked our auditors to go
13 in and to take a look at it.
14 We were not at liberty to announce
15 who the auditors were. There were particular --
16 I believe it was we were by law required not to
17 do that, and I don't know what you can do. I'm
18 not certain about that. We were not in a
19 position where we could do that.
20 MR. HENDRICKS: But we have to know
21 why, because you're in the trust business and
22 it's hard to trust if you don't know who's doing
23 the oversight.
24 MS. BRUENING: The important thing is
25 that we did have a third party auditor come in

1 and look at that and gave Microsoft a clean bill
2 of health. We can only operate under the rules
3 as they exist. If there was a situation where
4 that isn't enough, if we need to look further to
5 see if there's another way we should do that,
6 we'll look at that.
7 MR. HENDRICKS: Could you say which
8 rules? Are they the TRUSTe's rules or the
9 auditing company's rules?
10 MS. BRUENING: The auditing rules.
11 If there's a special provision and we decide at
12 some point it's got to be done in a different
13 way, we'll have to look at that. But under the
14 rules as they exist now, we did what we could do
15 to resolve that. We haven't gotten any more
16 complaints on that. I think it's a situation
17 that has been resolved satisfactorily.
18 Okay, the other two, do you have
19 those? The first question, about how would
20 companies like TRUSTe redress or enforce
21 violations of the NAI practices. First of all I
22 have to say, just because I'm sitting on this
23 side of the table, I have not had any prior
24 knowledge of this announcement. I heard it when
25 everybody else heard it, so I'm operating with
the information that I heard in the last half an hour.
I think that, first of all, TRUSTe requires compliance with fair information practices and we would welcome working with these companies to the extent that we think these companies are willing to work toward fair information practices. I haven't looked closely at the provisions that you've announced, but that would be very important.
I think that, to the extent we could work with them, at this point, unless we look at your program and decide something else would be necessary, that this would be such a special case, I think that NAI would probably fall under the same rules that the rest of the licensees fall under where we have a dispute resolution process, that there are inquiries that we can make with companies when there are questions raised by consumers, that we can raise the level of that inquiry of things aren't resolved, that we can require audits. We have the ability to refer to the FTC and we do ultimately have the possibility to revoke a seal if that's necessary.
I have to reinforce, and I think that the incidents of the last week have made clear, that we're living and we're working in an environment that's evolving and we have to keep evolving this program. So I think that this may well just present another challenge where that's what we have to do.
MR. ZINMAN: Can I respond to just one of those comments. Just one of Evan's comments about after the RealJukebox thing I think happened. I think we weren't in the offices of RealNetwork, so we can't imagine the scurry and fury that went around there when they found out this was happening, but I do know, being another company in the industry, when you see something like that happen you respond immediately by taking a look at your own practices.
So I'd say that there was a lot of response that happened within the industry, people making sure that they weren't making any similar mistakes. This is part of the dynamic of a very fast-growing industry. So the challenge is, do we want to criminalize all this behavior or what we need to do is we need to work in a self-regulatory environment where all the companies who are involved in the fast pace of change can kind of work at doing their best to meet fair information practices and setting up standards for future activities with new technologies.
MR. HENDRICKS: I don't want to criminalize it. I just want to create a civil right of action so that if their wishes aren't respected they can do something about it.
MR. CATE: Well, I at this late moment would just like to briefly return to the broader set of issues, although it's difficult to do that without some reference to the discussion that's already been had. So let me be very brief.
First, self-regulation seems like -- it's fairly unremarkable to say that it's a good thing. That is, without regard to whether a specific piece of self-regulation is, that it's a good thing because it can deliver, backed up by effective enforcement, it can deliver very effective privacy protection. It can be far more specific. It can be far more easily changed in response to changing conditions than, for example, the 60 years it takes Congress to enact a bill or even the time it takes the FTC to act on a matter. So the self-regulatory approach has a tremendous amount to recommend it.
The second point, of course, goes back really in some ways to the last panel and to the issues more specifically dealing with profiling, which is this issue of treating non-personally identifiable information as having this privacy interest.
The complexity or the oddity of this is highlighted by the very problem of how do you opt out of its use. I want to tell you not to use information that's not about me or that you don't know if it's about me, and you said, well, we'll put a cookie on your computer. Well, again we're back to where I was in the last panel, which is now my computer has a privacy interest and it's opting out, but if I use my laptop that opt-out is no good.
This at least raises one potential problem and it's not a novel problem in self-regulation, and that is it's important that it not create confusion. In other words, the goal of self-regulation presumably is to be clear and direct and let people know what they are opting
in or opting out of or what have you.
2 This is one of the specific points I would raise with this, to be very clear that if we're letting people -- if we're giving the impression that you can opt out of non-personal information, in fact we don't know realistically what that means.
3 The point was mentioned earlier, opt-in versus opt-out, whether -- I think it was you -- whether this should be an opt-in situation. I just can't let the sort of reference pass without at least noting it's not just six of one or half a dozen of the other.
4 The ramifications of one versus the other are very significant, and even places like the EU, which you mentioned, which have clear opt-in laws on the books, we see increasingly using opt-out as the de facto enforcement mechanisms, the way in which they work.
5 This is particularly true, say, for HR data in Europe. We have not see data on the books, we see increasingly using opt-out as the de facto enforcement mechanisms, the way in which they work.
6 This is particularly true, say, for HR data in Europe. We have not see data on the books, we see increasingly using opt-out as the de facto enforcement mechanisms, the way in which they work.
7 Finally, though, and very much on point with the panel, one has to wonder to some extent that technology isn't about to put a lot of these concerns to rest. You know, we saw the presentation earlier. We all know about other types of technologies. We see new technologies debuted all the time which make it increasingly easy and affordable to browse the Internet wholly anonymous, anonymous in every sense of the word.
8 I think as we think about self-regulation one of the components that necessarily has to be thrown in here is thinking about the availability of these technological solutions as well.
9 Thank you.
10 MS. BURR: Andrew.
11 MR. SHEN: I just have a comment about regulation in general and about fair

1 information practices. I think it's important to look at fair information practices not as a goal, not as something we should aspire to reach, but as something that consumers should have now. We're talking about information collected from individuals and, whether companies believe it or not, this is information that they may want control over.
2 I'm not going to refer to Dr. Westin's survey. I'm actually going to refer to a different survey done by Georgia Tech. I have the results from 1997. Sorry I don't have the more current ones, but this is based on more than 14,000 respondents, which I believe Dr. Westin's survey was based on about 400.
3 It said that 87 percent of the users believe they should have complete control over the demographic data. Now, I can attest that complete control follows notice, consent, access, and security, not the sort of stripped-down measures that we often see, like notice and opt-out. So I think it's important to keep that in mind, that consumers want more and the government has the ability to provide it to them and that we shouldn't rely on self-regulation as the only model out there.
4 MR. JAYE: Could I make just one comment? If we're going to bandy surveys about, there's a very interesting result that Professor Westin presented in Cambridge at the U.K. Privacy Laws in Business Conference this summer. He referred to it briefly this afternoon. But one of the interesting results that came out in his presentation was the fact that consumers in the United States had better privacy protection than they did.
5 So the interesting anecdote there is that regulation alone isn't a solution, either. I think that self-regulatory frameworks are absolutely essential. We believe at NAI that this industry is so fast-paced, so moving, the things we're talking about now almost no one understood three or four years ago.
6 I think it would be very difficult for regulations to be able to be enacted that wouldn't necessarily hamper the growth of electronic commerce and advertising on the Internet.
7 MR. SHEN: Can I respond to that very
quickly. I hear that argument a lot, that the
Internet is moving very fast. We hear the phrase
"Internet time" all the time, that it's
impossible for the government to regulate on
specific issues, like online profiling and the
collection of information. But the fact is that
fair information practices are never going to
change. These are the cornerstones for the
ability of the consumer to control their
information -- notice, access, security, consent.
I mean, these are never going to be
changed, and these can be enshrined into law.
The FTC recently did a very good job on the
Children's Online Privacy Protection Act. It was
a very complex issue. They're dealing with how
parents should be involved in the process of
giving up the information on their children, but
the FTC did a very good job and it did it within
one year. So it is possible to do that and do it
effectively.

MS. BURR: Steve and then Jerry.
MR. LUCAS: Just two quick comments.
We haven't talked much about the economics of
to what we're doing from the perspective that we all
know that click-throughs are dropping through the
do not include the notion of specific and
unambiguous consent and don't include the notion
of access, we still have countries outside of the
EU that have very strict data privacy laws.
While I'm not suggesting that we fold
up the tent and agree with every data protection
law that's out there, most of the other countries
have similar types of fair information practices.
\There's over $500 billion worth of e-commerce
that's at stake here between ourselves and
Europe, and at some point in time -- we can put
delays off as long as we want to and we can put
all the hope we want into safe harbor, and I have
all the confidence in the world that we'll be
able to solve this issue.

But if we don't, at some point we're
going to have to step up to these issues.

They're not going to go away.

MR. MEDINE: We have time for just a
few more comments, but I know you wanted to
respond on information-based marketing.

MR. ZINMAN: That's right. Just
quickly, I have no doubt that advertisers will do
whatever is necessary to improve the returns they
get from advertising. So I don't think we should
be debating the effectiveness of one method of
advertising versus another, because advertisers
are going to direct their money at the one that's
most effective.

So if you're right and if we have
another panel, next time everyone will be doing
permission-based marketing.

MS. BURR: Jerry.

MR. CERASALE: The only thing, don't
force a specific business model. I think that
the real key here is to give American consumers
the knowledge and they're going to make a smart
choice. They're going to vote with their feet,
or in this case they're going to vote with their
mouse clicks.

That's the real key here, is to have
some faith in the American public when you give
them knowledge and you give them choice that
they're going to make, they're going to make
their decision. They're going to vote and
companies are going to fail that don't provide
what they need.

I think that's really the important
thing here, is to try and make sure that we give
them notice. The problem we had here today is
that people didn't know what was there. It wasn't transparent. It wasn't a relationship. So create it and let the marketplace go and put the faith back in the American consumer.

MR. KAMP: Jerry just made about half of my points just there. I agree with him, but I also think that one of the things that's going on here is this is an awfully complicated system. Computers for most of us are very fragile devices that crash on us and make us crazy, and one of the ways in which we get to where Jerry is is we make these things a lot simpler than they are today.

I think the fact that our law professor was confused this morning doesn't surprise me, and we have to get to that simplicity in this area so that consumers can understand the choices that they're able to make.

MS. BURR: The last word.

MR. HILL: Just in response to Jerry's comments, I think one of the things we've heard come out of this is this idea that a lot of the privacy initiatives are anti-marketing. I think that nothing could be further from the truth. I know my company's going to spend $20 million this year on advertising. Most of that or a large percentage of that will be online.

For us, we're looking for partners in our advertising initiatives that can meet the same standard of customer relationship that we have for ourselves. And it's proving somewhat difficult, but there is a growth. This group does not represent all the advertising initiatives. There are groups like Yesmail, Yoyodyne, Alladvantage -- different initiatives that have consent, permission-based.

One of the problems with the sole economic "let's let it work itself out" is what we saw with Firefly. Firefly came in and said: We're going to build consent tools, permission tools. And at the end of the day, whether through execution or bad timing, Firefly went almost bankrupt. That technology was acquired by Microsoft and has been turned into the number one profiling tool on the Net.

So that's the danger, is if we set up these profiles and there's no redress for consumers, when the companies that do fail because profiling wasn't in the best interest of customers, you've now got 80 million profiles on the auction block ready to be sold to someone.

And if customers don't have a way to say, you know what, I never agreed to engage in business with this company, then I think we have a problem with our framework.

So I think there are other options.

MR. MEDINE: Our apologies to Cookie No. 247. We weren't able to get to your question.

MS. BURR: That's emblematic of the day. This has been a very interesting panel and a very interesting day. Clearly, our work in this area is beginning and the companies here have told us that they are continuing to work and want input from the people around the table, and I imagine around the room as well, on the work that they are doing.

So thank you for coming forward, and we look forward to working with you on that.

We are going to go to some wrap-up comments, but before we do, since everybody likes to scoot out at the end, I'm going to give a few well-deserved thank-you's before we do that.

This truly has been a team effort of the Federal Trade Commission and the Department of Commerce.

Whoever said federal agencies don't work together well was wrong.

So I'd like to thank -- and this is for both David and myself -- people that we've worked with who have been instrumental and but for their hard work this event would not have happened: Martha Landesberg at the FTC, Laura Mozzarella at the FTC; Wendy Later, Sandra Leonis, and Christina Speck at NTIA; Don Friedkin and Mary Street at the Office of the General Counsel here at the Department of Commerce. And we've seen a lot of AV guys running around. The only one I recognized was Hershel Gelman, but whoever all the rest of you are, you deserve our thanks. Thank you very much to all those people.

We spent a lot of time getting up to speed on this technology and getting all of the various viewpoints that we heard around the table. So to all those people who worked on it, thank you very much.

(Applause.)

MR. MEDINE: We'd like to ask the panelists to keep their seats, and we'd like to invite up to the podium Jody Bernstein, who is
 REMARKS OF ANDREW J. PINCUS, GENERAL COUNSEL, U.S. DEPARTMENT OF COMMERCE

MR. PINCUS: Thank you, David.

First of all, I want to reinforce my thanks, not just to the people in the two agencies, but all the people who participated on panels today and the people who came and listened and participated in the audience. I think this workshop did just what we hoped it would do, which is to focus attention on an issue, a privacy issue that we feel has gotten less attention than it should, to put out there the business community's views, the privacy community's views, some of the technology that's out there, and really to begin a conversation about what to do about it that was helpfully kicked off by some of the initiatives that were announced here by the business community.

But that's not the end of it, that's the beginning; and we obviously hope that this dialogue will continue and will result, as other dialogues have that started in workshops such as this, with an approach to protecting privacy that will work for the growth of the Internet and that will also work to provide real and concrete protection to the privacy of consumers.

I guess Becky kiddingly said federal agencies don't often cooperate, but we have a very good cooperative relationship with the FTC. I think the reason for that is that both of us realize that addressing this issue in a real and concrete way is critical to both of our missions. For the Department of Commerce, we obviously care a lot about the growth of electronic commerce. It's a driver of our economy and the President has asked us to look over that issue. But we recognize that that won't happen if consumers don't feel that this is a safe environment in which to do business. So protecting privacy in all its manifestations is critical to that.

Just as important, the FTC realizes that in its role as the chief consumer protector of the government, protecting privacy is a critical element of that mission. So it's really an instance where both of our missions point us in the same direction and have really caused us, not just in this endeavor but in the whole privacy issues, to really be working together in lockstep, and it's something that we're very proud of.

I don't want to rehash everything that's happened today. It seems to me, as I said, a lot got put on the table and there's a lot for everyone to digest. I think it's also important to remember, as with anything in the world of e-commerce, we're dealing not just with our own domestic situation, we're dealing with a medium that's international. So to the extent we can devise solutions that work in the cross-border world, we're going to devise solutions that have a much better opportunity of effectively protecting consumers' privacy.

That's one of the reasons that we have concluded that self-regulation is an important and effective way to go, because it provides consumers with an ability to protect themselves, not just domestically with respect to laws that may or may not apply to any particular web site, since there's no way to be sure exactly what laws govern any particular web site, but through seal programs and other mechanisms, visual cues, give consumers a way to protect themselves. So we think that's an important methodology to pursue, with the caveat that that protection has to be real.

So we look forward to participating with all of you in the continuing discussions both of this issue and the other issues relating to privacy.

Now I introduce Jody Bernstein, who is, as David said, our colleague in this endeavor. Jodie is a true path-breaker in public
On-Line Profiling Workshop
Washington, DC
November 8, 1999

1 service. She's served in a number of roles in
2 the government, everything from Health and Human
3 Services to Environmental Protection to the FTC.
4 I'm proud to say she was a client of mine when I
5 was in private practice and we had a wonderful
6 working relationship then and we have a wonderful
7 working relationship now. She really puts
8 herself on the line every day to protect
9 America's consumers.
10 Jodie Bernstein.
11 (Applause.)

REMARKS OF JODIE BERNSTEIN, DIRECTOR,
BUREAU OF CONSUMER PROTECTION,
FEDERAL TRADE COMMISSION

MS. BERNSTEIN: Thank you very much,
Andy, for a very nice introduction. If I may say
also, as others have, what a pleasure it has been
12 to work with you and others at the Department of
13 Commerce on this very, very significant issue. I
14 do thank all of you participants, both on the
15 panels and in the audience as well, because I
16 think, once again, what we set out to do today
17 we may have achieved. That is to open up a
18 process so that all of us could better understand
19 a very complex issue.

Now, I really never dreamed that I
20 would stand here before any audience and say, you
21 know, I agree with Jerry Cerasale about these one
22 or two things. I never agree with Jerry Cerasale
23 at these things, so there has to be a certain
24 uniqueness about any given one of these sessions
25 that we hold.

But when Jerry said, and others have
26 said it as well, that the real problem here I
27 think that we were addressing today is no one
28 knew that this was going on, nobody knew -- I
29 mean, us ordinary people didn't know what was
30 happening. And at least from our experience,
31 whenever Americans find out that something is
32 affecting them that they know absolutely nothing
33 about, whether they had any ability to control it
34 or not, they get very upset and they want to know
35 what's going to be done about it and do they have
36 a way of controlling it.

I noted that in connection with the
37 children's statute and the rulemaking that,
38 happily, someone did point out that we did it in
39 one year because it needed to be done, and as
40 soon as parents understood that the theory behind
41 the law and the way we were going to implement
42 the law was to put parents in charge of
43 protecting their own children, they were
44 immediately comfortable with what was happening
45 to them. I think the same thing is probably at
46 issue in this instance.

A lot was accomplished today, I
think. A lot of sort of consensus issues were
addressed that will serve us all well. We were,
I think, to be encouraged by DMA and NAI in
connection with an effort to achieve what's been
achieved in other areas, and that is a self-regulatory
program that addresses what the
problems were today.

I'm looking over at Evan because I
never agree with him, either, and he always has --
luckily, they always give me a chance after
Evan has attacked the FTC to at least be on the
platform. In that context, I would just add to
Evan and others that, while the FTC has been very
supportive of self-regulatory programs, it is not
without the FTC's commitment to law enforcement.
Those things are coupled together in this area
and in other areas, and I think that is in my
judgment and I think in others why self-regulation has
achieved the amount of

credibility, particularly in the online
environment, that it has.
I would make one other point that I
don't think had sufficient stress today, and that
is that your program also included an education
component. We also believe that that's an
essential element of achieving an overall
comprehensive program that can -- and we've all
not seen all the details of everything -- can be
a successful one.

I think the key word is
"transparency," and if we all keep that in mind -- and I
think everyone has spoken for that
concept -- that we will have moved a long way.
We look forward to watching as this
program develops as you get more experience with
it, as we all get more experience with it. In
the end, I think that this forum which the
Department and the FTC sponsored will have
achieved at least an initial beginning of
achieving what has been a very complex, very
complex set of issues.
I would only add one more thing, and
that is that when we talk about notice and
opportunity to opt out, among the words that I
1 heard today was don't make it confusing, keep it
2 simple, don't have it be so confusing that people
3 say, oh yes, it's out there, but how do I use it.
4 That's for all of us who would like to have a
5 very simple program so that we can tell others
6 what's happening.
7 Thank you very much. Again, thank
8 everybody for coming.
9 (Applause.)
10 (Whereupon, at 4:38 p.m., the
11 workshop was concluded.)
12
13
14
15
16
17
18
19
20
21
22
23
24
25