

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

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.



Page 6

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

Page 7

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.

Page 8

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.

Page 9

1 (Applause.)  
 2 REMARKS OF HON. ROBERT PITOFSKY, CHAIRMAN,  
 3 FEDERAL TRADE COMMISSION  
 4 CHAIRMAN PITOFSKY: Good morning,  
 5 everyone. I am delighted to be here with  
 6 Secretary Daley to jointly sponsor this workshop  
 7 examining online profiling. Senator Daley  
 8 continues to be a leader in advocating United  
 9 States interests and U.S. consumer interests in  
 10 electronic commerce.  
 11 The FTC has been involved in this  
 12 area for a long time. Starting four years ago,  
 13 we began to hold some workshops like this and  
 14 forums and seminars to try to find out the ways  
 15 in which electronic commerce was working and  
 16 where it was going. Our concerns were to find  
 17 out what information was being gathered in online  
 18 commerce, how it was used, what kind of notice  
 19 was given about use to consumers, and what were  
 20 their choices in controlling that kind of  
 21 information.  
 22 This is a promising new medium -- I  
 23 needn't tell this crowd about that -- perhaps one  
 24 of the most revolutionary new developments in the  
 25 marketplace in a hundred years. And yet one must be

<p style="text-align: right;">Page 10</p> <p>1 concerned about seeing to it that this  2 marketplace achieves its full potential. We are  3 aware that the reason people give who are not  4 currently engaged in purchases online or who  5 limit their purchases is that they do not think  6 it's a secure environment, and we must take that  7 into account.  8         Today we focus on a new aspect of the  9 collection of information from people. This is a  10 collection by firms that have no direct  11 relationship to the customer and where the  12 customers have no reason to believe that  13 information is being collected. An example: If  14 you were surfing the Web and you come across a  15 web page and there are some ads there,  16 information is collected that that's an ad that  17 you are exposed to, that you saw, and information  18 is collected from which people draw inferences  19 from this information and tailor future ads to  20 the supposed preferences of the viewer -- all  21 this without the knowledge and consent of the  22 person who is doing the viewing.  23         Not only do they not have notice or  24 an opportunity to opt out, but they don't even  25 know it is going on. That seems to me troublesome and</p>	<p style="text-align: right;">Page 12</p> <p>1 they address the serious concerns that all  2 must have about a technology that collects  3 information from people when they don't even know  4 the information is being collected.  5         So I look forward to hearing the  6 results of this workshop and I wish all of you  7 good luck for the remainder of the day. Thank  8 you.  9         (Applause.)  10         MS. BURR: Thank you, Secretary Daley  11 and Chairman Pitofsky.  12         Next I'd like to introduce Peter  13 Swire, who serves in the Office of Management and  14 Budget as the United States Chief Counselor for  15 Privacy. This is a recently created position  16 which demonstrates the importance that the  17 Clinton Administration places on issues  18 surrounding privacy.  19         Professor Swire is currently on leave  20 from Ohio State University College of Law and  21 from editorship of the Cyberspace Law Abstracts.  22 Peter.  23         REMARKS OF PETER SWIRE, ESQ.,  24 U.S. CHIEF COUNSELOR FOR PRIVACY,  25 OFFICE OF MANAGEMENT AND BUDGET</p>
<p style="text-align: right;">Page 11</p> <p>1 therefore requires careful  2 concern and careful review by all of us.  3         Maybe this is a good thing for  4 consumers. It might be. We are not opposed to  5 target marketing if the consumer remains in  6 control of the information that is collected.  7 Therefore, we want to learn more so we see what  8 the possible problems are, we know what the  9 virtues are of this technology, and we want to  10 learn more.  11         That is the occasion for the workshop  12 that we are conducting today. Our goal is to  13 develop consumer confidence and balance the  14 virtues and the possible problems of this kind of  15 online marketing.  16         I was pleased to learn just in the  17 last few days that leaders of industry and online  18 privacy have agreed to provide consumers with  19 more control in the creation of online profiles.  20 We have had good experience to date with self-regulation  21 in other areas of online commerce and  22 my hope is that we will have a good experience  23 here as well.  24         So I look forward to learning the  25 details of this proposal and seeing the extent to which</p>	<p style="text-align: right;">Page 13</p> <p>1         MR. SWIRE: Good morning.  2         What I'm going to talk about in my  3 brief remarks today is an attempt to put this  4 profiling workshop in context with some other  5 recent privacy developments and try to define  6 this term "online profiling" for our use today,  7 and then briefly preview the three panels.  8         I think when historians, if there  9 ever are any, of the privacy area in American law  10 and policy look back on when privacy took off,  11 the last few weeks may be a period that they'll  12 look back on as an historic change in how the  13 United States government and its people have  14 looked at privacy. Three weeks ago the Federal  15 Trade Commission made the final regulations for  16 the children's online privacy area.  17         In the last few weeks Congress has  18 been finalizing in the financial services area an  19 historic change that will have pretty much all of  20 the fair information practices built into the  21 financial services modernization that is going to  22 go forward. There will be new notice rules and  23 choice rules, access and security relating to  24 financial services, and new enforcement  25 provisions by all the functional regulators.</p>

<p style="text-align: right;">Page 14</p> <p>1           Then, ten days ago, President Clinton  2 in an Oval Office ceremony announced sweeping  3 medical privacy regulations that will require  4 patient consent for your medical information to  5 be used in a wide range of circumstances.  6           So as we think of some online  7 initiatives, financial services, medical, we see  8 a lot of things happening right now related to  9 privacy, and today's workshop looking at online  10 profiling continues that trend. This workshop  11 today was called for by Vice President Gore. He  12 invited the Federal Trade Commission and the  13 Department of Commerce to move forward to try to  14 study the phenomenon of online profiling and try  15 to see if there were any appropriate initiatives  16 from the privacy, if possible, to have a better  17 way of handling personal information.  18           In thinking about how to define  19 "profiling," I'd like you to consider two  20 hypothetical companies whose names I can use in  21 public because I checked ahead of time and they  22 have not been used. We have two companies. One  23 is Sellstuff.com and the other we'll call  24 Bannerad.com.  25           To define online profiling, I think much of</p>	<p style="text-align: right;">Page 16</p> <p>1   different when Bannerad.com is selecting  2 information and using it than when Sellstuff.com  3 is? I think the first point is that many people  4 don't realize that Bannerad.com is collecting  5 that information. Many people might guess that  6 Bannerad.com will collect information if you  7 click on a site. You then choose to go to that  8 site. You go to see what the ad takes you to.  9 You expect certain things to follow from that.  10           But almost anybody, except the  11 experts in the field, is surprised the first time  12 they realize that, they go to Sellstuff.com and  13 information about that transaction is going to  14 somebody else, is going to Bannerad. And that  15 surprise leads to a question of what will be done  16 next.  17           The concern that we have for this  18 online profiling, for the activities done by  19 Bannerad.com, is that there is a lack of  20 transparency on the who and the what of the  21 transaction. On the who, surfers don't know who  22 is that third party who's collecting information,  23 a company they've never heard of. Surfers also  24 don't know the what, what about them is being  25 gathered.</p>
<p style="text-align: right;">Page 15</p> <p>1   the attention today has been on the  2 Sellstuff.com's of the world, what you might call  3 first party web sites. So that means I go  4 online, I go to Sellstuff.com, and what are the  5 rules going to be about how Sellstuff handles my  6 information? What we've seen is a tremendous and  7 historic self-regulatory effort in this area.  8 TRUSTe is here today, Better Business Bureau  9 Online. Other groups have been working with  10 industry to come up with a set of principles and  11 a set of practices that make sure information  12 will be handled well when you go to  13 Sellstuff.com. That's the company that you  14 thought you were dealing with.  15           Today the focus is on something  16 slightly different, on what you might call third  17 parties that are at a web site. So now I go to  18 Sellstuff.com and there's a whole series of ads  19 up there. One of the ads might be from  20 Bannerad.com, a company maybe I've never heard of  21 before, and there are various ways that  22 Bannerad.com can collect information about me  23 while I'm surfing, and that's the focus of  24 today's workshop.  25           Why is profiling different? Why is it</p>	<p style="text-align: right;">Page 17</p> <p>1           So that we talk in the first session  2 today about cookies and other techniques that  3 help gather information, many times information  4 that we applaud. But for now let's point out how  5 little even a sophisticated surfer typically will  6 find out by looking at those cookies. If a  7 sophisticated surfer checks for the cookies and  8 gets an alert, they'll learn the name of the  9 company that's doing the collection and they'll  10 also learn the expiration date, which I usually  11 set for some number of years after the computer  12 will be junked. So again, that's all you'll find  13 out if you do your cookie alert: the name of the  14 company and some distant date of when the cookie  15 will expire.  16           Up until today's efforts, until what  17 I hope we'll be hearing this afternoon, the  18 surfer would not usually learn more about the  19 what, nor about what kind of data is being  20 collected, and under what terms and conditions. So what  21 we see then as a central issue is the  22 concern about transparency for the Bannerad.com  23 collection.  24           With that, let's preview what the  25 three panels are today and some of what we hope to</p>

<p style="text-align: right;">Page 18</p> <p>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.</p>	<p style="text-align: right;">Page 20</p> <p>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</p>
<p style="text-align: right;">Page 19</p> <p>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</p>	<p style="text-align: right;">Page 21</p> <p>1 in the first panel to come up to the stage and we  2 will move right into the program. Thank you.  3       Just a few housekeeping details as  4 the panelists come up. First of all, panelists,  5 what I suggest is you drag your chairs and move  6 them over to the side so you'll be able to see  7 the presentations.  8       Throughout the day, on the sides of  9 the room there are cards and pencils for  10 questions. Those questions will be brought up to  11 the table and we will ask the panelists as many  12 of those as we can. Also, the record of this  13 proceeding will be kept open through November  14 30th.  15       We're going to start this morning  16 with two presentations, two demonstrations of the  17 technology. First we will hear from Dan Jaye,  18 the co-founder and Chief Technology Officer at  19 Engage Technologies. Engage provides-driven  20 marketing solutions and Jaye is responsible for  21 delivering interactive database marketing  22 products and information services.  23       We will next move immediately, and I  24 won't stand up here and talk to you, to Martin  25 Smith, the Director of Enterprise Services at</p>

Page 22

1 MathLogic, Inc., an integrated digital marketing  
 2 solutions provider.  
 3 Dan.  
 4 REMARKS OF DANIEL JAYE, CHIEF  
 5 TECHNOLOGY OFFICER, ENGAGE TECHNOLOGIES, INC.  
 6 MR. JAYE: Thank you, Becky, for your  
 7 introduction and for your efforts on behalf of  
 8 the Department of Commerce to find the right  
 9 solution that benefits both consumers and  
 10 corporate marketers.  
 11 I am pleased to stand before you once  
 12 again to discover our common goals, to respect  
 13 the rights of consumers with regard to online  
 14 privacy while simultaneously pioneering an  
 15 industry that benefits all involved. I'm here to  
 16 inform all interested parties about online  
 17 profiling technology and its implications for  
 18 consumers.  
 19 Since I founded Engage in 1995, our  
 20 organization has been completely committed to  
 21 providing a novel and valuable technology, a  
 22 technology that enables the creation of online  
 23 profiles while keeping the identity of the  
 24 consumer protected and unknown to us.  
 25 Some of you may be asking, what is

Page 23

1 online privacy -- what is online profiling,  
 2 rather, and what are some of the benefits?  
 3 Profiling is the collection of non-personally  
 4 identifiable data by Engage about a browser that  
 5 enables web sites to customize ads and-or  
 6 content.  
 7 Profiling yields more effective  
 8 marketing for advertisers and web sites, that  
 9 will increase the advertising dollars spent on  
 10 the Internet, which will create more free and  
 11 subsidized Internet services for consumers. It's  
 12 a very clear and straightforward value  
 13 proposition.  
 14 Why do the advertisers need online  
 15 profiling and effective marketing? Because the  
 16 investments that are happening in the Internet  
 17 today will have to show profitability at some  
 18 point, whether it's in two months, two quarters,  
 19 two years. At some point, the investments that  
 20 are being made are based on the promise of being  
 21 a very effective media for communicating to  
 22 consumers.  
 23 Web sites have two critical needs to  
 24 each this. One is to be able to measure and  
 25 information its audience, being able to

Page 24

1 understand how many unique visitors have reached  
 2 that web site, and what are the special interests  
 3 of those visitors so that the site can be made  
 4 more compelling. In addition, they need to make  
 5 sure that the content and ads that are shown to  
 6 those visitors are relevant and effective.  
 7 Next I'm going to talk a little bit  
 8 about how third party ad networks work and  
 9 exactly how they work and how important they are  
 10 to being able to provide advertising  
 11 infrastructure to the thousands of sites on the  
 12 Internet. It begins with the web browser. The  
 13 web browser, when it visits a publisher web site,  
 14 for example a web site like Lycos or Yahoo, makes  
 15 a request to that web site for a web page.  
 16 When that web page comes back to that  
 17 web browser, it is displayed, but inside the web  
 18 page there are instructions that tell the web  
 19 browser to get an ad from an ad network. That  
 20 browser then makes a request of the ad network  
 21 for the ad to be displayed, and the ad network  
 22 then selects the appropriate ad based on a number  
 23 of different considerations, and that ad is then  
 24 displayed inside the web page.  
 25 At a future time, if the consumer

Page 25

1 clicks on that ad, the web browser then sends an  
 2 instruction called an ad click to an ad network.  
 3 This is important because the web site doesn't  
 4 actually know which ad was selected because the  
 5 ad network made the decision.  
 6 So the ad click goes to the network  
 7 so that the ad network can report on what  
 8 percentage of visitors clicked on the ad as well  
 9 as being able to send an instruction called a  
 10 redirect to the browser, so that the web browser  
 11 eventually gets the correct web page, whether  
 12 that be Procter and Gamble, IBM, or some other  
 13 advertiser. Then that advertiser's web site then  
 14 returns the correct web page to the consumer.  
 15 You can see that in this interaction  
 16 there are a number of different steps. The way  
 17 in which this information is delivered up to the  
 18 web site and back to the web browser relies on a  
 19 return address mechanism called an IP address  
 20 that many of you have heard of. It is critical  
 21 that the IP address, which is an inherent part of  
 22 the Internet, be transmitted to the ad network so  
 23 that the ad network knows to which computer to  
 24 return the ad.  
 25 What types of information do ad

<p style="text-align: right;">Page 26</p> <p>1 networks, the ad networks for example that use  2 Engage's solution, use? Our solutions are based  3 on non-personally identifiable information, which  4 we classify under two broad categories, and  5 management and reporting data. This is data that  6 is used to effectively run the ad service to be  7 able to report to an advertiser how many ads were  8 shown, how many visitors saw those ads, what  9 percentage of those visitors clicked on the ads.  10 Then the second area is what we're  11 terming ad delivery data. These are the types of  12 data that are used to determine what ad or what  13 content to show. In essence, ad delivery data is  14 ad management and reporting data that is used for  15 profiling.  16 When we use this type of information  17 for ad delivery, it is typically used by ad  18 networks to understand what the visitor wants,  19 without knowing specifically who they are. The  20 premise when I founded Engage was that on the  21 Internet you didn't need to know who the consumer  22 was to be able to deliver a relevant and  23 effective experience. We think that this is  24 actually an enhancement of privacy over  25 traditional marketing methods that require</p>	<p style="text-align: right;">Page 28</p> <p>1 cookies. Advertising spending is largely gauged  2 based on unique visitor counts. Being able to  3 determine how many unique visitors to a web site  4 or a portion of a web site requires the ability  5 to identify anonymously, or non-personally  6 identifiable, rather, an individual so that we  7 can determine whether or not that individual was  8 counted previously.  9 Then the final example of what  10 cookies are used for is to create and access  11 online profiles. At Engage an online profile  12 contains a collection of non-personally  13 identifiable information about the consumer's  14 preferences and interests. This is inferred at  15 Engage from the types of content visited.  16 At Engage our technology doesn't care  17 what page somebody went to. What we care about  18 is what types of content somebody went to. So it  19 involves a non-personally identifiable number or  20 identifier -- an example is shown on the screen -- and  21 the collection of interest scores scaling  22 from zero to one for that visitor or that  23 browser. The higher the score, the stronger the  24 interest.  25 The way in which this is built -- let</p>
<p style="text-align: right;">Page 27</p> <p>1 identifiable information, like name and address.  2 Typically this type of marketing is  3 implemented today using web cookies, a term some  4 of you may be familiar with. Briefly, a cookie  5 is information that is sent from a server to a  6 browser and that the browser then sends back to  7 that server when it returns to that web server  8 when it requests future web pages. Once again,  9 it goes back to the specific server that  10 originally sent the information down to the  11 browser.  12 Typically, these are used for three  13 purposes. First, remembering what was done  14 before. Sometimes this is called, technically,  15 state management. Second, shopping carts, the  16 ability to remember what purchases you have made  17 during a shopping visit, being able to figure out  18 what ad was displayed to that person, so when  19 they click on an ad they go to the right  20 advertiser's web site. Another example might be  21 sequencing of messages, for example telling a  22 story. These are all examples of state  23 management.  24 Remembering whether a visitor was  25 already counted is another critical use of</p>	<p style="text-align: right;">Page 29</p> <p>1 me take you through an example. If a user visits  2 a web site, for example Surfaround.com, he'll  3 receive this anonymous identifier or this non-personally  4 identifiable identifier, 23987  5 etcetera, and they have a score for money and  6 finance interest, sports interest, and automotive  7 interest based on their entire activity at that  8 site.  9 Now they visit another site that is  10 part of the Engage network -- and once again,  11 only sites that have a business relationship and  12 a set of contracts that cover in addition privacy  13 policies provide information for this type of  14 profiling at Engage. When they go to  15 Investinstocks.com, Engage will understand, not  16 that they went to that specific site, but rather  17 what is important, that they have a stronger  18 interest in money and finance.  19 If they visit another site that has a  20 relationship with us, like Golfing, at that point  21 their sports score will be enhanced and so then  22 we will also develop a score, for example, that  23 would indicate a level of interest in golf.  24 Then finally they visit an automotive  25 site. Automotive content will then impact the</p>



<p style="text-align: right;">Page 30</p> <p>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       What would it be used for? We talked  7 about today the example of banner targeting,  8 delivering once again golfing ads to a person  9 with golfing interests. But in addition it can  10 be used to navigation and web surfing easier, for  11 example moving content of interest to that person  12 to the top and obvious part of the page instead  13 of burying it three levels down on the web site.  14       Some of the things that we do at  15 Engage are areas that we think are important for  16 the industry, and some of these areas are  17 practices that we have implemented based on  18 conversations over the past several years with  19 the Department of Commerce and the Federal Trade  20 Commission. They have been very helpful in  21 providing us feedback and suggestions, and we  22 have tried to address these where we can.  23       First of all, we have been focused on  24 non-personally identifiable Internet marketing  25 since we were founded. In addition, we have a</p>	<p style="text-align: right;">Page 32</p> <p>1 many instances that can uniquely identify an  2 individual person.  3       Very briefly, our dual-blind  4 architecture is something that allows an ad  5 network that uses our solution to pass this non-  6 personally identifiable information. We then can  7 pass back to that ad network a list of types of  8 ads that are the relevant ads for that visitor.  9 It uses multiple levels of identification so that  10 we can ensure that no ad network or site that  11 works with us can ever correlate data with any  12 other site.  13       Briefly, our privacy formula can be  14 summed up as the fact that we use non-personally  15 identifiable online profiling combined with a  16 requirement for notice and opt-out capability for  17 consumer choice and contractual enforcement with  18 our web sites that requires that they post  19 privacy statements and a link explicitly to our  20 web site privacy page at Engage.  21       We also work with third parties like  22 TRUSTe for certification of our practices and FTC  23 oversight is invoked.  24       In summary, we believe that for other  25 businesses there are business models that may</p>
<p style="text-align: right;">Page 31</p> <p>1 technology called dual-blind, which is the  2 ability to add an additional layer of indirection  3 to non-personally identifiable numbers. We have  4 had contracts with our web sites that require  5 them to post a privacy policy since 1997.  6       We have been providing an opt-out for  7 the information that we gather, even though it's  8 non-personally identifiable, once again since  9 1997. In addition, there's a lot of information  10 that we don't need for our business, so we don't  11 retain it. So for example, we don't keep IP  12 address information at a detailed level. We  13 don't keep track of the specific URL's or pages  14 and the content and which visitors visit that  15 information, and we don't track sensitive  16 interest categories, such as medical information,  17 local content interests, medical interests,  18 etcetera.  19       Then finally, we make sure that the  20 data we have in our cyberdata center is  21 structured so that no combination of this data  22 can be reversed back to an individual. Sometimes  23 this is called triangulation. For example, we  24 don't keep the combination of zip code and the  25 exact date of birth of the individual, because in</p>	<p style="text-align: right;">Page 33</p> <p>1 give personally identifiable information and they  2 may be appropriate for other businesses that have  3 a direct consumer relationship and that follow  4 fair information practices. But at Engage we  5 believe that for us non-personally identifiable  6 information-based profiles balance consumer and  7 industry interests.  8       We also believe that as the industry  9 matures the business models and solutions will be  10 developed that will benefit both consumers and  11 marketers. For example, the work that is going  12 on with P3P as one potential innovative  13 technology, as well as other developments, will  14 cause rapid changes that we believe will help  15 everyone.  16       Thank you once again.  17       (Applause.)  18       REMARKS OF MARTIN SMITH, CHIEF TECHNOLOGY  19 OFFICER AND VICE PRESIDENT, MATCHLOGIC, INC.  20       MR. MARTIN SMITH: Good morning. I'm  21 Martin Smith from MatchLogic. Let me give you a  22 little bit of background. MatchLogic is a full-service  23 digital marketing services company based  24 in Colorado. We work with quite a number of the  25 leading advertisers in the Fortune 50 and also in</p>



<p style="text-align: right;">Page 38</p> <p>1 advertising is truly working.  2 To the first point of the predictive  3 modeling and the online profiling, why we're here  4 today, MatchLogic's profiling system -- I'll  5 provide you with a basic overview and then get  6 into the data specifically that we're capturing  7 within that, how then we generate the profiles,  8 how we use those profiles, and the privacy issues  9 that that creates.  10 What MatchLogic does is take  11 variables from our known data set. This is not  12 personally identifiable information. This is  13 non-identifiable information, such as  14 demographics, so age, income, gender. Because of  15 the nature of the targeting, we then, before we  16 put the segmentation in there, we actually do a  17 preclassification. So at the point the data is  18 entering into a profiling system it is already  19 pre-aggregated and is non-identifiable. No  20 identifiable data is brought across into the  21 process.  22 From the segments, we're then able to  23 look at what specifically the patterns of  24 information from the unknown or the web surfing  25 behavior is. From that we then train or build a</p>	<p style="text-align: right;">Page 40</p> <p>1 statistical algorithm.  2 We then take that and build our  3 prediction model and apply that. How we use that  4 information is in the serving of targeted  5 advertisements. That can be segment-specific, so  6 if an advertiser has specific geographic segments  7 or their product or service breaks down into a  8 number of brands or sub-brands they're able to  9 fit, based upon the segments, the right message  10 that is most appropriate to that segment.  11 That provides them with a very  12 powerful tool to then provide optimization across  13 the media. So if you think of the analogy,  14 rather than buying an audience on television,  15 where you have high potential wastage, you're  16 able to buy an audience of the same magnitude,  17 then segment it and optimize the inventory across  18 a number of services or products.  19 The second area, second key area, is  20 in site analysis, specifically what audience  21 segments are producing the most significant or  22 salient results. That provides key measurement  23 to either customization of the site or  24 presentation of the correct either navigation or  25 dialogue within the site. This leads to</p>
<p style="text-align: right;">Page 39</p> <p>1 model, using a combination of latent semantic  2 analysis, linear regression, and neural network  3 modeling.  4 The output of that model is then  5 tested against the unknown segments and  6 reapplied. From that, we are then able to  7 statistically predict the area and the geography.  8 So within the system, Martin Smith living in  9 Colorado does not exist within the system, nor  10 can it be tracked back through the system. The  11 fact that I am a male living in Colorado is about  12 as far as we go.  13 Third party ad serving is one of our  14 primary data sources. We also capture in  15 addition page, channel, search terms in some  16 cases, IP browser, operating system, date and  17 time. That information is linked by cookie,  18 which Dan identified and showed you what that is.  19 That as an input variable to the web  20 surfing behavior is encoded into a token, rather  21 like the one you saw from the Engage model.  22 Simply, that is a statistical value allocated to  23 that variable. So again, we're not passing  24 through into the modeling the specific nature of  25 site, content of that site. It becomes a</p>	<p style="text-align: right;">Page 41</p> <p>1 significant improvements in performance and  2 provides us the ability to really start to  3 customize content that is appropriate to those  4 specific segments.  5 As mentioned in the opening  6 addresses, this then does throw up some very key  7 issues from privacy. MatchLogic has been  8 instrumental in a lot of the thinking from the  9 industry point of view with regard to privacy,  10 with regard to how we relate to our consumer.  11 The third party model does provide us  12 with challenges. It is seamless to the consumer.  13 Our focus is to deliver advertising in a totally  14 clear way. Believe me, we would know if the  15 adverts did not get to the page, from both the  16 publisher and our advertisers. By that fact, we  17 are in the background.  18 Our challenge is to provide notice  19 and choice, which is part of what today is about  20 and will be addressed this afternoon. It is also  21 beholden to us to make sure we prohibit the  22 linkage of personally identifiable information  23 into the process, which is how we have  24 architected our systems. We have also  25 architected them to be able to preclude people</p>

Page 42

1 that do not wish to receive targeted  
 2 advertisements or to have any of their  
 3 information tracked across.  
 4       The next area is also to provide  
 5 education. As a founding member of TRUSTe, we  
 6 take that role very seriously and have invested  
 7 significant dollars in supporting that, and to  
 8 provide choice to the consumer.  
 9       Thank you.  
 10       (Applause.)  
 11       MS. BURR: Just give us a moment  
 12 while we rearrange here.  
 13       (Pause.)  
 14       PANEL DISCUSSION I  
 15       MS. BURR: Thank you. Those were  
 16 very interesting presentations and I think  
 17 they'll help us as we move through the day.  
 18       Let me just introduce the people who  
 19 are sitting up on this panel who will help us  
 20 discuss the technology issues this morning. To  
 21 my right is Lori Feena, who is the Chairman of  
 22 the Board of the Electronic Frontier Foundation.  
 23 Lori has worked for years to focus the  
 24 organization with respect to participation in  
 25 legislation, court proceedings, and a number of

Page 43

1 other areas in order to promote the protection of  
 2 civil rights and ethics online.  
 3       Jason Catlett is the founder and  
 4 President of Junkbusters Corporation, an  
 5 authority on privacy and marketing, and a  
 6 frequent participant in our conversations here.  
 7       I introduced Dan and Martin earlier.  
 8       To my immediate left is David Medine,  
 9 a familiar face to all of you from the Federal  
 10 Trade Commission and somebody I've worked with  
 11 for years on this issue.  
 12       Next to David is Kunwar Chandrajeet  
 13 Singh, or K.C., I believe, the founder of both  
 14 Hyperportals and Cyberknowhow. K.C. has been  
 15 involved in communications technology issues  
 16 since 1979, when he was responsible for the first  
 17 electronic interactive stocks and shares  
 18 information and trading system.  
 19       Richard Smith is an independent  
 20 Internet security consultant based in Brookline,  
 21 Massachusetts, and prior to that he was the  
 22 President of Farlap Software for 13 years. You  
 23 guys are outboarded here.  
 24       Eric Wenger is the Assistant Attorney  
 25 General in Attorney General Elliott Spitzer of

Page 44

1 New York's newly formed Internet Bureau. Eric  
 2 also serves as the Chair of the Internet Privacy  
 3 Working Group of the National Association of  
 4 Attorneys General, and Eric has also been active  
 5 with David and with me in a number of these  
 6 panels for years.  
 7       Finally, on the end is Danny  
 8 Weitzner, the Technology and Society Domain  
 9 Leader for the World Wide Web Consortium. I love  
 10 these titles. He is responsible for developing  
 11 Internet technology standards addressing many  
 12 issues, including user privacy. Before joining  
 13 W3C, Mr. Weitzner was co-founder and Deputy  
 14 Director of the Center for Democracy and  
 15 Technology, and after a two-year stay in Boston  
 16 we're very happy to have Danny located back in  
 17 Washington. He's been very important to us in  
 18 all of these.  
 19       The way that we will proceed is  
 20 familiar to those of you who've come to these  
 21 workshops before. This is a slightly more formal  
 22 setting than we've had, but obviously needed to  
 23 accommodate the interest that we have in it. But  
 24 generally, we've asked the panelists not to make  
 25 prepared statements. We really intend to have a

Page 45

1 conversation, and we will proceed on that basis.  
 2       David, do you have anything you want  
 3 to say?  
 4       MR. MEDINE: No.  
 5       MS. BURR: Okay. And just to remind  
 6 you all, as we have said before, there are cards  
 7 on the sides of the auditorium and your questions  
 8 will be brought up to us.  
 9       MR. MEDINE: I just wanted to mention  
 10 that the opportunity for people to submit  
 11 comments in writing to us, which started with the  
 12 publication of a Federal Register notice, will  
 13 continue until after this workshop, until  
 14 November 30th. So if there are issues that arise  
 15 today during the discussion that people would  
 16 like to comment on in writing, please submit  
 17 those comments pursuant to the procedure outlined  
 18 in the Federal Register any time up until and  
 19 including November 30th.  
 20       MS. BURR: Thanks.  
 21       Okay, we've heard about MatchLogic's  
 22 technology and Engage's technology. Before we  
 23 get down to the policy issues, I'm curious about  
 24 other technologies that are used by online  
 25 profiling companies to collect information about

<p style="text-align: right;">Page 46</p> <p>1 consumers. Can either Martin or Dan or both of  2 you talk just briefly about other, or Jason or  3 anybody else at the table, briefly about other  4 technologies that are out there and perhaps  5 differences significant for privacy purposes?  6 MR. MARTIN SMITH: I'll take that one  7 as I don't have to speak ill of any competitor.  8 Dan in his talk today said that Engage's profiles  9 are not personally identifiable. His company's  10 made a commitment to not personally identifying  11 these profiles. However, obviously these  12 profiles could by some other company that had not  13 made such a commitment become personally  14 identified.  15 The dangerous thing about these  16 profiles is that they amass a huge amount of  17 information. Dan gave you three examples,  18 banking and a couple of other examples. But the  19 interest vectors are typically several hundred  20 fields wide. That represents an enormous  21 profile, which can be collected over a period of  22 years and then subsequently identified. That is  23 where they become so unfair.  24 There are many companies out there  25 who will gladly identify a profile for you based</p>	<p style="text-align: right;">Page 48</p> <p>1 Internet and will take appropriate measures. The  2 problem, as my colleague just mentioned, is that  3 there are companies who would not, and especially  4 companies outside the country. One of the main  5 concerns that I have is that if the control of  6 Internet were to go out of these shores, then  7 most of what you are talking about here would be  8 hypothetical.  9 MS. BURR: Lori.  10 MS. FEENA: I think actually that is  11 a very good segue. First, the delineation  12 between online profiling and offline profiling is  13 a false one. We really can't assume that the  14 bricks and mortar world is no longer part of this  15 discussion. The bricks and mortar world of real  16 life stores and situations where you aren't  17 actually touching a keyboard also collect data  18 that goes into this profile.  19 As you drive through the easy-pass or  20 whatever, the toll booth convenience payment  21 systems are, they collect data. You don't have  22 to be online to do that. As you shop in the  23 grocery stores, you are building a profile.  24 They're not just simply trying to figure out an  25 easy way for you to clip coupons. You're</p>
<p style="text-align: right;">Page 47</p> <p>1 on a cookie. Two leading companies in this area  2 are Navient.com and Cogent.com, and I don't  3 believe that they're represented here. So I just  4 came from Adtech last week, the leading  5 conference in this field, and the explosion of  6 technologies for adding identity of the offline  7 world to online data is really one of the hottest  8 issues in that industry.  9 So really, we're not seeing the  10 entire picture. If we think this is 100 percent  11 ethical and this has been identified, that is  12 where the money is and that is where the industry  13 is going.  14 MS. BURR: K.C.?  15 MR. SINGH: I'll take that.  16 Basically, we are only talking about containing  17 the loss of privacy here. There is going to be  18 some loss of privacy. Each wave of technology  19 brings with it the inevitable dilution of  20 privacy. When the written word was invented, so  21 was the possibility of somebody actually taking  22 your letter and intercepting it.  23 So I am sure that all the companies  24 that are involved in profiling realize that  25 profiling is also vital for the growth of the</p>	<p style="text-align: right;">Page 49</p> <p>1 building a profile.  2 So the discussion of online versus  3 offline is really where the technology is going.  4 We are all connected on a network, whether it's a  5 bricks and mortar store or whether you're at your  6 keyboard at your desktop. I think the profiling  7 demonstrations that were given here talking about  8 the online world are also -- very appropriately  9 can be applied to the offline situation as well.  10 So we aren't talking about a  11 situation where this is simply the online world.  12 MS. BURR: Danny.  13 MR. WEITZNER: Thanks, Becky. I  14 think Lori just explained to us why President  15 Bush avoided those supermarket scanners.  16 While we are sort of pushing on some  17 of the distinctions here --  18 VOICE: We can't hear back here.  19 MR. WEITZNER: Can you hear now?  20 VOICES: No.  21 MR. WEITZNER: Is the microphone on?  22 VOICE: No.  23 MR. WEITZNER: Can you hear me now?  24 Yes, you can hear me.  25 While we're discussing some of the</p>

<p style="text-align: right;">Page 50</p> <p>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 But we should certainly recognize  21 that there's going to be an explosion of profile-based  22 information, both provided by users and  23 created by a whole variety of services, with  24 advertising profiling really probably only the  25 tip of the iceberg.</p>	<p style="text-align: right;">Page 52</p> <p>1 Briefly, with regard to IP addresses,  2 the technology doesn't really care very much  3 about IP addresses. It is important that between  4 one page request and the reply to a page request  5 by the server that the network is able to return  6 the page from the server to the correct browser.  7 But over time persistent or static IP addresses  8 are by no means acquired and in fact are not the  9 norm on the Internet at this time.  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 MS. FEENA: Just to further note on  16 that, the IP address is simply one way to create  17 a global user ID. This is a new term that I  18 think we are all going to become much more  19 familiar with. Some people call them GUID's.  20 Essentially, there needs to be some identifier to  21 create a profile to continue to aggregate  22 information about the identity or the person  23 profiled. So there's generally a global user ID,  24 in some cases -- well, it's true. You can create  25 many different ways to put walls between the ID</p>
<p style="text-align: right;">Page 51</p> <p>1 I would just add also that the  2 gentlemen at the end of the table have been very  3 clever at working with really what is widely  4 recognized as entirely inadequate technology,  5 namely cookies, to do all the profiling and in  6 some cases to provide a level of security and  7 privacy, which is even harder in some ways. I  8 think that we're going to certainly see on the  9 web the rise of much more structured information,  10 information that carries with it much more  11 meaning, that identifies certain information as  12 credit card numbers or as a name, etcetera.  13 So the good news and the bad news is  14 that this technology for profiling purposes is  15 going to become far more capable than it is  16 today.  17 MS. BURR: Does the use of this  18 technology depend on a persistent IP address? In  19 other words, people coming through AOL get a  20 differently generated IP address whenever they go  21 out on the web. Are you able to use this  22 technology for that segment of the web users?  23 And if so, could you explain how?  24 MR. JAYE: This microphone is  25 working? Good.</p>	<p style="text-align: right;">Page 53</p> <p>1 and who the person is, but the reality is there's  2 a central identifier.  3 In many cases, databases are not  4 always aggregated according to one ID. There are  5 many different technologies, as we have seen  6 today, used in the offline world to aggregate  7 information and create a profile about a person  8 from many diverse databases, and frequently they  9 aren't joined together with perfect knowledge.  10 A lot of information, as you have  11 seen -- how many of you have gotten -- I happen  12 to be somebody who's divorced and I still get  13 information connected to me about my ex-husband,  14 although I've been divorced for many years.  15 Sometimes they take databases and they realize,  16 well, these two people used to be married, they  17 must still be married, and this address change  18 must be applied globally to this person.  19 Well, it isn't because I told them  20 so. It's because they had one database here and  21 one database there and they decided to link this  22 and put that in my profile, too.  23 So one of the things that we have to  24 worry about are some of the data movement and  25 data management tools that are used to better</p>

<p style="text-align: right;">Page 54</p> <p>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?</p>	<p style="text-align: right;">Page 56</p> <p>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, etcetera.  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</p>
<p style="text-align: right;">Page 55</p> <p>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</p>	<p style="text-align: right;">Page 57</p> <p>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.</p>

<p style="text-align: right;">Page 58</p> <p>1 I think that it's also important to  2 recognize that from a legal perspective, with the  3 exception of the children's rules and the  4 Children's Online Privacy Protection Act, there  5 are not really requirements that companies tell  6 consumers what they're doing with the information  7 that they're collecting.  8 Having said that, if a company does  9 post a policy, then we know that the Federal  10 Trade Commission and other law enforcement  11 agencies, including my office, are going to be  12 very interested in making sure that the policies  13 that they post are accurate.  14 I think that there is also some good  15 news with regard to the stories that we've seen  16 recently. The good news is that the marketplace  17 clearly puts costs on those who fail to propose  18 privacy policies. We've seen that in the  19 increasing number of web sites that have posted  20 privacy policies in the last year or two after  21 the Federal Trade Commission and the Department  22 of Commerce have thrown light on the past  23 inadequacies in that area.  24 We also see that companies who have  25 bad privacy policies that are exposed quickly</p>	<p style="text-align: right;">Page 60</p> <p>1 are and what you do so that they have the  2 opportunity to exercise in a meaningful manner  3 the opportunity to opt out.  4 MS. BURR: Can I follow up, Eric.  5 We've heard both from MatchLogic and Engage that  6 they are not collecting personally identifiable  7 information and not matching that information up  8 with individuals and not triangulating to get  9 that information. They also talked about a  10 commitment to do that.  11 In the absence of a relationship  12 between the data gatherers and the data subject,  13 how is that commitment enforced and are we  14 comfortable that that is an enforceable  15 commitment? Do you want to respond to that  16 before we go on?  17 MR. WENGER: I think that's the  18 challenge for law enforcement and for consumers  19 as well, for them to have some sort of faith in  20 the idea that the promises that they're going to  21 get from Engage and MatchLogic are going to be  22 followed or that there aren't other companies  23 that don't follow policies that are as privacy  24 friendly as the ones we've heard about here  25 today.</p>
<p style="text-align: right;">Page 59</p> <p>1 change them because they don't want to face a  2 public that has concerns about dealing with those  3 companies.  4 The Attorney General along with the  5 Federal Trade Commission and along with the  6 Department of Commerce favors the continued  7 development of self-regulatory mechanisms. But I  8 have raised in the past at other workshops some  9 concerns about whether in this marketplace, where  10 there are a lot of small companies and low  11 barriers to entry, self-regulation can reach all  12 those companies.  13 I want to add another concern here,  14 and I think this is something that has been  15 expressed, is the concern that if consumers don't  16 realize the companies with whom they're dealing,  17 then self-regulation may be a flawed model,  18 because if they don't know that they're dealing  19 with a particular company how can they be  20 expected to opt out of the databases. That's the  21 challenge that goes to this industry now.  22 I read with great interest the  23 proposals that they're putting forward about  24 opting out and I think that's going to be the  25 biggest challenge, is letting people know who you</p>	<p style="text-align: right;">Page 61</p> <p>1 That's going to be a difficult thing.  2 I think that the key for them if self-regulation  3 is going to work is to provide as much  4 transparency as possible to the consumers so that  5 they know who they're dealing with and also for  6 them to engage the services, I guess, of  7 companies that can perform audits for them, so  8 that they can certify that they are following the  9 policies that they say that they're going to  10 follow.  11 MS. BURR: We have a lot of requests.  12 Richard, then K.C., then Jason and Lori and then  13 Danny, in that order.  14 MR. RICHARD SMITH: Yes. My concern  15 here with right now this talk of anonymous  16 profiling is the fact that to identify somebody  17 is very, very easy at some later date. Jason  18 made this point a little earlier, but the fact is  19 you collect all this data and you want to match  20 it up to a cookie; well, all you do is you send  21 out an e-mail message that sends back both the e-mail  22 address and the cookie. So it's basically  23 pretty trivial for them to do matching e-mail  24 addresses.  25 So you know, if they want to put it</p>



<p style="text-align: right;">Page 62</p> <p>1 in blood here that they'll never do these kinds  2 of matching, that's fine. But business realities  3 make me concerned here. I mean, DoubleClick is  4 looking, is moving in the direction of matching  5 up online profiles to people, and to expect the  6 competitors not to go down that route if they're  7 being beat up in the marketplace is a bit much.  8       Also, companies are being bought and  9 sold all the time and promises today don't really  10 necessarily have anything to do with two or three  11 years from now. So the collection of these  12 massive, of these very large online profiles is  13 eminently matchable up with personal information  14 down the road, and that's the real concern here.  15       MS. BURR: K.C.  16       MR. SINGH: Thank you.  17       Firstly, the triangulization is  18 inevitable. We have to assume that, because all  19 the business sits on thousands of geocommercial  20 faults and there's upheavals going all the time,  21 and to say that one company is going to carry on  22 that policy is just impossible, because the  23 policy may not work with the new configuration  24 later.  25       But this has been all very, very</p>	<p style="text-align: right;">Page 64</p> <p>1 the cookies or even data mining based on the hard  2 drive or a persona of a person, basically a  3 persona of a computer, may find that there's all  4 kinds of interesting numbers of computers sitting  5 in different places sending out different  6 personas. So all the profiling technology may  7 have to change accordingly.  8       We can go back to the negative side.  9       MR. CATLETT: Since we're on the big  10 picture here, I'd like to discuss why advertising  11 has changed. About three decades ago --  12       VOICE: Would you mind speaking right  13 into the microphone.  14       MR. CATLETT: I'd like to talk about  15 how advertising has changed. About three decades  16 ago, Vance Packard wrote a book called "The  17 Hidden Persuaders" where he showed how  18 advertisers were using psychology to manipulate  19 people in ways that they weren't aware of. The  20 icon that we have now for that is Joe Camel.  21       Now, advertising has moved from an  22 era of mass communication to one of individually  23 targeted communications on the Internet.  24 Psychology also has moved from a theoretical  25 discipline to a very empirical one. It's now</p>
<p style="text-align: right;">Page 63</p> <p>1 negative. Let me just add very, very quickly a  2 small positive point, and then we can go back to  3 the negative side.  4       (Laughter.)  5       MR. SINGH: The positive thing, I  6 mean, we create vertical portals focused on a  7 single subject at a time. Just to give you an  8 example, if somebody is buying a book, say  9 "Catcher in the Rye," I'd like to make available  10 to him or her at the same time the information  11 that there are half a dozen chats going on about  12 "Catcher in the Rye" or related to that subject,  13 should he or she be interested in them. That's  14 very useful information and that's time-saving  15 and relevant.  16       The other thing is, a little googly,  17 as they say in cricket terms, is that the  18 consumer has with him that we don't realize yet,  19 we're in the early stages of computers. It's  20 like the time when there was just one TV in a  21 house. There is going to be a different computer  22 and thus a different hard drive in numerous  23 different places, workplaces, leisure places,  24 cars, in pockets, and so on.  25       All the companies what are sending</p>	<p style="text-align: right;">Page 65</p> <p>1 even called behavioral science. The icon for  2 that is the Skinner box, invented by a  3 psychologist called B.F. Skinner, where you have  4 a rat in a box and they flash a red light or a  5 green light and they give the rat an electric  6 shock or a piece of food or something.  7       Now, that is basically what is being  8 done now to consumers. Instead of the red light  9 and the green light, we have the choice of  10 thousands of different ads to choose from based  11 on the models that have already been built, and  12 the response that the rat gives -- I'm sorry, the  13 consumer gives -- is whether to click or not.  14       So every time you see an ad, you are  15 being experimented on, and you see a lot of ads.  16 On average, a consumer sees about 5,000 ads per  17 year. Each bit of data that's collected with  18 that goes into your profile, building these huge  19 profiles, which are totally unacceptable. They  20 are unfair practices and they should be stopped  21 immediately.  22       MS. BURR: Let me just follow that  23 up, because I think that's a little bit different  24 from what we heard this morning, unless I missed  25 something. Certainly it's true that information</p>

<p style="text-align: right;">Page 66</p> <p>1 is being collected about what users want, like,  2 and I think we'll hear a little bit later on that  3 in fact users really want that personalization  4 and value it.  5 But every time I see an ad it's not  6 clear to me that anybody actually knows anything  7 about me at this point, because my computer at  8 home is used by my husband, who likes  9 motorcycles, and my 14 year old son, who likes  10 God knows what. So anybody who's using  11 information about the cookies on my hard drive at  12 home is getting a pretty confused picture of what  13 the world looks like.  14 MR. JAYE: Just two real quick  15 points. On that specific issue, the issue of  16 multiple users sharing the same computer, in  17 certain cases, depending on what browser you're  18 using, people are more and more personalizing  19 their browser because they have their favorite  20 home pages, they like to see their news a certain  21 way. When you use those types of techniques to  22 personalize your computer, generally the computer  23 manages cookies separately, so the profiles are  24 separate.  25 But in the case where it's one where</p>	<p style="text-align: right;">Page 68</p> <p>1 who the consumer is; our standard is that we  2 can't. Literally, if you go through our  3 database, we can't figure out who you are, not  4 that we won't.  5 MR. CATLETT: That's because your  6 company has gone to a tremendous effort in that  7 respect. It's actually easier to take, and  8 cheaper, to take the route of going directly to  9 the identity of the consumer, don't you agree?  10 MR. JAYE: Actually I don't, because  11 I think that the amount of effort and time that  12 would be spent to try to wade through all the  13 noise of changing computers and IP addresses and  14 networks and directories and then trying to deal  15 with -- there is a requirement, I believe, at  16 some point for the consumer to disclose an e-mail address  17 or some piece of information to  18 create linkage, and many studies show that  19 upwards of 70 percent of the information that's  20 disclosed is either deliberately or accidentally  21 misleading or inaccurate.  22 So once again, we believe there are  23 significant challenges to companies that try to  24 match online and offline data. And we believe  25 that we can deliver just as effective, if not</p>
<p style="text-align: right;">Page 67</p> <p>1 that isn't happening, then what you end up with  2 is what we would term a household profile, which,  3 from a positive standpoint, it might be somewhat  4 confused, but at least you know that somebody in  5 the household might be a golf fan and perhaps a  6 spouse wants to buy a present for their spouse,  7 etcetera. So it may not necessarily be  8 ineffective.  9 I did want to just point out one  10 thing. The comment was made about easy to match  11 a person's name and a cookie and the comment  12 about easy to match, you just send an e-mail  13 address and it sets a cookie. The whole point is  14 that e-mail addresses are personally identifiable  15 information. When we say we're non-personally  16 identifiable, we've already assumed and said we  17 don't have the e-mail address.  18 MR. RICHARD SMITH: You can buy the  19 e-mail address from a mailing house.  20 MR. JAYE: No, we have no way to  21 match it. The example I'm going to --  22 MR. MARTIN SMITH: The company who  23 buys you will.  24 MR. JAYE: The standard is not that  25 we won't violate privacy or we won't figure out</p>	<p style="text-align: right;">Page 69</p> <p>1 more effective, advertising through the use of  2 non-personally identifiable techniques.  3 MS. BURR: We're going to go to Lori  4 and Danny, but I have a question from the  5 audience for Lori and Danny, which is: How do  6 offline data collection practices compare with  7 non-PII profiling in terms of the privacy impact?  8 So in whatever you were going to say, if you  9 could address that as well.  10 MS. FEENA: Actually, I think that  11 I'll start with that. What we've seen in the  12 online world is, because of the great deal of  13 awareness that a consumer has that they are  14 actually on a network when they're on the  15 computer, there's been a higher degree of  16 concern, and I think the programs that we've put  17 in place -- I should also for clarity disclose  18 that I'm also a co-founder of TRUSTe, so I'm  19 wearing both hats, EFF and TRUSTe, when I say  20 this.  21 We took a higher standard of going  22 after notice and consent in the online world,  23 probably a higher standard than in the offline  24 world.  25 Secondly, as is demonstrated by a lot</p>

<p style="text-align: right;">Page 70</p> <p>1 of what Dan is saying and what Mike has also  2 done, is that architecture -- we have a saying at  3 EFF that architecture is policy. Architecture  4 begets policy. And Danny can probably touch on  5 this with the WC3. You've got many policy  6 standards that are being set right now that would  7 predict many technical standards, that would  8 predict how policies get implemented.  9 Things like SDML, which is a standard  10 for music listening and music players, actually a  11 portion of their standard deals with how  12 information is reported back from the player to  13 the server about a person's listening standard.  14 Some people may think that that actually is just  15 a technology standard and how nothing to do with  16 policy. But it does get into the whole area of  17 how do you give the consumer notice.  18 The same thing with profiling: How  19 do you make sure that technology that happens in  20 the background actually has a way for a consumer  21 to control this? So what we have here is sort of  22 a battle of the desktop or a battle on the  23 telephone or a battle on the little handheld  24 device for the goal of consumer control with  25 consumer convenience and consumer customization.</p>	<p style="text-align: right;">Page 72</p> <p>1 pointing out, they don't want to have to share  2 their browser preferences with their kids or  3 their parents. They want to have an experience  4 when browsing from some computer in a hotel  5 similar to their experience at their office or at  6 home.  7 For this reason, people want profiles  8 to work well for them and to serve them. I think  9 that what people don't want is to be surprised by  10 profiles. This is really a lot, and I think  11 we'll see this even more in the electronic  12 commerce arena with wallets.  13 People will want to carry their  14 electronic wallets around with them, be able to  15 make purchases easily, and certainly all of those  16 of you with commercial in this room want people  17 to make purchases easily and seamlessly, without  18 having to fumble around for their credit card  19 number and mistype the expiration date, etcetera.  20 At W3C we've developed the P3P,  21 platform privacy preferences, in order to help  22 users have more control over the various profiles  23 that are created of them, created about them, and  24 we think that's going to be an important part of  25 all these services. That's not going to solve</p>
<p style="text-align: right;">Page 71</p> <p>1 MS. BURR: Danny, you're on. I think  2 that one may be working now.  3 MR. WEITZNER: Is it working now?  4 No.  5 MS. BURR: Hopefully we'll get these  6 fixed at the break.  7 MR. WEITZNER: Thanks.  8 I want to come back to this question  9 about, I want to come back to the question about  10 the extent to which it's possible to re-identify  11 previously unidentified information. I guess I  12 think that we really shouldn't rely on the web  13 not being able to do things to get us to the  14 right policy outcome.  15 I think that companies, organizations  16 that make commitments to only follow certain  17 kinds of profiling practices, are to be  18 commended. But I frankly don't think that you  19 all aren't smart enough to do this if you want  20 to, and I think the underlying technology really  21 makes possible quite a lot of profiling.  22 I think that's only going to become  23 more and more true, for the simple reason that  24 people do want a personalized web experience.  25 They don't want to have, as Dan I think was</p>	<p style="text-align: right;">Page 73</p> <p>1 the problem all by itself, but it will help users  2 to manage the increasingly complex relationships  3 that they have, whether with services that are  4 really way in the background and they don't  5 necessarily know much about or services that they  6 have a more direct relationship with.  7 So I think the key is going to be to  8 give users the ability to have control over these  9 various profiles, to know they're there, and not,  10 as I think Eric pointed out correctly, have to  11 opt out from a profile that they don't even know  12 existed.  13 MR. MEDINE: Following up on that  14 point, to what extent do users today have control  15 over the technology that ad networks are using?  16 Are there ways that consumers can empower  17 themselves with current technological fixes, from  18 deleting files or setting browsers, to address  19 some of these concerns?  20 Obviously, later in the day we'll  21 hear about some industry efforts, but what can  22 the technology empower consumers to do today?  23 Dan?  24 MR. WEITZNER: As I mentioned in my  25 presentation, Engage has offered on our web site</p>

<p style="text-align: right;">Page 74</p> <p>1 an ability to opt out of our non-personally  2 identifiable profiling for several years now.  3 But it does -- a major question we deal with is  4 how do we get that capability and information out  5 to the users.  6 The way that we've done this to date  7 unilaterally has been through contractually  8 requiring our web sites to have a prominent  9 policy statement that discloses what's happening  10 and has a direct link to our privacy policy  11 statement at Engage.  12 You'll hear later on today some  13 discussions we've been having in the industry  14 about trying to make that a more uniform  15 practice. I think the point to be made is that  16 Danny is absolutely right on the fact that there  17 is not only a technology solution here. As one  18 of the original members of the P3P working team  19 and one of the original co-authors of the syntax  20 specification technical work on P3P, it is a  21 great technology that will yield benefits to  22 consumers and to marketers. However, it has to  23 be within an umbrella, a framework.  24 We believe that that framework should  25 be based on self-regulatory principles because</p>	<p style="text-align: right;">Page 76</p> <p>1 But I find this a completely  2 unacceptable solution to the problem because it  3 shifts the burden onto the consumer to defend  4 themselves against a practice of which they're  5 completely unaware and that's grossly unfair.  6 MS. BURR: Eric is next and then you.  7 MR. WENGER: I wanted to add one more  8 problem to the mix here with the idea of  9 transparency. That is, if I like MatchLogic's or  10 Engage's privacy policies, I don't really have  11 the opportunity to select which ad networks are  12 going to be giving me ads from the web sites I go  13 to. That I think is another fact that's going to  14 make the attempts at self-regulation difficult  15 here.  16 One other question I wanted to raise  17 is, we sort of glossed over the idea that  18 somebody put out the idea that static IP  19 addresses are becoming less common. I'm not sure  20 that that's true. I'd like to see the data on  21 it, because the cable industry is growing very  22 rapidly as far as Internet service is concerned.  23 My understanding is that they use static IP  24 addresses because you're permanently on the  25 network. And I imagine that most other broadband</p>
<p style="text-align: right;">Page 75</p> <p>1 the Internet evolves so quickly. Four years ago  2 there weren't ad networks. The models change  3 very quickly, and one of the concerns I think  4 that consumers should have is whether  5 legislation, hard and fast legislation, could  6 possibly keep up with the new nuances in  7 technologies that have come up.  8 MS. BURR: Mike, do you have anything  9 to add?  10 MR. CATLETT: I'd just add to David's  11 question about what consumers can do. The  12 simplest thing you can do is just turn off  13 cookies. Unfortunately, many sites export  14 cookies from you by not allowing you to use their  15 services, such as free web-based e-mail. Late  16 model browsers have a feature where you can turn  17 off cookies for all other than the site that  18 you're visiting, and that gets around this  19 invisible monitoring aspect of cookies.  20 The other thing that you can do is  21 use a product to filter out banner ads and that  22 removes the opportunity for surveillance  23 completely. My company, Junkbusters.com, has  24 been publishing a free banner-out filter for more  25 than two years.</p>	<p style="text-align: right;">Page 77</p> <p>1 technologies are going to use something similar  2 to that where, if you're going to be on all the  3 time, then you're going to have a number that, if  4 it's not -- it may be dynamic, in that with each  5 session the number changes, but if your sessions  6 go on for days then it's actually a fairly static  7 number.  8 The other thing is that the  9 percentage of people who get their Internet  10 service through work when they're on a network  11 that has a static IP address I think is fairly  12 high as well. So I wouldn't necessarily just  13 accept the idea that static IP addresses are  14 something in the past.  15 MS. BURR: I'm going to go to  16 Richard, but there's a question for you about  17 going back to the sorts of technologies that are  18 used in tracking, like GIF's and one by one web  19 bugs.  20 The other question that's come up is  21 that we often hear that the protocols as they're  22 written are not supposed to enable anybody other  23 than the site that set the cookie to read it, but  24 we've lately been hearing more about cookie  25 synchronization, and I'm wondering how prevalent</p>

<p style="text-align: right;">Page 78</p> <p>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.</p>	<p style="text-align: right;">Page 80</p> <p>1 So the transparency is extreme, and it's an  2 intentional one also.  3 MS. BURR: Mike.  4 MR. MARTIN SMITH: On the cookie  5 synchronization issue, what we really mean by  6 cookie synchronization is the matching of cookie  7 across the domain. What you're highlighting  8 there is the request to the server within a site  9 that somebody or the browser has actually  10 appeared on the site.  11 That is used for measurement across  12 the site rather than gathering any specific  13 demographic information. What it brings back is  14 the cookie, the IP, the operating system, and the  15 date and time. What it's saying is, if it's  16 associated to advertising data, how effective has  17 my advertising been, what pages within the site  18 has the navigation been.  19 There isn't any intention to  20 synchronize between the domains.  21 MR. RICHARD SMITH: Well, maybe not,  22 but what I did notice here is your slide talked  23 about demographic information like sex and age,  24 and what I was seeing in the Procter and Gamble  25 case is those one by one GIF's were very</p>
<p style="text-align: right;">Page 79</p> <p>1 Indeed, we have an opt-out option for that, but  2 that's after weeks of asking questions. That's  3 not really offered as an option.  4 Another quick thing here, cookie  5 synchronization gets even more sort of -- I won't  6 use the word "sinister," but interesting, let's  7 say, with the use of one by one GIF's. As an  8 example, prepping for this discussion here I was  9 looking at Procter and Gamble. They have  10 approximately 40 sites that are product specific,  11 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.</p>	<p style="text-align: right;">Page 81</p> <p>1 strategically placed to identify demographic  2 information. It was done also in the case of  3 some stuff for children and so on.  4 It's all hidden. That's what I'm  5 wondering about here, why is it hidden?  6 MR. MARTIN SMITH: The reason it's  7 hidden is for essentially page load. So we're  8 like a guest on that particular site. All we  9 need is a call to our servers. The reason we  10 need that call is if the page gets cached behind  11 a proxy server and you have high volumes of pages  12 cached, then there will be no counting across  13 those pages, so your actual media analysis, your  14 ROI analysis if it's a destination activity,  15 would absolutely be hosed. You would not get  16 consistent measurement.  17 We actually ran studies with Ernst  18 and Young two to three years ago in this area and  19 found that the percentage of pages that were  20 being served from behind proxy servers and  21 therefore not visible were actually on average  22 about 70 percent and on highly trafficked web  23 sites to the order of 700 percent, which in terms  24 of an order of magnitude from a measurement point  25 of view completely disrupts it.</p>

<p style="text-align: right;">Page 82</p> <p>1           So that's why it's there. The  2 reason, it's very clear, is that it's a very  3 lightweight request.  4           MR. JAYE: I just want to add to that  5 for a second because I just want to clarify one  6 issue. The examples you're giving, none of those  7 are cookie synchronization. It's a very  8 important point you're bringing up. Cookie  9 synchronization is taking cookies, which are  10 inherently as part of the protocol domain  11 specific, and trying to match them across  12 different domains.  13           So cookies are not inherently multi-  14 domain. Cookie synchronization is what takes  15 them across domains. In the case of, say, an ad  16 network serving onto another page, that is not  17 cookie synchronization -- so you gave the  18 DoubleClick example -- because the site that  19 DoubleClick is serving onto never sees  20 DoubleClick's ID.  21           So there is no passing of information  22 between the domains. There is no cookie  23 synchronization.  24           MR. RICHARD SMITH: AltaVista gives  25 your search string off to DoubleClick. That's no</p>	<p style="text-align: right;">Page 84</p> <p>1    investigating and we'll be announcing later today  2 with TRUSTe is that we do intend to extend the  3 same principles and practices that we've been  4 pioneering with many of the people in this room,  5 that we have pioneered on the web sites, to  6 actually apply to software and third party  7 services.  8           I think it's very important to  9 realize that this is not a simple solution. It's  10 a very complex problem and it's going to require  11 technology, P3P technology and other  12 technologies, to bridge this gap. It's going to  13 require programs like TRUSTe and BBB and  14 certification programs, as well as -- I'll even  15 bring this up -- I think it will also require  16 certain laws, because we do have a great deal of  17 this gap is being filled by the market forces, by  18 technology, by programs, and by very voluntary  19 high watermarks by industry leaders, but it  20 doesn't address many of the things that have been  21 brought up, which are the companies that haven't  22 participated, the companies that aren't  23 disclosing to consumers.  24           So when we look at this issue of  25 transparency to the consumer and consumer</p>
<p style="text-align: right;">Page 83</p> <p>1    passing of information?  2           MR. JAYE: No, there isn't. If you  3 would look at my architecture slide you would see  4 that the third party ad network doesn't have a  5 connection to the web server. It has a  6 connection to the browser.  7           MS. BURR: Excuse me one second. We  8 have just gotten a helpful technical message and,  9 since this is the technical panel, I want to pass  10 that on. The best way to keep the feedback off  11 the mikes is to tilt them down and bring them  12 closer, since all of us have them up.  13           Lori, you had a comment?  14           MS. FEENA: Yes. On the area of how  15 do you create this transparency for these third  16 party technologies -- can you hear now?  17           VOICE: Can you get closer to your  18 mike?  19           MS. FEENA: Okay, I will get closer.  20 How's that? Any better? I see heads shaking.  21           MS. BURR: Here's a mike.  22           MS. FEENA: This one's very much on.  23           In the area of trying to create  24 transparency for third party data in the  25 background, one of the things that we are</p>	<p style="text-align: right;">Page 85</p> <p>1    control, I think it's really important that we  2 look at this as not a self-regulation or law.  3 It's going to take informed consumers, because if  4 you give a consumer a choice but they don't know  5 what choice they're making it doesn't really  6 help.  7           What we have in the Internet is a  8 situation where huge decentralization is  9 happening, and we can't create a magic policy or  10 a magic law or a magic technology that can figure  11 out what the right amount of information is to  12 disclose in any particular transaction. It's  13 very contextual.  14           MS. BURR: I want to go to Danny and  15 Richard. I have a question from the audience  16 that one or both of you might take up, which is:  17 Why isn't the answer just cookie-killer software?  18 If you can't place cookies or they don't stay on,  19 you can't serve up these ads.  20           MR. WEITZNER: I think that certainly  21 the answer with respect to cookies is a better  22 specified technology, which is work under way at  23 the Internet Engineering Task Force, and that  24 we're certainly looking forward to seeing move  25 forward and implemented, because indeed cookies</p>

<p style="text-align: right;">Page 86</p> <p>1 are a pretty blunt instrument at this point.  2 But getting rid of cookies, as Jason  3 pointed out, maybe the problem there is not quite  4 extortion, but sites actually have good reason  5 for using cookies which have nothing to do with  6 invading anyone's privacy or surreptitiously  7 collecting information.  8 But I really want to just underscore  9 Lori's point because I think it's critical. I  10 don't know how many of you could follow the  11 interplay about this kind of cookie versus that  12 kind of cookie, but I can guarantee you that 99  13 percent of people who use the web can't follow  14 that kind of discussion, have no interest in  15 following that kind of discussion.  16 So certainly what we really need is  17 the commitment across the board from people who  18 are building services and building technologies  19 to put real tools in the hands of users that make  20 this experience less threatening, more  21 accessible, gives users more control. I think  22 the successful services in this area try to do  23 that.  24 I can tell you it's not easy and we  25 are still a ways away. I tried to install one of</p>	<p style="text-align: right;">Page 88</p> <p>1 discussing here is extremely important.  2 MR. WEITZNER: Could I just intercept  3 this on the way in that direction? There are  4 good models for addressing this sort of problem  5 and probably the best one that we can think of is  6 a technology called SSL. Most people don't know  7 what SSL is, but they do know what the little  8 locker key at the bottom of their browser is.  9 That one tiny piece of real estate on  10 web browsers has gone so far to close the  11 confidence gap that users have in purchasing  12 items over the web with their credit cards. We  13 need to get to that level of accessibility for  14 users, so that users see on their browsers tools  15 that they know how to use, that help them manage  16 their privacy relationships with all the entities  17 that are out there.  18 MR. RICHARD SMITH: Real quickly on  19 the question of the cookie buster software, the  20 big problem really is that there are sites that  21 require them. For example, I use my Yahoo for  22 customization and I need cookies for that site so  23 I don't have to keep logging in each time, and  24 the controls on the browsers are kind of all or  25 nothing. That's a problem.</p>
<p style="text-align: right;">Page 87</p> <p>1 the services that's going to be discussed on a  2 panel later today and erased most of my Windows  3 registry. So I had a sort of unpleasant weekend.  4 But I have a higher tolerance for this kind of  5 thing, and I guess to some extent I get paid to  6 deal with this sort of problem, whereas the  7 consuming public does not.  8 If we fail to close the usability gap  9 that Lori talked about, which I think has to be  10 addressed at all levels, at the level that the  11 certification programs work and at the technology  12 level and at the standardization level, we're  13 going to have an increasingly frustrated web-using  14 public.  15 MS. BURR: Eric and then Richard.  16 MR. WENGER: On the way to passing  17 the microphone I'll just through in one last  18 comment. I don't think it can be overemphasized,  19 the point that Danny's making, which is that if  20 consumers don't feel comfortable using this  21 technology and that their privacy is going to be  22 protected and that they're going to be protected  23 from fraud, then they're going to shy away from  24 it. That means that the continued growth of e-commerce  25 may be stunted. So the topic that we're</p>	<p style="text-align: right;">Page 89</p> <p>1 Maybe if there were some level of who  2 you'd accept cookies from, maybe like only from  3 the web site that you explicitly go to, rather  4 than an embedded image, that might be an  5 interesting solution.  6 MS. BURR: K.C.  7 MR. SINGH: First of all, if you see  8 us trembling it's because it's cold, no other  9 reason.  10 MS. BURR: It is very cold.  11 MR. SINGH: The important thing is  12 the e-commerce part of it, and the moment you  13 give your credit card there goes the  14 triangulation.  15 MS. BURR: Let's hear from the e-commerce  16 folks over there.  17 MR. JAYE: Consumer confidence is an  18 absolutely critical issue that we are very  19 concerned about, and that's one of the reasons  20 why we do want to find solutions that deal with  21 the transparency issue. We do think that there  22 is a middle ground here that benefits the  23 consumer and the companies that, candidly, pay  24 for all the free services and the free stuff on  25 the Internet, which are the advertisers, and that</p>





<p style="text-align: right;">Page 94</p> <p>1 advertising and bad advertising costs the same,  2 but the results are immeasurably different, holds  3 very true. Used correctly, targeting to segments  4 is producing significant results.  5 MS. BARR: I think we're going to go  6 to a break now. When we come back at 11:00,  7 we're going to hear some more information about  8 this from the consumer perspective.  9 I'd just like to point out that your  10 coffee break is brought to you by the Center for  11 Media Education, and we'd like to thank them very  12 much for their generous help in this.  13 (Applause.)  14 (Recess.)  15 MR. MEDINE: Thank you very much.  16 First a few announcements. If  17 someone from the Law Offices of Allen Schlaefler  18 has left a Daytimer, we have it and feel free to  19 come up and get it.  20 Second, again the comment period for  21 this workshop will be left open until November  22 30th.  23 Third is, Dr. Westin will be taking a  24 few questions and so, as with the prior panel, if  25 you do have questions, there are cards down on</p>	<p style="text-align: right;">Page 96</p> <p>1 (Pause.)  2 It's a pleasure to join this  3 workshop, which I think is addressing an  4 absolutely central question about the future of  5 the Internet and the way consumers will use it.  6 As I see it, we really have two concepts that are  7 trying to relate to one another and see if  8 there's the possibility of harmonious  9 relationship. The business model that's being  10 used on the Internet is to collect extensive  11 information about individuals as they move  12 through the Internet, to assess how the Net is  13 working, how presentations work, what responses  14 are to various kinds of offers, and also to offer  15 personalized communication to consumers.  16 But the consumer model is a powerful  17 desire to exercise informed individual choice as  18 to how personal information is collected and used  19 about people when they're on the Internet. So  20 the key issue is do these two models have the  21 potential to coexist, how do majorities of people  22 using the Internet see this issue today, and what  23 is it that they want Net companies to do if  24 they're going to collect and use personal  25 information.</p>
<p style="text-align: right;">Page 95</p> <p>1 the side of the auditorium and if you'd like to  2 pose a question to Dr. Westin, please fill out  3 the cards and they will be brought up to us.  4 It's my real pleasure to introduce  5 Dr. Alan Westin, who has been a regular  6 participant at all of the FTC and Commerce  7 Department privacy workshops. Dr. Westin has  8 been the Professor of Public Law and Government  9 at Columbia University since 1959 and he's  10 considered the nation's leading expert on  11 information privacy.  12 He's been a member of a number of  13 federal and state government privacy commissions,  14 an expert witness before state and federal  15 legislative committees and regulatory agencies,  16 and the academic adviser to Louis Harris and  17 Associates for 15 national and public opinion and  18 leadership surveys on privacy.  19 It's my pleasure to introduce Dr.  20 Westin to hear his latest survey results. Thank  21 you.  22 (Applause.)  23 REMARKS OF DR. ALAN A. WESTIN, PROFESSOR  24 OF LAW AND GOVERNMENT, COLUMBIA UNIVERSITY  25 DR. WESTIN: Are we up?</p>	<p style="text-align: right;">Page 97</p> <p>1 I think that we can gain some  2 insights from survey research in general, which I  3 want to talk about first, and then a particular  4 survey that has been done dealing with the issue  5 of collecting personal information for banner ad  6 presentations.  7 Actually, it's 40 national surveys, I  8 hasten to say, that I've been involved with since  9 1978, either with Louis Harris and Associates,  10 now called Harris Interactive, or Opinion  11 Research Corporation in Princeton, New Jersey. I  12 think the central theme in every one of these  13 surveys which we've tracked and I think has been  14 extraordinarily useful for the public policy  15 process is to trace the rising, steady concern of  16 American consumers, citizens, employees, about  17 personal information and privacy.  18 When we asked our first set of  19 questions right after Watergate in 1978, 68  20 percent of the American public said they were  21 concerned about threats to privacy. I think it  22 was something like 30 or 35 percent chose "very  23 concerned." Now we have 94 percent of  24 respondents saying in survey after survey, 92, 94  25 percent, that they are concerned about threats to</p>



<p style="text-align: right;">Page 102</p> <p>1 extraordinarily privacy-asserting and active in a  2 way that was not true in the data in the early  3 nineties or the middle 1990's.  4       Just look at these numbers. 78  5 percent of the public, representing 152 million  6 adult Americans, say that they have refused to  7 give information to a business because they felt  8 it was too personal or wasn't needed. 58  9 percent, representing 113 million, asked a  10 company they patronize not to market additional  11 products to them. And 54 percent, over 100  12 million, 105 million, decided not to use a  13 company or buy because they weren't sure how  14 their information would be used. That's the new  15 privacy veto at work.  16       Some other figures: 53 percent asked  17 a company they were using not to give their name  18 to another company for marketing, 103 million  19 adults. And in smaller numbers, but very  20 significant in terms of what I think will be a  21 rising trend, 21 percent looked to see whether a  22 business had a privacy policy -- that's 41  23 million adults -- and 35 million, 18 percent,  24 asked to see the contents of their own record.  25       So I think that what we're seeing is</p>	<p style="text-align: right;">Page 104</p> <p>1 people, would you be willing to do this if the  2 company gave you notice of how they would be  3 using your information and an opportunity to opt  4 out of uses that you did not approve of, we then  5 pick up 25 or 30 percent of people who were  6 initially negative and we wind up with 75 or 85  7 percent of the adult American public saying that  8 kind of customization is acceptable with notice  9 and opt-out.  10       (Slide.)  11       With that as background, let me turn  12 to the survey that I'm reporting on today, which  13 we call "Personalization and Privacy on the Net."  14 Questions were developed by me, put onto the ORC  15 weekly Caravan survey. This is a representative  16 national survey of roughly a thousand  17 respondents. What we got was 474 of those 1,000  18 who said they use the Internet, and that  19 represents about 92 million adults self-reporting  20 that they use the Internet once a week or more.  21       In survey jargon, that leads to a  22 confidence factor of about plus or minus 4  23 percent, which is not what you want if it was  24 electoral statistics, but is perfectly acceptable  25 if what you're looking at is broad public</p>
<p style="text-align: right;">Page 103</p> <p>1 an extraordinarily active consumer population in  2 the United States, concerned about privacy, but  3 not just concerned in the abstract, ready to take  4 actions to patronize or not patronize, to  5 exercise opt-out or not exercise opt-out, based  6 upon their sense of the way in which they want to  7 see their privacy balances set.  8       Right away in terms of understanding  9 the picture fully and therefore framing my  10 presentation today, we want to recognize that the  11 American public still represents extraordinarily  12 active and avid consumers. 110 million people  13 bought last year from direct mail that was sent  14 to their residence, and 48 percent of the public,  15 93 million adults, say they're interested in  16 getting information from companies about new  17 products and services.  18       60 percent, representing 117 million  19 people, say that it doesn't bother them at all,  20 it's acceptable, for companies to look at their  21 profiles in their records in order to customize  22 communications to them about other products and  23 services that the company thinks might be of  24 interest to them.  25       Then when we add a statement to</p>	<p style="text-align: right;">Page 105</p> <p>1 attitudes in an area such as privacy.  2       The survey was sponsored by  3 DoubleClick, well known as an industry company  4 that works in the banner ad area. I was the one  5 who developed the questions and wrote the report.  6 They were the sponsor of the survey.  7       (Slide.)  8       First a little bit about the sample.  9 As we analyzed it, 58 percent of Net users,  10 representing 53 million netizens, say that  11 they're interested in getting information from  12 businesses about new products and services. I  13 think it's interesting to note that that's about  14 10 percent higher than people who are not on the  15 Net, so Net persons have a bit more interest in  16 hearing about new products and services than  17 those who are not yet using the Internet.  18       37 percent of Net users say they've  19 purchased something or paid for information when  20 they were on the Internet. Half of Net users, 50  21 percent, say they have clicked on a banner ad to  22 view some kind of offer that was made in that ad.  23 But -- and this is a very important figure -- 27  24 percent of those who did click on banner ads say  25 that they bought something at a web site that</p>

<p style="text-align: right;">Page 106</p> <p>1 they went to. So you have roughly one-quarter of  2 people who click on banner ads saying they buy  3 something after they've gone to view what the  4 banner ad presents.  5 One of the things that I always try  6 to do in a survey is to make sure that the  7 attitudes about privacy of our sample track what  8 we know to be the national figures from many  9 other surveys, and we confirmed here that, as far  10 as Net users are concerned, 92 percent said they  11 were concerned about possible misuse of personal  12 data when they were on the Internet and 67  13 percent said they were very concerned.  14 So we have a kind of clear  15 confirmation that our Net sample paralleled the  16 general privacy concerns and attitudes of the  17 adult population of the United States in general.  18 (Slide.)  19 So we turn to banner ads and  20 personalization. Our key question asked: When  21 banner ads are presented to you as you use the  22 Internet, how positive would you be in having  23 some of these ads tailored to your interests  24 rather than seeing only random ads that are aimed  25 at all Net users? 61 percent chose positive,</p>	<p style="text-align: right;">Page 108</p> <p>1 they would use your information and you could opt  2 out of uses you did not approve." 29 percent of  3 those who were initially not willing said this  4 would make them willing, which gives us a total  5 of people who said they'd be willing to supply  6 their own information of 68 percent.  7 Now, obviously we used the term  8 "spelling out how they would use your  9 information" and that assumes on my part that  10 only a company that met a standard of spelling  11 out how you would use that information could  12 claim that this answer supported the way in which  13 they were operating on the Internet.  14 If a company only says, hey, we use  15 it for anything we like, or we use it in a way  16 that doesn't give somebody the ability to choose  17 and opt out intelligently, then in the broadest  18 sense the requirement of good notice or of good  19 communication would not have been met.  20 Secondly we asked: "By asking you to  21 allow information about your visits to web sites  22 on the Internet to be used to tailor Internet  23 banner ads to you." You can see that 44 percent  24 initially were willing. Then when we add those  25 that said they would be willing if there were</p>
<p style="text-align: right;">Page 107</p> <p>1 divided up into 18 percent very and 42 percent  2 somewhat, and that represents, as you see, about  3 56 million users of the Internet.  4 Having done that, we then wanted to  5 see what kind of information Net users say they  6 would be willing to give or to have collected and  7 under what conditions. The way we did this is in  8 a two-stage process that we've used in many  9 surveys in offline as well as online contexts.  10 First we asked in general: To tailor ads to  11 individual Net users, companies need information  12 about the user. How willing would you be for  13 companies to obtain such information in the  14 following ways?  15 First we asked about people supplying  16 their own information, and so we put the  17 question: By asking you to describe your  18 interests to them and you supplying whatever  19 information you wanted to have used for that  20 purpose. 56 percent of Net users said that they  21 would be willing to do this, representing 52  22 million users.  23 Then we asked the people who were not  24 willing if they would be willing: "If the  25 company providing tailored ads spelled out how</p>	<p style="text-align: right;">Page 109</p> <p>1 notice and opt-out, we get a total of 58 percent  2 that said that they would be willing to have  3 their web site visits collected.  4 Third, we asked about allowing  5 information about purchases on the Internet to be  6 used to tailor banner ads. You can see that it  7 dropped to 38 percent willing. But then when you  8 add those who would be willing if there was  9 notice and opt-out, it brings it back up to 51  10 percent or 47 million Net users.  11 By asking you to allow information  12 about your purchases from catalogues and stores  13 not on the Internet to be used to tailor Internet  14 banner ads to you, for you; 41 percent willing  15 and, after providing notice and opt-out, brings  16 it up to 52 percent or 49 million net users.  17 The fifth test was by asking you to  18 allow information about your purchases from  19 catalogues and stores not on the Internet to be  20 combined with information about your purchases on  21 the Internet, to be used to tailor Internet  22 banner ads to you. 45 percent were initially  23 willing; with notice and opt-out, it brings it up  24 to 52 percent or 48 million Net users.  25 Finally, and what obviously is the</p>

<p style="text-align: right;">Page 110</p> <p>1 most integrative of all, we asked: "Many  2 companies on the Internet would like to combine  3 information about your purchases, your visits to  4 web sites, and the personal information you  5 furnish to them into a profile that they use to  6 present banner ads reflecting your interests as  7 you use the Internet."  8       44 percent said this was initially  9 acceptable; and then when you add those with  10 notice and opt-out, it comes to 53 percent.  11       So when you draw back and look at all  12 6 of the examples that we tested, you see that a  13 majority of Net users, ranging from a low of 51  14 percent to a high of 68 percent, feel  15 comfortable, say that they would be comfortable,  16 in supplying or having their data used to tailor  17 banner ads to their interests, and it's the  18 provision of notice and opt-out that increases  19 acceptability by approximately 10, 15 percent  20 depending on the particular issue.  21       The survey is also very clear in  22 indicating that a solid minority of Net users,  23 ranging from 32 to 49 percent, would not be  24 willing to give or to have their personal  25 information collected for various types of banner</p>	<p style="text-align: right;">Page 112</p> <p>1       So we tested three central policies,  2 indicating that: "These are policies that could  3 be adopted by companies that were collecting  4 online and offline profile information in order  5 to present tailored ads. How important would  6 each of these policies be if you were to  7 participate in tailored ad profiles?"  8       (Slide.)  9       First we said: "The information  10 given by users or collected from their actions on  11 the Internet would be used only for presenting  12 tailored ads and other communications to them and  13 users would always be able to opt out of  14 communications they did not want to receive."  15 Not surprisingly, 71 percent rated that as  16 important and 51 percent chose "absolutely vital  17 or very important."  18       Second: "A user's interest  19 information would be used only by the banner ad  20 company and would not be sold or given to other  21 companies." This rose to 79 percent rated as  22 important and two-thirds, 66 percent, said it was  23 either absolutely vital or very important.  24       Finally, we said: "A user  25 participating in a tailored banner ad program</p>
<p style="text-align: right;">Page 111</p> <p>1 ad personalization.  2       In my judgment this is quite  3 consistent with all of the other survey research  4 that I summarized at the beginning.  5 Approximately one-third to one-half of Net users  6 are privacy fundamentalists, and the more you  7 combine data sources from different activities on  8 the Internet the higher their sense that their  9 privacy would be invaded and the more they would  10 want to have a privacy veto on any such  11 collection and use.  12       On the other hand, when you put  13 together the privacy unconcerned and the privacy  14 pragmatists you get between 51 and 68 percent  15 saying that they're willing, especially with  16 notice and opt-out, to have various sources of  17 information used for tailoring banner ads.  18       We didn't feel that it was  19 appropriate just to leave it there with a broad  20 statement about notice and opt-out, but rather to  21 test some of the key fair information practices  22 concepts that have always been at the heart of  23 the way in which the consumer privacy  24 relationship has been dealt with in the United  25 States.</p>	<p style="text-align: right;">Page 113</p> <p>1 could ask to see his or her profile and remove  2 any items that the user did not want in the  3 profile." This drew the highest importance  4 rating, 83 percent, and 70 percent calling this  5 absolutely vital or very important.  6       (Slide.)  7       I draw the following conclusions from  8 my results and from my thinking about how this  9 fits into the larger picture of consumer privacy  10 dynamics that I've sketched. First of all, we  11 have a clear division of the Net user population  12 into a majority that says it would be comfortable  13 with banner ads tailored and personalized in this  14 way and a strong minority that is clearly  15 opposed.  16       Secondly, the scope of the  17 information combination and integration is a key  18 factor in how many people will be comfortable and  19 how many people would walk away from a particular  20 combination.  21       Third, the privacy policies or fair  22 information practices we tested drew overwhelming  23 support from Net respondents: limited use with  24 opt-out, no sharing beyond the provision of  25 tailored ads of communications, and user access</p>

<p style="text-align: right;">Page 114</p> <p>1 to and control of the profile.  2 My fourth conclusion relates back to  3 what I presented as the new privacy-asserting  4 behavior by consumers off and online. It seems  5 to me clear from our data that Net advertisers  6 who want to get personal information must embrace  7 the privacy or fair information practices  8 policies that I describe or they're going to face  9 a consumer privacy veto.  10 I see no signs that there are passive  11 consumers on the net, slaves to whoever wants to  12 bounce something at them, incompetent to decide  13 whether to surf or not. I think the data about  14 privacy-asserting actions cuts two ways. It  15 tells net advertisers that's the price of  16 admission for this new relationship with the  17 consumer and, secondly, that consumers in fact,  18 through a lot of media and privacy advocacy and  19 business activity, are in fact paying significant  20 attention to this issue and will not be supine or  21 lifeless when it comes to it.  22 Finally, I would think that Net  23 industry associations need to adopt these  24 policies and to work on them, that privacy  25 advocates do an excellent job if they expose non-</p>	<p style="text-align: right;">Page 116</p> <p>1 there was no position of neutrality. Do you  2 think that affected the results of your survey?  3 DR. WESTIN: Let me say right away,  4 I'm not a survey methodology expert. I've done a  5 lot of surveys, but I'm not the statistical  6 expert.  7 My understanding is that you can use  8 a five-point response in which you have a middle  9 or neutral answer and that gives you one kind of  10 spread. Or if you choose four points, two  11 positive and two negative, you have a tendency to  12 push people a little bit to commit themselves.  13 My sense over the years is that by  14 using the four-point -- agree completely, agree  15 somewhat, disagree somewhat, disagree completely -- you  16 give people a range that they  17 can locate themselves on. In every question,  18 don't know and no response is always recorded, so  19 if somebody says "I don't know" they're put into  20 the don't know or no response.  21 So I'm really not myself able to say  22 that the five-point scale with the neutral is  23 preeminently better than the four-point. I just  24 note that both Harris and ORC in the work I've  25 done with them use that as the response</p>
<p style="text-align: right;">Page 115</p> <p>1 adopters or deviations from promises or  2 misleading privacy policies, and that I continue  3 to applaud the role of the Federal Trade  4 Commission to hold privacy workshops such as this  5 to oversee the issue, support these processes,  6 and always to be ready, if there is not a  7 significant adherence to these by the  8 overwhelming majority in the Net advertiser and  9 Net business community to recommend, if  10 necessary, regulations to see that that is  11 followed.  12 Thank you very much.  13 (Applause.)  14 MR. MEDINE: Thank you, Dr. Westin.  15 Dr. Westin actually has his own  16 conference going on right now on privacy, but he  17 has graciously agreed to stay for a few more  18 minutes to answer some questions. So you stay up  19 here and I'll pose some questions to you.  20 Is this working? Hello, hello? No.  21 One question from the audience is:  22 Do you think the absence of a neutral position  23 affected the results of your survey? Neutral  24 position, that is your survey called for people  25 to express positive, very positive, somewhat, but</p>	<p style="text-align: right;">Page 117</p> <p>1 categories.  2 MR. MEDINE: What are the  3 demographics of your Net user sample? How were  4 they selected? How were they polled?  5 DR. WESTIN: This was a  6 representative national sample, as I indicated.  7 A thousand respondents were questioned by  8 telephone using the automated call system that  9 most of the major survey firms use today, and  10 people were asked: "Do you use the Internet, I  11 think it read, "once a week or more?" If people  12 said yes, then they were in the sample, which  13 gave us a randomized, nationally representative  14 sample of 474 respondents.  15 In the material that has been passed  16 out, you'll find a box that describes for that  17 sample gender, race, age, education, etcetera.  18 So if you want to see what the components of the  19 sample were, you'll find them there.  20 But I think it's an accurate  21 statement to say that this is a representative  22 sample of the people who say that they are using  23 the Internet in a larger, nationally  24 representative sample of American adults 18 years  25 of age and older.</p>

<p style="text-align: right;">Page 118</p> <p>1 MR. MEDINE: Your survey results did  2 not ask the question, how would consumers feel  3 about providing this information assuming there  4 was no notice and out-opt. Can you essentially  5 take the converse of the percentages and say,  6 since 75 to 85 percent were comfortable were  7 comfortable with notice and opt-out, that only 15  8 to 25 percent would be comfortable without notice  9 and opt-out?  10 DR. WESTIN: I don't think you can  11 say that, because we first asked it without  12 notice and opt-out. We said how willing would  13 you be to, for example, number one, give your  14 personal information that you wanted to see used  15 for personalizing banner ads?  16 We didn't say with or without notice  17 or opt-out. But for the people who said they  18 would be willing, obviously in their mind I think  19 there was not a requirement that they would have  20 had to have heard notice and opt-out in order to  21 participate.  22 Then by asking those who said they  23 weren't initially willing whether notice and opt-out  24 would lead them to participate, I think we  25 picked up the people who had that in their mind</p>	<p style="text-align: right;">Page 120</p> <p>1 particular collection of information for this  2 benefit acceptable to you, you'll get the numbers  3 that we did at the front end, and then putting  4 the notice and opt-out brings them up.  5 But I wouldn't for a minute quarrel  6 with anybody -- my data produce it all the time -- that  7 notice and opt-out is perceived as the  8 bargain on the part of consumers if they're going  9 to be comfortable in giving their personal  10 information for marketing and for other kinds of  11 consumer purposes.  12 MR. MEDINE: Are there surveys of a  13 like nature being conducted in Europe? If so, by  14 whom? Are their findings similar?  15 DR. WESTIN: I'm happy to tell you  16 that if you go to the IBM web site -- I don't  17 happen to have the citation at the moment -- we  18 did a national survey with identical questions  19 testing American consumers, U.K. consumers, and  20 German consumers. And you'll find there some  21 fascinating material, because you'll find, first  22 of all, that American consumers are by very large  23 differences -- 20, 30, 40 percentage points -  24 more privacy-asserting today than individual  25 consumers in the U.K. and in Germany.</p>
<p style="text-align: right;">Page 119</p> <p>1 when they said they would not otherwise  2 participate.  3 MR. MEDINE: I guess the follow-up  4 here is that, along the same lines, the first  5 group you didn't tell one way or the other  6 whether there was an opt-out.  7 DR. WESTIN: That's correct.  8 MR. MEDINE: Did you consider telling  9 that group, by the way, would it make a  10 difference to you if there were no notice and  11 opt-out, essentially to highlight the privacy  12 consequences that you did for the second group?  13 DR. WESTIN: It's an interesting  14 point. I guess my experience in other surveys  15 that I have done is that if you ask the question,  16 how important is it to you that there be notice  17 and opt-out before you give your personal  18 information for this or that purpose, we always  19 draw 70, 80 percent that say that's important.  20 So you have sort of two results to  21 put together. As a matter of general outlook,  22 it's absolutely clear that three out of four or  23 more of Americans, when asked how important  24 notice and opt-out is, will say it's important.  25 But if you try it the other way and say, is a</p>	<p style="text-align: right;">Page 121</p> <p>1 Area by area, if you're interested in  2 attitudes toward getting information, concern  3 about Internet privacy, what U.K., German, and  4 U.S. consumers are doing at financial service web  5 sites, health web sites, retail web sites, and  6 insurance web sites, our data show how the  7 activities of consumers in all three countries  8 compare with one another. So we now have some  9 very good data with identical questions in three  10 different countries comparing consumer behavior,  11 attitudes, experiences, and so on.  12 MR. MEDINE: That's it. Thank you  13 very much again for being with us today.  14 DR. WESTIN: Thanks very much.  15 (Applause.)  16 MR. MEDINE: If those on the second  17 panel could please come up. Thank you.  18 (Pause.)  19 <b>SESSION II. IMPLICATIONS OF ONLINE PROFILING  20 TECHNOLOGY FOR USER PRIVACY</b>  21 MR. MEDINE: Can people hear me?  22 Yes? Okay.  23 Thank you for joining us for our  24 second panel, in which we're going to explore the  25 benefits to consumers and to business of the</p>

<p style="text-align: right;">Page 122</p> <p>1 technology we have been hearing about, as well as  2 the privacy and consumer concerns about the  3 technology as well.  4 I am pleased that we have a  5 distinguished panel, some of whom have been here  6 before and some of whom are newcomers to our  7 privacy workshop. Starting to my right, we have:  8 Bradley Aronson, who serves as the President of  9 i-frontier, which is an Internet advertising  10 agency focusing on achieving client goals. I-frontier's  11 objective is building brands,  12 generating leads, selling products, and  13 increasing page views to measure success.  14 Next to him is Fred Cate, who's a  15 Professor of Law and Director, Information Law  16 and Commerce Institute at the Indiana University  17 School of Law at Bloomington. I guess I should  18 disclose that I was formerly a professor at that  19 same institution. He's also a senior counsel  20 for information law at the Indianapolis law firm  21 of Isemiller, DiNadio, and Ryan, specializing in  22 information and privacy law.  23 Next is Jason Catlett, who was on our  24 prior panel, who's already been introduced.  25 Jeff Chester, who we can thank for</p>	<p style="text-align: right;">Page 124</p> <p>1 which currently delivers ads based on location or  2 context to suit the advertiser's needs.  3 Jonathan Shapiro, to her left, is the  4 Senior Vice President of Business Development at  5 DoubleClick, Inc. DoubleClick is a global  6 Internet advertising solutions company  7 specializing in developing the solutions which  8 make advertising work on the Internet for web  9 publishers and web advertisers.  10 Solveig Singleton is a  11 telecommunications lawyer and the Director of  12 Information Studies at the Cato Institute, a  13 public policy research foundation.  14 Robert Ellis Smith is a journalist  15 who uses his training as an attorney to report on  16 the individual's right to privacy. Since 1974 he  17 has published "Privacy Journal," a monthly  18 newsletter on privacy in the computer age.  19 Lastly, Shari Steele is an attorney  20 with the Electronic Frontier Foundation. She  21 works primarily on civil liberties issues for  22 people communicating online and on issues  23 involving access to government information.  24 I want to start off with Solveig  25 Singleton and ask the question: We've heard a</p>
<p style="text-align: right;">Page 123</p> <p>1 the refreshments during the break, in addition to  2 being the Executive Director of the Center for  3 Media Education, one of the country's leading  4 consumer organizations working on electronic  5 media issues affecting children and youth.  6 Austin Hill serves as President of  7 Zero-Knowledge Systems, an Internet privacy firm  8 that develops end user-controlled privacy  9 solutions to enhance the privacy of Internet  10 users.  11 Deirdre Mulligan is Staff Counsel at  12 the Center for Democracy and Technology. One of  13 CDT's concerns involves the privacy issues  14 surrounding the deployment of the Intel Pentium  15 III processor serial number.  16 Dan Jaffe serves as Executive Vice  17 President of the Association of National  18 Advertisers and is dedicated to serving the  19 interests of companies that market regionally and  20 nationally, many of whom engage in electronic  21 commerce.  22 To my left is Megan Hurley. She  23 serves as Associate General Counsel at 24/7 Media  24 and oversees database development issues. 24/7  25 is a third party ad network and e-mail marketer</p>	<p style="text-align: right;">Page 125</p> <p>1 lot about how marketing is done online. How does  2 that differ from the old world model of a  3 shopkeeper keeping an eye on the shopkeeper's  4 customers and inviting them to take advantage of  5 new products or services that the shopkeeper  6 knows from prior experience they might be  7 interested in?  8 MS. SINGLETON: I think it's  9 generally very similar. Of course, the  10 shopkeeper example is more familiar. One analogy  11 that one might make is if you view the Internet  12 as a sort of mall, the shopkeeper, if he does not  13 collect some kind of information from people as  14 they visit his site, is essentially in the  15 position of a shopkeeper who is standing in his  16 store and he's blindfolded and he's got earmuffs  17 on, so as people come into his store he can't  18 look at them and say, oh, you know, that's a  19 young teenager, maybe they're a shoplifting risk,  20 or it seems to me that there are mostly older  21 people coming into my store, and so on and so  22 forth.  23 So from the standpoint of electronic  24 commerce, then, in order for a merchant to have  25 kind of a general familiarity with who is</p>



<p style="text-align: right;">Page 126</p> <p>1 visiting him and where they're going, it's  2 natural that he would want to seek out some kind  3 of information and collect it.  4       Once that information is collected -- and  5 here's a difference -- he'd have  6 additional opportunities to use that information  7 because, it's actually preserved in electronic  8 form, to develop new products or to move things  9 around or to improve security and so on.  10       MR. MEDINE: Jeff.  11       MR. CHESTER: I'd like to respond  12 because I think it's entirely different. The  13 Center for Media Education has been tracking  14 online advertising and online profiling since  15 1996, when we handed the FTC our report "Web of  16 Deception," which led to the Children's Online  17 Privacy Protection Act. Indeed, microtargeting  18 of children was our early concern.  19       But I want to underscore from our  20 observations at the Center that online profiling  21 threatens the privacy of all Americans, and we're  22 especially concerned about children and teens.  23 An unprecedented technological apparatus has been  24 put into place over the last few years to track  25 and identify behaviors, values, psychological</p>	<p style="text-align: right;">Page 128</p> <p>1 interests, and strategies behind that information  2 to get you to buy over a long period of time.  3 The consumer in this country has no idea and they  4 would have responded to Dr. Westin's study in a  5 totally different way if they knew that in fact  6 we are creating a psychological profile of you:  7 We want to know your vulnerabilities and your  8 interests.  9       So we think that this is a very  10 critical issue here that the Federal Trade  11 Commission must grapple with now.  12       MS. BURR: Shari.  13       MS. STEELE: I don't think the  14 analogy of the shopkeeper really works. It would  15 be a shopkeeper who is watching you as you were  16 browsing through their store. They're following  17 you down the aisles, peering at everything you  18 pick up and look at.  19       It's also the shopkeeper who, you've  20 walked in and you've got stamped on your forehead  21 all of the purchases that you've made the  22 previous stores that you've gone to. It's also  23 the shopkeeper that you might choose to pay cash  24 because you don't want information about what  25 you've just purchased kept somewhere by someone,</p>
<p style="text-align: right;">Page 127</p> <p>1 characteristics of individuals. This information  2 is being collected online. It's being added to  3 offline material.  4       I know that we have a big panel, but  5 I'll just give you an example of one of the many  6 ads that appear in all of the ad trade journals.  7 This happens to be in the current issue of Red  8 Herring. There's a guy on a motorcycle, a  9 motorcycle helmet -- I'm sorry you can't see it -- and  10 the big copy says: "Has a nose for rare  11 bordeaux, calls mom every weekend, grows award-winning  12 roses. His name is Axel."  13       This is from the Navient Company:  14 "New precision web targeting from Navient  15 combines physical world data with online behavior  16 for the very first time, so you can deliver  17 customized banner ads without the waste of  18 scattershot messaging. With the acquiring of  19 IQ2Net, we're taking data integrity to a level  20 that's never been reached before, that includes  21 name, address, demographics, psychographics, and  22 click stream behavior."  23       I want to finish by underscoring, the  24 psychographic scales, the technology that relates  25 to identifying you as an individual, your</p>	<p style="text-align: right;">Page 129</p> <p>1 personal kinds of purchases.  2       And that information, you're not  3 being given a choice as to whether or not that's  4 collected about you or whether or not advertising  5 is being directed at you based on those  6 purchases.  7       So I just think that, while there are  8 a couple of really basic similarities to a  9 shopkeeper, it's really so much more intrusive  10 with online communications because of the  11 magnitude of information that's being collected  12 and the amount of information that's being shared  13 among shopkeepers.  14       MR. MEDINE: Deirdre.  15       MS. MULLIGAN: I wanted to build on  16 some of what Shari just said, that I think,  17 unlike an online service provider or a web site,  18 where an individual actually has some role in  19 initiating the relationship, I think one of the  20 most troubling aspects of the advertising  21 networks that we're discussing today is that they  22 don't directly serve consumers. Consumers are  23 unaware of their existence. They have no  24 knowledge that someone else is reaching through  25 your shopkeeper's store and extracting data about</p>

<p style="text-align: right;">Page 130</p> <p>1 them.</p> <p>2           They certainly are not aware that</p> <p>3 this data is being used to build an ongoing</p> <p>4 profile of their likes, their dislikes, their</p> <p>5 preferences, and any other kind of inferences</p> <p>6 that might be developed, and that that</p> <p>7 information, while it may not be attached to</p> <p>8 their name and address, is uniquely attached to</p> <p>9 them and will follow them around like a little</p> <p>10 thread as they navigate the web, dictating the</p> <p>11 experiences that they have at other web sites.</p> <p>12           Now, we can disagree as to whether or</p> <p>13 not it's a benefit to consumers to have</p> <p>14 information tailored or not. But I don't think</p> <p>15 anyone here would disagree that individuals</p> <p>16 should have knowledge and that their consent</p> <p>17 should be given when we're talking about a</p> <p>18 secondary use of data, that no consumer is</p> <p>19 visiting a web site in order to enable ad</p> <p>20 serving. This is all about a secondary use.</p> <p>21           MR. MEDINE: Austin.</p> <p>22           MR. HILL: A couple points. One of</p> <p>23 the analogies that I think Shari has kind of</p> <p>24 touched on breaking down is the Internet as a</p> <p>25 mall. I think it further breaks down when you</p>	<p style="text-align: right;">Page 132</p> <p>1 about is all of the unintended consequences and</p> <p>2 all of the ways this data can be used. One of</p> <p>3 the things I also think we need to address is the</p> <p>4 use of cookies and the use of profiling is just</p> <p>5 milliseconds into the Internet age. We're just</p> <p>6 starting to realize how some of these techniques</p> <p>7 can be used.</p> <p>8           Already we're seeing a growth in</p> <p>9 super-profile managers, so-called identity</p> <p>10 managers like Microsoft Passport that is taking</p> <p>11 the entire Hotmail base and saying: Your Hotmail</p> <p>12 identity is now going to create a master profile</p> <p>13 that will be shared and be one-click login for</p> <p>14 every one of your sites. So instead of having</p> <p>15 individual profiles, we'll now give you one</p> <p>16 profile that's good for everywhere.</p> <p>17           This is something that everyone's</p> <p>18 really driving towards, is the so-called identity</p> <p>19 managers who are going to build better profiles</p> <p>20 because they watch you everywhere, not just on a</p> <p>21 number of sites. So I think we really need to</p> <p>22 question all of these techniques as we go forward</p> <p>23 and rationalize them with every single one of the</p> <p>24 uses that we use on Internet, not just solely</p> <p>25 will this person buy something because they saw</p>
<p style="text-align: right;">Page 131</p> <p>1 actually think about what goes on on the</p> <p>2 Internet. The whole birth of e-commerce, the</p> <p>3 whole birth of malls, and the incredible</p> <p>4 valuations that we're seeing in the Internet age</p> <p>5 is a recently new phenomenon.</p> <p>6           This is a communication medium. This</p> <p>7 is the same medium that we're being asked to put</p> <p>8 our medical records on. This is the same medium</p> <p>9 that people are reaching out to talk about</p> <p>10 support groups, get advice about cancer. Every</p> <p>11 single aspect of our lives is being pushed onto</p> <p>12 this online form.</p> <p>13           So it's not just a mall where</p> <p>14 shopping goes on. The same profiling and the</p> <p>15 same techniques are being used to help an</p> <p>16 insurance provider make a decision on whether or</p> <p>17 not someone's a viable prospect for insurance.</p> <p>18 Did they visit a risky web site? Did they go to</p> <p>19 a web site that was unpopular?</p> <p>20           An employer who's doing a background</p> <p>21 search can now go into Dejanews and look at</p> <p>22 someone's opinions, religious beliefs,</p> <p>23 discussions that went on eight years ago that are</p> <p>24 archived in there forever.</p> <p>25           So one of the things we need to think</p>	<p style="text-align: right;">Page 133</p> <p>1 our ad.</p> <p>2           MR. MEDINE: Just to briefly</p> <p>3 interrupt the discussion, if Clark Rector is</p> <p>4 here, please call your office as soon as</p> <p>5 possible.</p> <p>6           Jonathan.</p> <p>7           MR. SHAPIRO: The most important</p> <p>8 thing here is that the research that we've seen</p> <p>9 suggests that users, a majority of users,</p> <p>10 actually like the notion of having advertising</p> <p>11 and content personalized for them. Now, we</p> <p>12 recognize that the majority doesn't mean</p> <p>13 everyone. So what we want to do is provide users</p> <p>14 notice and choice, as Deirdre mentioned, so that</p> <p>15 the user gets to decide whether they're</p> <p>16 participating in this profiling.</p> <p>17           DoubleClick for the last two and a</p> <p>18 half years has provided users that choice. We've</p> <p>19 had a selective opt-out that allows you to opt</p> <p>20 out of the DoubleClick cookie and basically de-link, take</p> <p>21 away our technical ability to profile</p> <p>22 you.</p> <p>23           MS. MULLIGAN: Can I just respond?</p> <p>24 Actually, I agree with you that notice and</p> <p>25 consent are critical. But notice, when you talk</p>

Page 134

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

Page 135

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.

Page 136

1 Now, the industry, at least the  
 2 members that I represent, the major national  
 3 advertisers, see very clearly that giving people  
 4 privacy protection is critical. We can see all  
 5 sorts of data that says that people are not going  
 6 on the Net in the numbers that they would or  
 7 using the Net as they would because of privacy  
 8 concerns.  
 9 So up until this workshop we've been  
 10 discussing getting web pages to put their privacy  
 11 policies out, and now we're going on to the next  
 12 stage, which is that there are some people who  
 13 are, by the way, working for these people who  
 14 have already stated that privacy is a very great  
 15 concern, my members, to get these people to be  
 16 visible, to make it transparent.  
 17 I understand that in the third panel  
 18 we're going to hear a great deal of commitment to  
 19 this point. It's very clear now that unless the  
 20 industry self-regulates there will be regulation.  
 21 I believe that, even if there is regulation, that  
 22 the Net will never really be fully protected  
 23 unless there is self-regulation.  
 24 There is just no way that any  
 25 government or all governments trying to track

Page 137

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

<p style="text-align: right;">Page 138</p> <p>1 vests. They want to know something that will  2 allow them to provide ads to people so that they  3 can make choices that are more likely to be  4 meaningful to them and therefore create an  5 economic benefit both to the consumer and for  6 business.  7 MR. MEDINE: It would be helpful on  8 the comments on profiling, where is value added  9 at networks and web sites, as well as the  10 benefits to consumers. Then I'll turn to Megan  11 to address what you wanted and possibly that as  12 well.  13 MS. HURLEY: Before getting to the  14 benefits, I just wanted to address the  15 transparency issue of the ad networks. We  16 realize that consumers don't know who we are and  17 that we have to get to them. Consumers are our  18 business. If they're unhappy, we're not going to  19 have happy advertisers and we're out of business.  20 So some of the ad networks, like  21 24/7, require all of the web sites that are in  22 our network to post a privacy policy that is in  23 adherence with the highest industry standards,  24 such as TRUSTe or DMA. So that is one way, not  25 the only way, that is one way that the ad</p>	<p style="text-align: right;">Page 140</p> <p>1 networks to describe what they do: predictive  2 databases, targeting algorithms, flow states. Recently  3 one of the heads of Excite talked about  4 neural imputation.  5 Clearly there are other motives here,  6 in some sense to direct consumer choice without  7 consumers fully understanding why. Those choices  8 are linked in fact to editorial content also made  9 available, which raises other public interest  10 issues.  11 But it's not just about giving people  12 what they want. It's about steering them and  13 having long-term strategies to steer them, and  14 none of this is understood by the consumer and  15 the citizen. I do think it has implications far  16 beyond advertising and marketing, including for  17 political speech. But it's very important we  18 deal with this issue now, early on, to develop  19 the safeguards.  20 MR. MEDINE: Jason, Bradley, Fred,  21 and Deirdre.  22 MR. CATLETT: Thanks, David.  23 I'd like to give people some specific  24 cases of URL's that they can go to to see this  25 technology and this kind of proposal in action.</p>
<p style="text-align: right;">Page 139</p> <p>1 networks recognize this problem and that we're  2 addressing it. You'll hear much more on panel  3 three, when the advertisers talk about the new  4 initiative that they're putting in.  5 But the benefits economically to the  6 web sites and to the advertisers and to the  7 consumers are obvious. You see from the various  8 studies that consumers want to see ads that are  9 targeted to them. Their fear is of the unknown,  10 how is this information used? So I think our  11 struggle here is to start with reaching consumers  12 and educating them to the fullest.  13 So I think that, before we talk about  14 benefits, is a key issue.  15 MR. CHESTER: David, I'd like to just  16 -- I'm glad to hear that the industry will  17 address it and I know you're saying it sincerely.  18 But I think we have to look beyond the notion  19 that this is really about giving consumers what  20 they want or choice.  21 I suggest that we have to look behind  22 the technology and see if there are other  23 motivations and really have a debate about the  24 proper use. Let me just share with you some of  25 the phrases used with the online ad targeting</p>	<p style="text-align: right;">Page 141</p> <p>1 The first one is Netdeals.com, which is related  2 to DoubleClick. It's a sweepstakes where you  3 enter your name for a contest, and there's a  4 privacy policy down at the bottom that says that  5 the company will protect your privacy, and you  6 actually have to scrawl down to see some of the  7 details there that they are going to link that.  8 So that is a first point of call.  9 The second one is a popular finance  10 site called Quicken.com, and there are ads on  11 this served actually, I believe, by MatchLogic.  12 There are also these web bugs, as Richard Smith  13 calls them, or pixels, clear GIF's, transparent  14 GIF's -- they have a number of names -- which  15 basically tells the advertising network that you  16 are going to that page.  17 This can be tremendously valuable to  18 the advertising network. For example, the  19 Quicken site has areas on mortgages, on  20 insurance, and finance, and it's very valuable  21 for the advertisers to know what you're shopping  22 around for. But it's also highly intrusive.  23 Let me give you a final URL, which  24 has a poetic irony to it. It's  25 Mentalwellness.com/mask, Mentalwellness.com/mask.</p>

<p style="text-align: right;">Page 142</p> <p>1 Now, if you go to this page you will read a  2 touching story of people who in history, great  3 figures, have overcome mental illness and gone on  4 to greatness.  5       What is not -- there are no ads on  6 this page and it's not clear to anybody who  7 doesn't know to view source and look at the URL  8 to see that there is one of these web bugs  9 pointing, telling the advertiser when you are  10 visiting this page, and I find that very  11 offensive.  12       MR. MEDINE: Bradley.  13       MR. ARONSON: I wanted to address a  14 few issues. The first is Austin had brought up  15 how it's kind of we're only milliseconds into  16 what's going on, and that's really important  17 because no one really knows what's next. The  18 risk of coming up with some sort of set  19 regulations is that we could be stunting the  20 growth of something we don't know.  21       To address the economic issues, most  22 of the web sites out there are supported by  23 advertising. That's why the content is free.  24 And advertisers need to see results and targeting  25 delivers results.</p>	<p style="text-align: right;">Page 144</p> <p>1 networks to track what's going on. It's for the  2 advertiser to track whether or not they're having  3 success. For example, on a lot of our sites we  4 run different ads. We need a way to track after  5 someone clicks on the ad, what do they do on the  6 site, because it's not really -- we can't say we  7 had a successful ad campaign if someone clicks on  8 the ad and just comes to the web site. I want to  9 know did they go to the right section of the web  10 site and which ads drove the people who delivered  11 orders or leads.  12       MR. MEDINE: Fred.  13       MR. CATE: Thanks, David.  14       I just want to turn, I guess, to the  15 question asked right at the outset, which is the  16 question of harms and benefits, because, to be  17 perfectly frank, I'm confused and this may come  18 more in the guise of a question than a statement.  19 In terms of harms, what we heard about so far  20 this morning is non-personally identifiable  21 information, is collections of information that  22 may be linked to an IP address or a cookie, but  23 not linked to a person. And this is certainly  24 one of the first times that I've heard an  25 extensive privacy discussion about information</p>
<p style="text-align: right;">Page 143</p> <p>1       Consumers should definitely have  2 notice. They should definitely have choice. But  3 we need to be able to target, because if it's not  4 effective how are web site publishers going to  5 support what they're doing? It's going to be  6 kind of difficult.  7       I think advertisers will support  8 self-regulation. Look at the bigger picture.  9 For most advertisers the Net is a very, very  10 small portion of their budget and they're not  11 going to try to upset consumers by violating  12 their privacy through doing things that are  13 outrageous on the Internet. In fact, a lot of  14 the large advertisers say, we're only going to  15 advertise on sites that have clear privacy  16 policies.  17       By coming up with a set of guidelines  18 and saying, hey, here's what self-regulation,  19 what we're going to do to make it safe for  20 consumers, I think advertisers can really, with  21 consumers, make that vote and say, hey, we're  22 only going to advertise on the sites that do  23 this.  24       Then to also address the clear GIF's  25 on the pages, those aren't usually for ad</p>	<p style="text-align: right;">Page 145</p> <p>1 that isn't linked to an individual, that isn't  2 the privacy of an individual, but is rather the  3 privacy of a machine or an IP address at issue.  4       I'm concerned. What is the nature of  5 this harm? Now, in reading the comments filed  6 before this proceeding, without exception they  7 talked about the harm of being marketed to, the  8 harm that somebody might actually advertise  9 things to you that you would want. I'm again  10 concerned about the nature of this harm.  11       If it is a fraudulent or deceptive  12 trade practice, you've already got jurisdiction,  13 I assume. If we are talking about marketing in  14 terms of sending people the types of ads or type  15 of information, type of opportunities that  16 they're interested in, again it's unclear to me  17 what the privacy, what the privacy harm is.  18       On the benefits side, although you  19 asked earlier about the economics within the  20 industry, something which I'm not in a position  21 to comment on, but the benefits as a user, as a  22 consumer, would seem to be not paying for a great  23 deal of that content that we access on the web.  24       I thought earlier during the panel  25 this morning of Encyclopedia Britannica. When it</p>

<p style="text-align: right;">Page 146</p> <p>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</p>	<p style="text-align: right;">Page 148</p> <p>1 well has been described as an invasion of privacy  2 as a tort matter by the U.S. Supreme Court. In  3 1995 they said that target marketing aimed at a  4 vulnerable population is an invasion of privacy.  5 And that's, even though we haven't used the word  6 yet, on two points this is an invasion of  7 privacy.  8 I'd like to give you a scenario of  9 about 20 years ago, when movie theater owners  10 discovered that they could flash up instantaneous  11 messages on the screen for just a portion of a  12 second and get people to buy products, whether it  13 said "You're thirsty" or "You like popcorn."  14 They could do that immediately on the screen.  15 That involved no collection of  16 personal identifying information at all. Is it  17 an invasion of privacy? Of course it is. It's a  18 diminution of our autonomy. It's commercial  19 manipulation in an unfair way, simply because the  20 individual in the theater doesn't have the same  21 resources to respond in a meaningful way.  22 The Federal Trade Commission, by the  23 way, acted immediately to say that that sort of  24 technology ought to be suspended until we knew  25 more about it. It then gravitated towards</p>
<p style="text-align: right;">Page 147</p> <p>1 consumers and require their consent?  2 I don't know, Robert, if you want to  3 speak to that or other issues.  4 MR. ROBERT SMITH: Well, I think Fred  5 Cate might well be confused because we have not  6 in a session on privacy even talked about  7 privacy. In order to know whether something like  8 this violates privacy, we should define privacy  9 and know what it is.  10 Privacy is not just the keeping of  11 secrets. The concern about privacy goes far  12 beyond breaches of confidentiality. Even if no  13 individually identifiable information is kept in  14 a marketing scheme like this, it would violate  15 privacy.  16 What Jeff Chester describes is a  17 scenario that violates privacy in two aspects.  18 One, the right to privacy includes the right of  19 personal autonomy. To the extent that I am  20 manipulated in the marketplace, especially  21 without my knowledge and especially if I'm a  22 vulnerable individual, it is a violation or a  23 diminution of my autonomy and therefore a  24 violation of privacy.  25 The scenario that he described as</p>	<p style="text-align: right;">Page 149</p> <p>1 television and the Federal Trade Commission said  2 right away, without any mantra of self-regulation,  3 without any forums, without any  4 workshops, they said: No, this can't be done;  5 this is deceptive on its face.  6 So I would say when you combine the  7 case law that I've just described, you'd make a  8 case for a class action, I think, to show that  9 this kind of manipulative technology, especially  10 on vulnerable populations, is an invasion of  11 privacy, and I would suspect that that's the way  12 regulation will go, that it will be a privacy  13 sector class action that will put an end to this.  14 MR. MEDINE: Deirdre.  15 MS. MULLIGAN: I want to, at least in  16 part, respond to Fred's question, which is a very  17 important question. It's what data are we  18 talking about? Is this data truly aggregate  19 data? Is it non-identifiable data? Is it, as I  20 would argue, data that is uniquely attached to a  21 specific individual and used to make decisions  22 about them and therefore has privacy  23 implications, regardless of the fact that you may  24 not know their name?  25 Or is it fully identifiable</p>

<p style="text-align: right;">Page 150</p> <p>1 information, which I believe at least some of the  2 services, the companies that are engaged in these  3 services, are moving to making this information  4 that is identifiable with an individual in both  5 their online capacity through a unique identifier  6 and their offline capacity?  7 Now, I have a question that I think  8 might help illustrate this. Have any of -- I  9 guess we have Bradley, Austin, Michael -- no,  10 Megan, and Jonathan -- have any of you been  11 served with either a civil or a criminal subpoena  12 for access to information contained in your  13 databases? And if you were, would you be able  14 to, either retrospectively or prospectively,  15 attach the profiles that you have to an  16 individual? And if yes, what would it entail?  17 MR. MEDINE: Jonathan.  18 MR. SHAPIRO: Let me address that.  19 We have not been served a subpoena, and if we  20 were we would not today be able to attach any of  21 the information we have to a unique individual.  22 But let's be clear. The ad networks  23 are not the best source if someone wants -- if a  24 legal agent wants to get information on someone.  25 The ISP has a view of everything that the ISP's</p>	<p style="text-align: right;">Page 152</p> <p>1 you register, so your name and your address and  2 your e-mail address.  3 We are going to link that information  4 to both online information and offline  5 information, and then we're going to use that  6 information. Now, what are we going to use that  7 information for, because it gets to some of the  8 other questions earlier and Fred's comments on  9 harm. We are going to use that information to  10 target advertising to you. That's it. We're  11 going to send you marketing messages.  12 We want to get -- DoubleClick and all  13 the ad networks are in the same business. We  14 serve advertisers. We want to help advertisers  15 get the right message to the right user at the  16 right time. We want to put information in front  17 of consumers that's relevant to them, and that's  18 what we're going to use all the information we're  19 collecting to do going forward.  20 Can I, just one more comment, David.  21 You know, to Robert's comment on this is personal  22 autonomy being a key component of privacy, we  23 agree. Again, Dr. Westin's research suggests  24 that Americans are very active about managing  25 their privacy. We are providing notice and</p>
<p style="text-align: right;">Page 151</p> <p>1 members do, and if someone wants a picture of  2 someone's transactions, you know, Visa and  3 American Express have a much more complete  4 picture than anything that any of the ad networks  5 would ever have.  6 MS. MULLIGAN: So you're saying  7 technically you cannot?  8 MR. SHAPIRO: Technically, today we  9 cannot associate the name and address or  10 personally identifiable information with the  11 profile that we have.  12 MS. MULLIGAN: No, an IP address or a  13 unique ID? If I --  14 MR. SHAPIRO: Well, let me clarify.  15 If someone's volunteered their information, if  16 someone has volunteered their name and address  17 somewhere on the web where we were, we could  18 technically at that point, we could give them  19 notice and choice and then we could associate it.  20 So for example, the Netdeals site  21 that Jason cited earlier -- by the way, I  22 encourage all of you to go and visit because you  23 can win a million dollars -- at that site we  24 clearly state that we are going to take  25 personally identifiable information from you when</p>	<p style="text-align: right;">Page 153</p> <p>1 choice, and that gives them the tool to exercise  2 their autonomy.  3 Moreover, we have made business  4 decisions where we think that, even though we can  5 aggregate certain information, it's inappropriate  6 for targeting. So a vulnerable population like  7 children, we will not gather or link information  8 on children's activities to a profile or ever use  9 that information for targeting purposes, because  10 we think that's inappropriate.  11 Detailed financial information we  12 think is inappropriate, and clearly health,  13 mental health or health-related information is  14 inappropriate. So there are classes of  15 information that we at DoubleClick, and I'm sure  16 the other ad networks would echo, are  17 inappropriate for targeting.  18 MR. MEDINE: Thanks.  19 Austin, then Jason.  20 MR. HILL: Just addressing two  21 points, one Fred's and then Bradley's point. One  22 of the comments was who was being harmed? We're  23 receiving advertising, advertising is an  24 acceptable form of reaching consumers in this  25 culture. One of the things I don't think has</p>





<p style="text-align: right;">Page 158</p> <p>1 better company, we're worth more to the public,  2 because we profile better, and that will lead to  3 better response rates.  4 It's not true. It is not true.  5 MR. ROBERT SMITH: David, can I ask a  6 quick question along that line?  7 MR. MEDINE: You're jumping on  8 Jason's time.  9 MR. ROBERT SMITH: I'm told it's an  10 open secret that the meters that are used on web  11 sites to show how many people visit a site can be  12 manipulated and altered as the site operator  13 wishes. Is that correct?  14 MR. HILL: Those actually, the  15 counters, the site counters, don't have a lot of  16 relevance when it comes to the ad tracking  17 networks because they don't base it solely on how  18 many times was this page loaded. They base it on  19 how many times did this person with this cookie  20 come back to this site.  21 So they can detect refresh rates,  22 they can detect if someone is just visiting for a  23 first time in a day. They have a lot more  24 valuable information because they do attach a  25 cookie to it, as opposed to solely how many times</p>	<p style="text-align: right;">Page 160</p> <p>1 that's the current way. Really, when you think  2 about it, the bank doesn't really want to take  3 the registrations, either. They think that  4 people are going to buy once they've registered.  5 So Wall Street has this perverse  6 incentive to give companies the motive to collect  7 absolutely excessive amounts of information and  8 to get it in ways that are really scrambling. So  9 the result of all this technology and money is a  10 single terrifying fact: If you give your name to  11 a single web site, then every other web site on  12 the Internet may know who you are the moment you  13 walk into their front door.  14 Now, once that message goes to  15 consumers around the country they will realize  16 that the Internet is a very unfriendly place and  17 e-commerce will be damaged far more than any  18 measure of limiting targeting could possibly do.  19 MR. MEDINE: Jonathan.  20 MR. SHAPIRO: Just because -- you  21 know, one of the things we've talked about here  22 today which we believe the ad networks I know all  23 share is very important is education. So it's  24 important that when we say things in a public  25 forum we say them accurately, and it's just not</p>
<p style="text-align: right;">Page 159</p> <p>1 was this site loaded.  2 MR. ROBERT SMITH: But they can be  3 reset with ease, isn't that correct?  4 MR. HILL: The site counters?  5 MR. ROBERT SMITH: Yes.  6 MR. HILL: The site counters can be  7 reset.  8 MR. ROBERT SMITH: So they're  9 deceptive inherently.  10 MR. HILL: Well, it depends how  11 they're being represented.  12 MR. MEDINE: Jason.  13 MR. CATLETT: Let me pick up on  14 Austin's comment about the economic effect, how  15 the flood of money from Wall Street is causing  16 these technologies to be developed. Wall Street  17 hasn't found a way to value Internet companies.  18 Their usual method of seeing how much money they  19 make doesn't work because they all lose money.  20 So they started looking at traffic, and the  21 trouble with traffic and measuring the number of  22 eyeballs that a site gets is the bank doesn't  23 take eyeballs.  24 So they dismissed that one, and now  25 sites say: Well, we've got registrations. So</p>	<p style="text-align: right;">Page 161</p> <p>1 accurate to say that once you've given your name  2 to one web site every other web site can know who  3 you are. That's just not accurate.  4 Dan Jaye described this morning,  5 cookies are domain-specific. They are only  6 associated with the domain that is putting the  7 cookie. So that means if you're at Amazon.com,  8 Amazon can place an Amazon cookie, but Amazon can  9 only read the Amazon cookie and they can only  10 place an Amazon cookie on you when you visit  11 Amazon. DoubleClick can only place a DoubleClick  12 cookie and we can only place it on a site that's  13 a member of our network.  14 MR. HILL: Sorry, Jonathan; that  15 includes AltaVista. So if I go to AltaVista, I'm  16 not going to DoubleClick, I'm not asking for  17 DoubleClick to send a cookie. I'm going to  18 AltaVista and I received, totally unbeknownst to  19 me, I never requested that, I never typed it into  20 my browser --  21 MR. SHAPIRO: Austin's right. When  22 you visit any member of the DoubleClick network,  23 DoubleClick will place a cookie on your browser.  24 And what we use that cookie for is to identify  25 that browser as a unique user. Today we do</p>

Page 162

1 things like we ask the question: Well, how many  
 2 times has this unique browser seen this  
 3 particular ad? We use it because we know that if  
 4 you've seen an ad three times and you haven't  
 5 responded, then it's unlikely that you're going  
 6 to respond in the future, so we will frequency  
 7 cap the delivery of that ad to you.  
 8       So yes, if you visit a site in the  
 9 DoubleClick network we will put a DoubleClick  
 10 cookie on your browser, that's absolutely true.  
 11 But only DoubleClick sites and sites that are  
 12 participating in the DoubleClick network through  
 13 us can know or recognize that cookie. So it's  
 14 not fair to say that if you've given your name to  
 15 DoubleClick through Netdeals, as an example, that  
 16 every other web site can know who you are.  
 17       MR. HILL: No, but it's also not  
 18 specific or accurate to say that only Amazon when  
 19 I visit Amazon can set or read a cookie, because  
 20 clearly if Amazon were to join the DoubleClick  
 21 network they now benefit from all.  
 22       MR. SHAPIRO: That's a great example.  
 23 That's a great example because even when, let's  
 24 say Amazon did join the DoubleClick network, even  
 25 if they were a member of the network, and I go to Amazon

Page 163

1 and I buy a book, my personally  
 2 identifiable information is not passed to  
 3 DoubleClick. It's not given to us.  
 4       So yes, there's a DoubleClick cookie  
 5 there, but it's not associated with the  
 6 personally identifiable information that was  
 7 given to Amazon. So it is, again, it's just not  
 8 accurate to say that once you've given your name  
 9 to somebody on the web that everyone has it.  
 10 It's just not accurate.  
 11       MR. HILL: Speaking to Jonathan's  
 12 point --  
 13       MR. MEDINE: Jason.  
 14       MR. CATLETT: I think I said that  
 15 anyone could technically do it. I didn't say  
 16 everyone can do it now. If you want to see the  
 17 details --  
 18       MR. SHAPIRO: Well, technically, you  
 19 know, the phone company could give everybody  
 20 everybody's name and address.  
 21       MR. CATLETT: And some people are  
 22 doing it, such as Navient.com.  
 23       MR. MEDINE: Dan has been waiting and  
 24 he yielded a moment of his time, but not all of  
 25 his time.

Page 164

1       MR. JAFFE: Thank you.  
 2       I think it's an interesting  
 3 discussion here, where people are trying to say  
 4 that they're going to decide how this should come  
 5 out economically, where I think really the  
 6 consumers should decide how it's going to come  
 7 out economically. If they don't want to click on  
 8 these ads, believe me, these ads are going to  
 9 disappear.  
 10       People are not just going to be  
 11 carrying on these practices for fun and for  
 12 economic waste. People are trying to use these  
 13 various means to sell products and to move the  
 14 economy forward. We are seeing all sorts of  
 15 companies that are taking on people who've been  
 16 around for a hundred years. Amazon.com is  
 17 clearly an example of that. One of the reasons  
 18 that people think that this can happen is that  
 19 they are going to be able to personalize, to have  
 20 one to one selling, to make selling more  
 21 relevant.  
 22       If that's not going to be the case,  
 23 by the way, I think that you're going to find the  
 24 Internet is going to not meet -- that all of  
 25 these great IPO's and others are going to be found to be

Page 165

1 much less effective.  
 2       I would like to finish.  
 3       Second of all, the problem is not  
 4 whether people are giving information away. The  
 5 problem is do people know about it. As I said  
 6 earlier, the industry, the advertisers, want  
 7 their customers to be happy. They want their  
 8 customers to feel secure. They want their  
 9 customers to use these mechanisms.  
 10       The data says that some of them are  
 11 not using this mechanism, and not an  
 12 insignificant number, because they are concerned  
 13 and frightened, and therefore it is a tremendous  
 14 interest of business to help the consumer feel  
 15 secure. That's why we are pushing within our own  
 16 membership, many other groups are doing it, to  
 17 get the privacy policies up on the advertiser's  
 18 site, up on the web page.  
 19       Now a point has been made, but there  
 20 are other players that people don't know about.  
 21 But who are these other players? They're not  
 22 free riders. They're working for somebody.  
 23 They're working for people who are known.  
 24 They're working for the Fortune 500 companies who  
 25 have a reputation and a brand to protect. Therefore,

<p style="text-align: right;">Page 166</p> <p>1 those companies are going to push to  2 see that these people become known and that  3 consumers are going to be able to protect  4 themselves, because if they don't it's going to  5 undermine the economic model.  6 I can't believe that anybody in this  7 room can honestly say -- you know, there's all  8 this discussion, and I did take experimental  9 psychology, about Skinner boxes. I just don't  10 think most consumers see themselves in a little  11 box being shocked and stimulated. The consumer  12 thinks that he can make choice when he knows what  13 his choices are.  14 So what we're trying to do is allow  15 the consumers to have a fair shot and to make  16 this process more transparent. Everybody in this  17 room agrees that there needs to be more  18 transparency. That is going to come because it's  19 in the businessman's interest, it is in the  20 consumer's interest. And if we don't do it, the  21 government is going to step in, and many of us  22 believe if they do in a fast-moving target  23 they're going to miss the target, they're going  24 to injure the whole process.  25 So we know that if we don't self-regulate</p>	<p style="text-align: right;">Page 168</p> <p>1 marketing companies' advantage to help  2 consumers, they're going to do it. But if it's  3 not to their advantage, if they can get advantage  4 from not helping consumers, they're going to do  5 that, too.  6 Even if we've got on this panel a  7 whole bunch of good actors, and even if the first  8 marketing groups that we're seeing online are all  9 good actors, which they aren't, but even if we  10 say that they are, that doesn't mean that self-  11 regulation is ever going to be the answer to  12 truly protect consumers.  13 There have been lots of cases in the  14 past where it's to a marketing advantage to hurt  15 consumers. Making the system transparent is  16 clearly going to be the answer, but we can't kid  17 ourselves into thinking that marketing concerns  18 or businesses in general are going to be doing  19 things that are against their own best interests.  20 It's only when the consumers' best interests and  21 the marketing companies' best interests intersect  22 that they're going to act on behalf of consumers.  23 Otherwise, there are going to have to  24 be other groups that are going to have to step in  25 on behalf of consumers in order to protect them.</p>
<p style="text-align: right;">Page 167</p> <p>1 there will be regulation. And I'm  2 telling you that even if there is regulation, you  3 should be clamoring for our self-regulation,  4 because the FTC doesn't have enough people,  5 neither does the DOC, neither do the other  6 governments around this world have enough people  7 to track this Net to protect the consumers.  8 So it's only self-regulation that is  9 going to finally give the protection that you  10 need and that you want and that consumers demand.  11 MR. MEDINE: Shari is next. Let me  12 just put on the table a comment that was brought  13 up in the written comments that were submitted to  14 the Commerce Department and the FTC, which is:  15 We've heard about the beneficial uses of this  16 technology in targeting consumers with ads that  17 they might be interested in. Is there the  18 opposite risk, that there could be what's called  19 electronic redlining or price discrimination,  20 where the same targeting process could result in  21 some consumers not getting offers they would  22 otherwise get or being charged higher prices for  23 the same merchandise based on their profiles?  24 MS. STEELE: Yes, and that's exactly  25 the point that I was going to get to. When it is to</p>	<p style="text-align: right;">Page 169</p> <p>1 MR. MEDINE: Jeff.  2 MR. CHESTER: Millions and millions,  3 tens of millions, of online profiles of you and  4 me have been created, and they don't need to know  5 your name, they don't need to know your address,  6 but they know you. The technology has grown  7 dramatically in the last few years. It is now  8 part of the foundation of the next generation of  9 the Internet.  10 That's why we think the Federal Trade  11 Commission, a number of privacy groups including  12 EPIC and Junkbusters and Center for Media  13 Education and Privacy Times and Privacy Journal  14 believe, that the Federal Trade Commission has to  15 launch an immediate 90-day investigation into  16 these technologies. The information is there.  17 It's on the web site, it's in the SEC. It's  18 there about what this technology can do and the  19 attempt to change behavior.  20 This really deserves an independent  21 and serious discussion. It's not just about  22 giving people what they want. That's fine, but  23 if you read the literature it's very clear. It's  24 about changing the color and changing the song  25 until you buy, and it's about writing the TV show</p>

<p style="text-align: right;">Page 170</p> <p>1 to have the e-commerce opportunity embedded.  2 Go to Veon.com, V-e-o-n, to link the  3 psychological aspects of the individual with the  4 emotional intensity of the editorial content.  5 Now, with broadband and the new system emerging,  6 this system is always going to be on. One to one  7 marketing and data collection and profiling and  8 targeting are at the heart of what will be  9 America's new media system in the twenty first  10 century.  11 The technologies are there, they're  12 off the shelf, and we're asking the Federal Trade  13 Commission to get off the plate, investigate  14 these technologies, and give a report to Congress  15 right away about what the policy protection  16 should be.  17 MR. MEDINE: Deirdre.  18 MS. MULLIGAN: Well, first, as an  19 organization that both works on First Amendment  20 issues, including commercial free speech, this is  21 not about limiting people's speech. It is about  22 limiting the collection of data without  23 individuals' knowledge and consent, and that you  24 can separate those things out and I think it's  25 important.</p>	<p style="text-align: right;">Page 172</p> <p>1 feel like their interest is being addressed here.  2 I think most consumers -- as we said, this is not  3 transparent. They have no knowledge of who  4 they're dealing with or that data's being  5 collected. They certainly don't understand the  6 extent of the profiles that are being created and  7 they certainly haven't given their permission by  8 any stretch of the imagination.  9 So I think I welcome the effort and  10 the goodwill that you bring to the table. But  11 I'm saying this is an enormous area, and I don't  12 think that an after the fact opt-out is going to  13 address this problem. So I welcome other  14 people's thoughts.  15 MR. MEDINE: Solveig.  16 MS. SINGLETON: I'd like to begin by  17 going back to Fred Cate's question and just say  18 briefly that, having heard now arguments about  19 some of the harms, that it still seems to me that  20 most of them are of sort of a vague philosophical  21 nature and, especially insofar as we're hearing  22 from consumers on this issue, it does seem that  23 those fears of the technology may be simply  24 stemming from ignorance rather than an  25 understanding of any real harm that might arise</p>
<p style="text-align: right;">Page 171</p> <p>1 I want to welcome Dan's call that  2 industry wants to step forward and address this  3 issue. I agree that self-regulation is part of  4 the puzzle here. I think one of the things that  5 is important to reflect on is that if each one of  6 us at this table operated an independent web site  7 and we wanted to create the kind of profile that  8 DoubleClick or 24/7 creates, we would both have  9 to collect information that was personally  10 identifiable and we would have to disclose it,  11 right, in order for us to do that independently.  12 So in that area I think the industry  13 players who have stepped up to the table said  14 that we need notice, which means clear and  15 conspicuous notice prior to the collection of  16 data; we need consent, at the very minimum the  17 ability to limit the use of data, particularly  18 the disclosure of data, for secondary purposes,  19 which is clearly what targeted advertising of the  20 type that you're talking about is about.  21 Now, I think just on those two  22 points, it is very, very difficult to figure out  23 how a consumer looks at this medium and finds  24 that, even by this minimal standard that we're  25 talking about, notice and consent, is going to</p>	<p style="text-align: right;">Page 173</p> <p>1 from people collecting information on you and  2 wanting to sell you something.  3 The second point I'd like to make  4 goes back to some of the discussion of the  5 benefits. It seemed to me that sort of implicit  6 in that discussion was the idea that the benefits  7 are primarily benefits to business or to industry  8 or to companies that want to market things. I  9 think there's a certain important area of  10 benefits that are being overlooked here, and that  11 is benefits to consumers.  12 One of the things that used to be  13 believed about advertising, for example, back in  14 the 1930's and the 1950's was that this was  15 essentially wasteful information, it simply made  16 people buy things that they didn't want to buy,  17 that it was manipulative and so on. But  18 empirical studies of advertising that economists  19 have done since then have shown that advertising  20 plays a big role in terms of market results in  21 delivering information to consumers, that is at a  22 lower price, delivering goods that are of better  23 quality, and giving them more choices.  24 So when you compare markets where  25 advertising is restricted to similar markets</p>



<p style="text-align: right;">Page 178</p> <p>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</p>	<p style="text-align: right;">Page 180</p> <p>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</p>
<p style="text-align: right;">Page 179</p> <p>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</p>	<p style="text-align: right;">Page 181</p> <p>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</p>

Page 182

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  
 5 don't think an opt-out is going to pass the smell  
 6 test.  
 7 MR. SHAPIRO: Deirdre, we haven't,  
 8 again --  
 9 MS. MULLIGAN: I'm saying if.  
 10 MR. SHAPIRO: But we can't. The only  
 11 way -- I agree with you. Here's what DoubleClick  
 12 is committing to --  
 13 MS. MULLIGAN: I understand what  
 14 you're saying. It's when I go to register there  
 15 will be a little thing saying: If you don't want  
 16 this to become part of your DoubleClick profile,  
 17 opt out.  
 18 MR. SHAPIRO: Yes.  
 19 MS. MULLIGAN: And I'm saying it  
 20 should say: We would like to give this to  
 21 DoubleClick; can you please opt in? It's a  
 22 fundamental change that has enormous -- the  
 23 extent to which all the businesses in this  
 24 discussion of gone to strip out personally  
 25 identifiable information from aggregate data

Page 183

1 about a specific individual highlights what a  
 2 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

Page 184

1 really talking about something that can have  
 2 profound economic competition, innovation values.  
 3 If you're in a small town, you  
 4 suddenly are having options that you never had.  
 5 Up until then you had that one store or two  
 6 stores or three stores to choose from. Now you  
 7 have the whole of the world and it's suddenly  
 8 competing with those two or three stores.  
 9 When we talk about redlining,  
 10 redlining is a real problem. We're not talking  
 11 about setting up a situation where online or  
 12 offline you're going to have an absolutely safe  
 13 world.  
 14 My concern when the whole Internet  
 15 got developed was that we were going to really  
 16 have an information-stratified society. I  
 17 thought that was the real danger, because it  
 18 looked like we were going to a subscription  
 19 approach. What does a subscription approach mean  
 20 if you depend on it? It means those with money  
 21 get the information and those people without  
 22 money don't.  
 23 What's happening is that the Internet  
 24 is opening up incredible information to our kids,  
 25 to ourselves, to all that will come after us, and

Page 185

1 at very low prices.  
 2 MR. CHESTER: I do have to say,  
 3 though, being a children's group, we have real  
 4 concerns about the industry, not this particular  
 5 part of the industry, but tying access into  
 6 having the child and having the family watch the  
 7 ads and giving computers to schools, school  
 8 libraries, forcing the kids to watch the ads.  
 9 We're not against advertising. I  
 10 want to make that clear. But advertising has  
 11 taken a fundamental shift over the last few years  
 12 with the development of these personalization  
 13 technologies that allow this unprecedented  
 14 individual tracking and profiling and potentially  
 15 behavior modification.  
 16 You have to link the technologies  
 17 with the online advertising campaigns designed to  
 18 get consumers to change behavior and to use  
 19 various psychological and other kinds of  
 20 psychographic and demographic approaches to  
 21 change behavior, and you need to make all of  
 22 these extremely transparent.  
 23 In terms of the First Amendment, I'm  
 24 not so sure that this in fact amounts to unfair  
 25 and deceptive practices, because when they know

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



Page 190

1 kind of business advertising model of television,  
 2 syndicated across the entire web. None of these  
 3 are transparent to the individual.  
 4 MR. ARONSON: I agree there  
 5 definitely needs to be transparency. But what  
 6 you're looking at for targeting is that you want  
 7 to target to someone who has shown interest.  
 8 It's not the type of psychological targeting that  
 9 people think that we're doing right now.  
 10 MR. CHESTER: But it is  
 11 psychographic, right?  
 12 MR. MEDINE: Okay, our time is up.  
 13 Two more comments. Jonathan and then we'll close  
 14 on an academic note with Fred.  
 15 MR. SHAPIRO: I just wanted to bring  
 16 this back. This I about the user and the  
 17 consumer. The research suggests that the  
 18 majority of users do want to receive tailored  
 19 information, targeted advertising. We recognize  
 20 again that the majority doesn't mean everybody,  
 21 so that the important point here is that the  
 22 users get notice. This is a transparency issue.  
 23 We agree we as an industry have to do a very good  
 24 job about educating the user about what's really  
 25 going on and then giving them the choice,

Page 191

1 providing them real notice and real choice around  
 2 whether they participate.  
 3 MR. MEDINE: A final remark.  
 4 MR. CATE: I have to say I'm left at  
 5 the end of this with something of a feeling of so  
 6 what, that the harms that we have discussed, the  
 7 little discussion we've had of harms, have tended  
 8 to focus primarily on this: I'll respond to  
 9 advertising if you show me these ads; if you give  
 10 me the color I like, then I'm more likely to  
 11 respond. That's what we've been doing forever.  
 12 There's nothing new about that. That's what  
 13 universities do. That's what people in grocery  
 14 stores do. There's nothing new about that.  
 15 We've asked one question and that is  
 16 is it manipulation? Subliminal advertising, as  
 17 Robert said, clearly manipulation. The FTC has  
 18 said you can't do it. The FTC has said you can't  
 19 do it.  
 20 In this case, we're asking about  
 21 collecting information for uses that so far,  
 22 which is not to suggest that there may be no  
 23 harms, but rather that so far we haven't targeted  
 24 the sort of harm that would justify, particularly  
 25 an opt-in requirement, something that you can

Page 192

1 only think of maybe three examples of in all of  
 2 U.S. law, that this would be the fourth example,  
 3 this with children's privacy. The FTC is going  
 4 to come to my home, protect me on the web. Maybe  
 5 you can set my VCR as well while you're there.  
 6 MS. BURR: Just the clock part.  
 7 MR. ROBERT SMITH: I've got a whole  
 8 list of problems with this profiling and the  
 9 question was never asked. The question was asked  
 10 today, what are the benefits of this technology.  
 11 So we've got them if anybody wants to hear them.  
 12 MR. MEDINE: Thank you very much, all  
 13 of you, for the discussion. The record does  
 14 remain open until November 30th.  
 15 For those who have not passed out for  
 16 lack of lunch, there are flyers outside about  
 17 local lunch places. Thank you. We'll resume at  
 18 2:30.  
 19 (Whereupon, at 1:02 p.m., the  
 20 workshop was recessed, to reconvene the same  
 21 day.)  
 22  
 23  
 24  
 25

Page 193

1 AFTERNOON SESSION  
 2 (2:45 p.m.)  
 3 SESSION III: THE ROLE OF SELF-REGULATION  
 4 MS. BURR: We're going to get started  
 5 with our afternoon panel. We've heard a lot this  
 6 morning and we're now going to turn to the  
 7 question of what the role of self-regulation is.  
 8 We're going to have two presentations before we  
 9 call the panel up this morning. To start with,  
 10 we're going to have Austin Hill from Zero-Knowledge  
 11 Systems give us a presentation. Is  
 12 Austin here? Great.  
 13 (Applause.)  
 14 REMARKS OF AUSTIN HILL, PRESIDENT,  
 15 ZERO-KNOWLEDGE SYSTEMS, INC.  
 16 MR. HILL: Thank you. As mentioned,  
 17 my name is Austin Hill. I think most everyone  
 18 was at the last panel. Zero-Knowledge Systems is  
 19 about consumer privacy online, giving consumers a  
 20 choice to understand how their data is being  
 21 used. The idea is not that we don't know  
 22 anything, just very little, about our customers.  
 23 That's the goal behind the company.  
 24 I want to talk about a couple of  
 25 different things very briefly and do a demo of our

<p style="text-align: right;">Page 194</p> <p>1 upcoming software that's being released in  2 December called "Freedom."  3         When we were designing Freedom, the  4 idea was to come up with a couple different  5 solutions to the problem of privacy on the  6 Internet. One of the big things with Internet  7 privacy is the idea that the actual  8 infrastructure, the underlying TCICP protocol,  9 this is something that was designed 25 years ago  10 and kind of got out of the lab. It wasn't  11 something that people said, we're going to put  12 medical records online, we're going to do  13 commerce and shopping. Everything after that has  14 just been layered on top.  15         We employ a bunch of really bright  16 cryptographers who look at how do we design  17 networks so that the network privacy is built  18 into the infrastructure, so it's not something  19 that afterwards you try and layer on top of, but  20 you can actually build it into the protocols.  21         So one of the key parts of this is  22 something we call the Freedom Network. Now, the  23 Freedom Network builds on the idea of separating  24 out information about a user from where they're  25 going online. Just because you're using a public network</p>	<p style="text-align: right;">Page 196</p> <p>1 no linkage to the client's actual IP.  2 This becomes real important as we look at things  3 like static IP addresses, IP Version 6 that has  4 unique identifiers, because it allows the user to  5 separate out the identity at an infrastructure  6 and a technical layer so that the network itself  7 doesn't reveal or compromise our identity, the  8 same way walking around on the street does not  9 compromise our identity. We may choose when we  10 walk into an establishment to identify ourselves  11 with a loyalty card or a credit card if we want  12 to pay that way, but simply by walking down the  13 street we're not giving up any privacy.  14         So the goal of the Freedom Network is  15 to establish that first basis. Then on top of  16 that we talk about separating out identity and  17 building an identity management system. Now, the  18 goal behind our identity management system is  19 something we refer to as "Nyms," "Pseudonyms."  20 Now, the goal behind Pseudonyms is to be able to  21 establish online personas that are separate and  22 unique from your real identity.  23         The idea that we're going to  24 establish in the future a single identity system  25 that acts as a national passport is very against privacy.</p>
<p style="text-align: right;">Page 195</p> <p>1 doesn't mean you want everyone in the  2 public to know what you're doing.  3         So one of the things we do is, a  4 consumer goes to browser the Net, if they have  5 our Freedom software installed we relay all their  6 packets with different layers of encryption  7 through a series of servers around the world.  8 What this ends up doing is making sure that no  9 one, not even Zero-Knowledge, knows the identity  10 of the customer as they go online.  11         That's the start. That's the  12 infrastructure. So this is an example of how a  13 packet would transfer or be formatted. There are  14 multiple layers of encryption, and as the packet  15 leaves the computer we have wrapped it with a  16 different layer of encryption for each one of the  17 servers.  18         So it leaves the client's PC and it  19 goes to one of the first servers. That first  20 server only knows the identity of the client PC.  21 It then sends it on to another server. That  22 server then passes it on to the final server,  23 which would connect to the end web site.  24         So now the client is browsing and he  25 appears to be coming from the final server. So there's</p>	<p style="text-align: right;">Page 197</p> <p>1 But at the same time, for transactions  2 like commerce, applying for health information  3 online, insurance applications, we need better  4 forms of identity. We need a way that we can  5 certify who we're talking to.  6         A lot of those situations, it's a  7 true identity certification. For instance, we're  8 not going to ask our doctor for X-ray information  9 under our handle "Looking for a Date at  10 Hoffman's." You want a true identity if you're  11 going to be asking for health care information.  12 But a lot of uses, let's say for instance talking  13 about health care concerns or you're taking part  14 in a support group online, you don't want it  15 associated with an insurance application. You  16 don't want it associated with all your  17 activities.  18         So Zero-Knowledge promotes the idea  19 of being able to separate out your identity so  20 that you have a unique identity for each one of  21 your online activities. Now, Zero-Knowledge does  22 that by establishing these Pseudonyms, and I'll  23 give you a quick example of how these Pseudonyms  24 work.  25         (Screen.)</p>

<p style="text-align: right;">Page 198</p> <p>1 I just have a web page. I think  2 that's Richard Smith's work.  3 (Pause.)  4 We're waiting for the demo. There we  5 go. Okay, so this is Freedom. You'll see that  6 it's sitting in a toolbar just beside my browser.  7 I have the ability with a pull-down menu to select  8 one of my identities. Each of my identities is  9 completely unique. It has its own e-mail  10 address, its own cookie file. It is completely  11 separated from any of my other identities, the  12 goal being I can create an ID, "Cancer Support at  13 Freedom.net," and that's separate from anything I  14 do with e-commerce, and I know that my activities  15 cannot be profiled across ID's.  16 Part of how we do that is we maintain  17 and separate out information. This is an  18 identity called "Half-Finger," so you have an  19 icon representing it. So there is the e-mail  20 address. You can define your security settings  21 for how much encryption you want, so you can  22 trade off speed versus performance.  23 We can also look in the cookie  24 folder, and if you look into the cookie folders  25 with this Pseudonym you can see all the cookies</p>	<p style="text-align: right;">Page 200</p> <p>1 or frequenting the same establishment over a long  2 period of time, that organization might want to  3 give us discounts, loyalty reward programs. But  4 by using a pseudonym-based relationship that is  5 separate from your true identity, it stops the  6 abuse of that site exchanging your data with  7 another, because every partner and every person  8 you interact with you can manage your identity  9 set, so you don't have to compromise more than  10 you are planning to.  11 MR. MEDINE: Thanks very much,  12 Austin, for an example of how the technology can  13 address some of the concerns that we've heard  14 about throughout the day.  15 I want to turn now to Jerry Cerasale  16 from the Direct Marketing Association. Jerry's  17 certainly a veteran of the FTC and Commerce  18 Department workshops. He's the Senior Vice  19 President for Government Affairs of the Direct  20 Marketing Association, which seeks to raise the  21 bar for privacy practices by assuring that its  22 members adhere to certain privacy practices.  23 Jerry.  24 REMARKS OF JERRY CERASALE,  25 SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS,</p>
<p style="text-align: right;">Page 199</p> <p>1 and you can selectively block per site or you can  2 block all cookies. So under one of my identities  3 where I have a higher concern for privacy, let's  4 say health care activities, I might choose to  5 block all cookies, where under another one of my  6 identities I might choose to only block cookies  7 from ad-serving networks, but accept a cookie  8 from Yahoo.  9 So it allows the user to selectively  10 choose which cookie they want to receive. At the  11 same time, if we go into another one, another  12 identity, and we look at the cookies, the cookies  13 are completely separate for that different  14 identity. So what we're allowing users to do is  15 gain the benefits of technologies like cookies,  16 digital certificates -- each identity has a  17 digital certificate and can authenticate itself -- but  18 not have to compromise their true identity,  19 which is a really important innovation, because  20 the idea on the Internet is not for everyone to  21 be anonymous.  22 Total anonymity fights back against  23 community. We want to establish relationships.  24 We want people to know who we are. We want to  25 maintain loyalty with a brand. If we're buying</p>	<p style="text-align: right;">Page 201</p> <p>1 DIRECT MARKETING ASSOCIATION  2 MR. CERASALE: Thank you very much,  3 David.  4 I'm in the process here of just  5 setting up my computer. Let me talk to you very  6 briefly before I show you this very simple, this  7 very simple demonstration. One, why DMA has  8 placed this? As you can see, I'm not  9 technologically literate here, so this is going  10 to be a very non-technical operation.  11 What's coming up is a panel on self-  12 regulation and the DMA is very much a proponent  13 of self-regulation. In July we required a  14 privacy promise to be a member of the DMA and any  15 member of DMA in any form, any medium that  16 collects information, personally identifiable  17 information, and transfers it to third parties  18 must let the consumer know and must give them  19 opportunity to opt out.  20 I think that's the situation as we  21 look at what we're talking about here today, is  22 ad servers, and we don't think it's very  23 different for them, either, in a situation where  24 you go to a web site and then turn onto, click  25 onto a banner ad. You're really in a situation</p>

<p style="text-align: right;">Page 202</p> <p>1 where there are three parties at play. There is  2 the web site that you're visiting, probably the  3 publisher.  4 I don't know if this is going to work  5 here.  6 (Screen.)  7 Yes, it does.  8 The web site that you're on is the  9 publisher and you have the advertisement, the  10 advertiser whose ad you click on, and then you  11 have an ad server that's between that. Clearly,  12 you know the web site you're on and they would  13 have a privacy policy. You know the advertiser  14 you clicked to and hopefully they have a privacy  15 policy.  16 But it's likely that you don't have  17 the foggiest idea who the ad server is. So we  18 took a look at that and said, how do we get  19 notice and choice, which is the key to the DMA's  20 privacy promise? We believe the place to give  21 notice in the first instance falls on the  22 publisher, the web site that you originally go  23 to. They already have the obligation, if they're  24 DMA members, or they should have the obligation  25 if they collect personally identifiable</p>	<p style="text-align: right;">Page 204</p> <p>1 relationship between the consumer and the third  2 party ad server. So that's the real important  3 thing that we're trying to push here.  4 The DMA in 1997, in trying to help  5 people put privacy policies on their own web  6 site, created a privacy policy generator at our  7 web site. You just answer a few questions and it  8 will print out what your privacy policy is.  9 Well, 1997 is a long time back in Internet time,  10 so we've decided it needed to be updated, and ad  11 servers is clearly one of the areas where we want  12 to update.  13 So we've added a few things to it:  14 whether or not you use cookies and things on ad  15 servers; if you decide to change your policy on  16 how you're going to use information; access and  17 correction; and security and some form of  18 reinforcement -- of enforcement, excuse me.  19 What I'd like to do is take you, if  20 this thing will move me there, to the DMA privacy  21 policy generator that is on our web site.  22 (Screen.)  23 This is it. These actual forms will  24 not be up. The web site is up, but item number 4  25 -- excuse me -- item number 5 will not be up</p>
<p style="text-align: right;">Page 203</p> <p>1 information themselves and give it to third  2 parties, including the ad server; they must  3 disclose it and give you an opportunity to opt  4 out.  5 We think that they should also  6 disclose to you whether or not they have any  7 relationship with a third party ad server and to  8 let you know that the third party ad server may  9 be independently collecting information on them,  10 and to give you a hot link to the privacy policy  11 of their contractual third party ad server.  12 From the ad server's point of view,  13 we think that they have the obligations that any  14 DMA member would have, that they provide notice  15 to the types of information they collect, what  16 they do with the information, and if their  17 navigational data is to be used in an  18 identifiable manner by the ad server that should  19 be disclosed. And there should be an opportunity  20 of choice for the consumer.  21 It's that simple: Let the consumers  22 know and give them a choice. The point of view  23 here is what's different with this situation is  24 when do you give them notice and who should give  25 them notice, because you don't have a</p>	<p style="text-align: right;">Page 205</p> <p>1 until later this week, whether or not you collect  2 cookies. We didn't have anything on it before in  3 1997. We think it is important to let people  4 know whether or not you place a cookie, not  5 collect cookies, excuse me; and if you do place a  6 cookie, what use you put it to.  7 So you can see the checklist. I  8 don't know if you can read it. You just click on  9 "Yes, I collect cookies" -- "I set cookies," or  10 "No, I don't," and then what uses you put it to.  11 Then there's an "Other" policy there where you  12 can add it in. So we would hope everyone would  13 answer that.  14 Then we go down to these other  15 privacy policy statements here, like name,  16 address, e-mail addresses, phone numbers,  17 etcetera. Those were all on our 1997 web site.  18 We've added this other one, "Ad servers," whether  19 or not you partner with someone, and if you do to  20 make a statement that in fact you do partner and  21 that they may collect information on you.  22 I've typed in, not to dump on any  23 company, "www.jerry.com" in order to show you in  24 a later slide what the privacy policy said. But  25 that would be there, and we'll try and make a hot</p>

<p style="text-align: right;">Page 206</p> <p>1 link with that.  2 We also added item number 12, which  3 has to do with dual uses. I think that was  4 something that came up in the panel this morning,  5 that we suddenly have a privacy policy, I've seen  6 it and I've given some information out, and you  7 decide to change that privacy policy. You decide  8 to change the uses, how you're going to let  9 people know, etcetera, and this is a series of  10 questions telling you what you will do and how to  11 notify the web site.  12 Another question that constantly  13 comes up is access, whether or not you allow  14 access, what information you can see. You can  15 see down at the bottom the last click there is  16 "No information that we have collected and that  17 we maintain about them," so that you do have the  18 negative option, you do not allow access. But  19 these are things that you can check off, and it's  20 not one or the other; it's all that apply, in the  21 hope that we can make it easy for not just larger  22 companies, but all companies who have a web site,  23 to go someplace, answer a few questions, get a  24 privacy policy that's fairly comprehensive about  25 what they do, and give it to their attorneys to</p>	<p style="text-align: right;">Page 208</p> <p>1 there, but we didn't do that. You're quite  2 welcome.  3 So that's pretty much where it is.  4 As you can see, way down at the bottom you can  5 generate this web page in HTML, you can e-mail  6 it, you can make it in hard copy, and so forth.  7 We do ask people to e-mail a copy to the DMA so  8 we know how many people use it. I'm not sure how  9 many people do that for us, but we do get a few  10 of those and know people have done it.  11 That's pretty much what we have done  12 to try and make it so that customers have an  13 opportunity to know if information is being  14 collected, to have an opportunity to say, no,  15 don't do it. And hopefully, with this  16 understanding we can make the web experience  17 rewarding, that people will not be afraid to go  18 surfing on the web, that they will not be afraid  19 of data that's not personally identifiable, that  20 helps them enjoy and get to places without re-  21 registering, don't see repeat ads, etcetera, and  22 not be afraid of it.  23 Thank you very much for your time and  24 thank you, David, for having me.  25 (Applause.)</p>
<p style="text-align: right;">Page 207</p> <p>1 switch things around, but then can quickly get it  2 up on their web site so that we can get  3 information to customers and consumers so they  4 know what's happening and have some choices,  5 because we want e-commerce to continually grow,  6 and the only way it's going to grow is if there's  7 consumer confidence and consumer confidence comes  8 from knowing what the web site is doing with  9 information.  10 Besides, if you sell something you've  11 got to deliver the product and it has to have  12 good quality. But really, the idea is we want  13 people to go searching on the web and taking a  14 look at our privacy policies.  15 Finally, we put out what kind of  16 security we have on the web site. We have some  17 additional questions in there about financial and  18 medical information that you can see, and you'll  19 be able to go to that web site and take a look at  20 it if you'd like.  21 Then on enforcement, if you have a  22 complaint where do you go. We put the DMA on  23 there. We added the FTC. I didn't put David  24 Medine's phone number on there, just a general  25 phone number. I was tempted to put David's on</p>	<p style="text-align: right;">Page 209</p> <p>1 MR. MEDINE: Thank you, Jerry. These  2 were all helpful pieces of how companies and  3 trade associations are responding to some of the  4 concerns we've heard throughout the day.  5 We'd like to now invite up the  6 panelists for the third panel.  7 MS. BURR: Just the keep you on your  8 toes and so that you don't get used to the usual  9 format here we're actually going to ask the  10 panelists to introduce themselves, and we'll  11 start way over on the end with Dan and just go  12 around.  13 MR. JAYE: Yes, I'm Daniel Jaye,  14 Chief Technology Officer and co-founder, Engage  15 Technologies.  16 MS. WANG: I'm Elizabeth Wang. I'm  17 General Counsel of DoubleClick.  18 MS. OAKES: I'm Lynn Chitow Oakes,  19 Chief Operating Officer for Flycast.  20 MR. ZINMAN: I'm Dave Zinman, VP of  21 Marketing and founder of AdKnowledge.  22 MR. HILL: I am Austin Hill. I still  23 have Zero-Knowledge.  24 MS. BRUENING: I'm Paula Bruening.  25 I'm the Director of Compliance and Policy for</p>

<p style="text-align: right;">Page 210</p> <p>1 TRUSTe.  2 MR. CERASALE: Jerry Cerasale, Senior  3 Vice President, Government Affairs, with Direct  4 Marketing Association.  5 MR. ROBERT SMITH: Robert Ellis  6 Smith, Publisher of Privacy Journal.  7 MR. CATE: Fred Cate. Because I was  8 confused, they invited me back.  9 MR. HENDRICKS: Evan Hendricks,  10 Editor and Publisher of Privacy Times.  11 MR. KAMP: John Kamp, Senior Vice  12 President, the American Association of  13 Advertising Agencies.  14 MR. LUCAS: Steve Lucas, Senior Vice  15 President from Industry and Government Relations,  16 PrivaSeek.  17 MR. LORDAN: Tim Lordan with the  18 Online Privacy Alliance.  19 MR. SHEN: Andrew Shen, Policy  20 Analyst, Electronic Privacy Information Center.  21 MS. BURR: I don't know if it's  22 intentional or not, but we seem to have  23 segregated the tables here. So I'm going to turn  24 to the table on my right.  25 We've heard a lot of very interesting</p>	<p style="text-align: right;">Page 212</p> <p>1 secretive way. Our companies are among the  2 leading providers of advertising solutions to web  3 publishers in advertisers, and the services we  4 offer have substantial economic benefits for both  5 consumers and companies.  6 According to Dr. Westin's most recent  7 survey, we are providing services that most  8 consumers want to receive using technology  9 adapted to the Internet. For example, most  10 smaller and medium sized web sites use our  11 services or similar services, and it's very  12 important to preserve the ability to deliver  13 effective services via third party ad servers to  14 allow these medium and smaller sites a chance  15 against the larger portals and the larger, more  16 established sites.  17 The goal of the group was to explore  18 ways in which we could collectively address the  19 types of consumer concerns and perceptions about  20 profiling that we have heard this morning.  21 Although our companies do not deal directly with  22 consumers on the Internet, we believe we can play  23 an important role in increasing consumer  24 confidence and contributing to the growth of  25 electronic commerce.</p>
<p style="text-align: right;">Page 211</p> <p>1 things today about this technology, about its  2 benefits, about the concerns that it raises with  3 Internet users. The topic of our panel this  4 afternoon is how self-regulation can help in this  5 area.  6 So I'd like to talk to the companies  7 and ask, what do you think?  8 MR. JAYE: Thank you. On behalf of  9 my colleagues in the Internet network advertising  10 business, I'd like to thank the Federal Trade  11 Commission and the Department of Commerce for the  12 opportunity to participate in today's workshop.  13 (Slide.)  14 Earlier this year, a group of  15 companies in the Internet advertising business  16 began talking with government officials about  17 issues surrounding advertising on the Internet.  18 They included 24/7 Media, AdKnowledge, AdSmart,  19 AdForce, DoubleClick, Engage, Flycast,  20 MatchLogic, NetGravity, and RealMedia.  21 The first thing to know about our  22 companies is that they are not mysterious  23 entities taking profiling technologies to  24 dizzying levels which threaten consumer privacy,  25 nor are they gathering data in a deliberately</p>	<p style="text-align: right;">Page 213</p> <p>1 To that end, we in the industry are  2 announcing the launch of the Network Advertising  3 Initiative, NAI. Our goal is to develop a  4 framework for self-regulation of our industry.  5 We believe our industry is distinctive because we  6 have no easy way to communicate directly with  7 consumers. Our business is not to make our own  8 web sites known to consumers. Our business is to  9 make our customers' web sites more useful to  10 consumers.  11 To do that, we provide a wide range  12 of advertising solutions to consumer-oriented web  13 sites, to support their development and growth.  14 Elizabeth Wang will talk in more  15 detail about what we have been working on.  16 MS. WANG: Thank you, Dan.  17 As many of the commenters today have  18 pointed out, there are significant benefits to  19 Internet advertising for consumers and the  20 industry. For consumers and web sites, it is the  21 reason why content on the web is available for  22 free or for nominal cost. For advertisers,  23 Internet advertising takes advantage of a medium  24 uniquely suited to delivering the right message  25 to the right consumer at the right time.</p>

<p style="text-align: right;">Page 214</p> <p>1 Our companies use technology to help  2 advertisers deliver tailored messages to  3 consumers. In fact, every consumer who uses the  4 Internet has likely seen the banners and other  5 advertising our companies deliver.  6 As Dan Jaye and Martin Smith  7 discussed this morning, the NAI companies collect  8 information in order to make decisions on which  9 ads to send to whom. Some NAI companies create  10 profiles about consumers in order to tailor that  11 message. As Dr. Westin's survey demonstrates,  12 most consumers want a more relevant message and  13 are willing to accept profiling, but they also  14 want to be given notice about the information  15 that is collected and used and a choice not to  16 participate in some uses of the collected  17 information.  18 Our companies understand consumer  19 concerns. As Lynn and David will explain, our  20 companies are fully committed to the principles  21 of notice and choice for consumers.  22 Today we are announcing the key  23 tenets of the Network Advertising Initiative:  24 First, each NAI company will continue to provide  25 consumers with a clear explanation of the</p>	<p style="text-align: right;">Page 216</p> <p>1 We believe that education is the key  2 to developing consumer confidence on the  3 Internet, and for that reason our companies are  4 committed to educating our business customers  5 about the data collection and use issues  6 associated with Internet advertising. This  7 includes the benefits of both the responsible  8 flow of information and fair information  9 practices.  10 We are also committed to educating  11 consumers about data collection and use issues  12 associated with Internet advertising. As Dr.  13 Westin's survey clearly indicated, most consumers  14 are willing to share information, even personal  15 information, with companies like ours if they are  16 provided with notice and choice.  17 As a first step toward meeting  18 consumer expectations, NAI companies will be  19 establishing an informational web site located at  20 www.networkadvertising.work, as pictured on the  21 screen behind me. This web site has been  22 developed to provide consumer awareness about our  23 industry and provide an easily accessible and  24 convenient place for consumers to exercise choice  25 regarding the use of their data.</p>
<p style="text-align: right;">Page 215</p> <p>1 information it collects, how that information is  2 used, and the benefit to consumers of such use.  3 Second, for consumers who choose not  4 to receive tailored messages, each NAI company  5 either currently provides or will soon provide an  6 easy to use method to opt out from such  7 tailoring.  8 Third, our companies are committed to  9 consumer outreach and education to let consumers  10 know about our companies and the role we play in  11 delivery of tailored messages over the Internet.  12 In other words, we have heard consumers' concerns  13 and we are committed to addressing them.  14 Now I'll turn the microphone over to  15 Lynn Chitow Oakes from Flycast, who will explain  16 more about our commitment to notice and choice.  17 MS. OAKES: Thanks, Elizabeth.  18 NAI companies are committed to  19 providing consumers with notice and choice about  20 Internet advertising. We believe that adherence  21 to fair information practices and data management  22 that we are going to describe today are in  23 accordance with the consumer expectations and  24 desires as outlined in Dr. Westin's survey and in  25 our own business experiences.</p>	<p style="text-align: right;">Page 217</p> <p>1 Our companies also adhere to the fair  2 information practices developed by the Online  3 Privacy Alliance and other organizations  4 interested in privacy. To that end, all the  5 Internet advertising sites owned or controlled by  6 one of our companies will disclose their data  7 collection and use practices on their web sites  8 in a clear, concise, and conspicuous manner and  9 in language that consumers can understand.  10 These disclosures will include the  11 following: what data are collected and what data  12 are not collected; how the data are used,  13 including whether they will be combined with  14 personally identifiable data from any other  15 source; what other data are collected and how  16 they are used, including the use of data for ad  17 management; and lastly, what opt-out procedure  18 are available for consumers who decline to have  19 data used to create a profile.  20 In addition, our companies will at a  21 minimum request that their customers, whether  22 they are publishers, e-commerce sites, or  23 networks, disclose their own data collection and  24 use practices, including posting a link to either  25 the NAI companies' web sites or the NAI gateway</p>

<p style="text-align: right;">Page 218</p> <p>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  8 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</p>	<p style="text-align: right;">Page 220</p> <p>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</p>
<p style="text-align: right;">Page 219</p> <p>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</p>	<p style="text-align: right;">Page 221</p> <p>1 displayed here.  2 As a way of informing consumers about  3 their choices, we will ask all of our customers  4 and participating web sites to link to our  5 individual sites or the gateway educational site.  6 So with that description, I'd like to  7 turn it back over to Dan to sum up.  8 MR. JAYE: Thank you.  9 We believe that the principles we are  10 developing will ensure the continued growth of  11 consumer confidence in the marketplace. However,  12 there is one more element necessary. Although we  13 know that we will follow these industry  14 principles, we want consumers to be assured as  15 well.  16 For this reason, our companies are  17 committed to not only complying with these  18 principles, but also to join or retain a third  19 party organization that provides periodic audits  20 of compliance with our privacy policy. This  21 includes organizations such as TRUSTe, BBBOnline,  22 WebTrust, as well as nationally recognized  23 accounting firms that provide such services.  24 Watch our web site in the coming  25 months. You will see information about our</p>



<p style="text-align: right;">Page 222</p> <p>1 companies, what we do, how we do it, and how  2 consumers can exercise choice. We will pursue  3 activities to promote consumer confidence and  4 trust.  5 We believe the measures we are  6 implementing are the foundation of a self-regulatory  7 framework for our industry that will  8 protect privacy while allowing the effective  9 advertising that makes the web free. We look  10 forward to working with our colleagues across the  11 industry to fulfil the commitments we have made  12 today.  13 Thank you.  14 MS. BURR: Thank you very much.  15 I'd like to turn to the rest of the  16 panel to solicit questions about what we have  17 just heard. And let me remind the audience that  18 we do have question forms and that people will be  19 going, picking them up and delivering them up to  20 us.  21 Andrew.  22 MR. SHEN: I think it's fair to say  23 everyone in this auditorium believes that  24 consumers should have the right to control their  25 information. However, I think there is really a</p>	<p style="text-align: right;">Page 224</p> <p>1 without the knowledge of most consumers, so the  2 opt-out option is not really a good way to  3 approach the problem because most consumers don't  4 know that this is occurring at all.  5 MR. JAYE: We believe that it's very  6 important for us to address those consumer  7 confidence issues. That's one of the reasons why  8 we have stepped forward and said that we would  9 like to provide choice to consumers even for non-  10 personally identifiable information. Fair  11 information practices literally to this date have  12 generally been interpreted to apply to personal  13 data, personally identifiable information.  14 We have taken a step forward and  15 understood the sensitivity of the information and  16 said that we are committed to providing an opt-out for  17 the innocuous information that we use for  18 non-personally identifiable profiling.  19 MR. MEDINE: I think it might be  20 helpful to clarify what your intentions are with  21 regard to the opt-out for non-personally  22 identifiable information. I don't think it's  23 immediately clear how it could be used for some  24 forms of ad management but not for profiling.  25 Could you maybe explain in a little more detail</p>
<p style="text-align: right;">Page 223</p> <p>1 distinction to be seen between what the companies  2 are providing in terms of control and what  3 consumers want.  4 Fair information practices have four  5 different --  6 VOICE: A little louder, please.  7 Speak into the mike.  8 MR. SHEN: Sorry. Is this loud  9 enough?  10 MS. BURR: It's working. Just bring  11 it closer.  12 MR. SHEN: Fair information practices  13 consist of four different elements: notice,  14 which is providing information to the consumer  15 about how the information is being collected and  16 how it's going to be used; consent, which means  17 that the person gives affirmative permission for  18 the companies to use that information; access, so  19 the consumer has access to the information that's  20 being collected on them, what is contained in the  21 profile; and security, so that information is not  22 distributed to other third parties.  23 The self-regulatory proposal done by  24 the NAI does not meet all those requirements.  25 Online advertising is something that happens</p>	<p style="text-align: right;">Page 225</p> <p>1 exactly what information is going to be captured  2 through the use of the cookies and how it will or  3 won't be used?  4 MR. JAYE: Certainly. One example  5 that we talk about in terms of profiling is the  6 use of a cookie to manage an identifier that then  7 could be used to build a profile for that web  8 site visitor. That type of information, we can  9 provide an opt-out and some companies around the  10 table have already done that by allowing that  11 cookie to be set to an arbitrary value like opt-out that  12 would be a signal to a web site to  13 remember that this browser is one of a number of  14 browsers that are not to be tracked.  15 However, it is also possible to have  16 other cookies on the computer that are being used  17 for application management or other purposes.  18 The most prototypical example would be for  19 counting unique visitors, being able to correlate  20 an ad click with the ad that was displayed, being  21 able to try to avoid duplication of ad displays.  22 In other words, avoiding repetition of the same  23 ad over and over again.  24 These uses are not targeting per se,  25 but they are important to the operation of the ad</p>

Page 226

1 industry. And once again, this is an industry  
 2 that is extremely important to nascent and  
 3 entrepreneurial web sites, as well as many medium  
 4 and in fact very large web sites that don't have  
 5 the infrastructure or manpower to staff these  
 6 services internally.  
 7 MR. ZINMAN: I just want to follow up  
 8 and say that one of the reasons that we're taking  
 9 this significant step is because fundamentally we  
 10 have a different relationship with the consumer  
 11 than a web site, where a person sees it. Most  
 12 consumers don't know we exist, so we need to go  
 13 the extra mile to allow the consumer to have  
 14 complete choice, even if it's only of information  
 15 that isn't personally identifiable.  
 16 So related to your question, your  
 17 question related to personally identifiable  
 18 information, which there's no question that you  
 19 have to be -- every company needs to adhere to  
 20 fair information practices, but on information  
 21 that's not even personally identifiable we're  
 22 willing to go the step to give the consumers the  
 23 choice as to whether we retain that information.  
 24 MR. MEDINE: So I understand, the  
 25 limits are that you would know which ad I have

Page 227

1 seen so it's not delivered to me again, but you  
 2 wouldn't know anything about me in order to  
 3 decide which ad I should receive if I have opted  
 4 out?  
 5 MS. OAKES: Absolutely.  
 6 MR. JAYE: That is what is provided  
 7 in our initial step of the principles.  
 8 MR. MEDINE: Another question in  
 9 assessing any self-regulatory system, one issue  
 10 is how broad is it, how much of the industry does  
 11 it cover? I know you're all fierce competitors,  
 12 but I suspect not all the competitors are in the  
 13 room today. Give me a sense of what percentage  
 14 of the industry the people who are part of the  
 15 NAI constitute?  
 16 MS. OAKES: The majority of folks  
 17 that are in the third party ad surveying are at  
 18 the table. There are ten companies involved that  
 19 represent, an estimate that we put together  
 20 today, actually about 85 percent of ads served on  
 21 the Internet today.  
 22 MR. ZINMAN: It is very difficult to  
 23 determine that, but if you look at just the  
 24 companies that are involved with doing just the  
 25 infrastructure work of delivering advertising,

Page 228

1 the vast majority of those ads that are served  
 2 are served by companies that are part of this  
 3 group. And I'd suspect that if there are a few  
 4 remaining companies that contribute significantly  
 5 to this, that they're going to be interested in  
 6 joining this as well.  
 7 MR. HILL: First of all, I want to  
 8 commend the Network Advertising Initiative. I  
 9 certainly think that any attempt to make the  
 10 process more transparent to users and get users  
 11 involved should be commended. I don't think that  
 12 there is one solution that fits all. Technology  
 13 can't solve the problem in and of itself. I  
 14 don't think regulation can solve the problem in  
 15 and of itself. At the same time, industry  
 16 efforts like this I think do a lot of good.  
 17 I have a couple of specific  
 18 questions. I'm just going to lay them out, let  
 19 you guys individually take it. You talked about  
 20 how fair information practices, the difference  
 21 between this and traditional fair information  
 22 practices that Andrew touched on, is because it  
 23 is not personally identifiable information, where  
 24 there is opt-out versus opt-in.  
 25 The question I would have is, for the

Page 229

1 cases where members of your group do adopt  
 2 personally identifiable information, would the  
 3 group be requiring them to adopt an opt-in for  
 4 that purpose that go the extra step?  
 5 The next question I would have is,  
 6 being that I think this group represents the good  
 7 players in the industry, the players who are  
 8 trying to make an initiative to protect  
 9 consumers, how would this group feel about some  
 10 sort of legal framework for redress and  
 11 accountability for bad players, so that in  
 12 situations where people aren't adhering there is  
 13 a legal framework to hold that person  
 14 accountable?  
 15 MS. WANG: Actually, in addressing  
 16 your question, Austin, I want to characterize  
 17 something, the way you characterized fair  
 18 information practices. The principles are  
 19 notice, choice, security, and access. Choice is  
 20 not opt-in. Choice is really, it can include  
 21 opt-out, and in the United States it's always  
 22 been opt-out, hardly every opt-in, except in very  
 23 sensitive situations like medical, financial,  
 24 kids.  
 25 So that's actually -- so in fact

<p style="text-align: right;">Page 230</p> <p>1 there's a very key thing in our principles today  2 and that is we are following the fair information  3 practices principles. We're not expanding them.  4 We're not extending them. We're not saying that  5 opt-in is the right answer for personally  6 identifiable information. In fact, we believe  7 opt-out with clear notice and an effective opt-out cookie  8 and an easy method to opt out actually  9 more than satisfies that requirement of the fair  10 information practices.  11       There is something that our  12 companies, the fact that we deliver ads and we're  13 not apparent to some consumers, although I think  14 we are quite apparent because certainly people,  15 consumers, know who we are even though they're  16 not in advertising or they're not web publishers.  17 I think we're more apparent than most people give  18 us credit for, and sometimes many of them are our  19 investors as well.  20       But getting back to your point, the  21 reason why in our situation the opt-out included  22 some information that was acquired for ad  23 targeting really went to the fact that it's a  24 relationship issue. We don't have a direct  25 relationship with the consumer. So it's an</p>	<p style="text-align: right;">Page 232</p> <p>1 consistent with other self-regulatory regimes, it  2 is this third party auditing that will provide  3 for the accountability.  4       MR. HILL: Just to follow up on that  5 question, so in a situation like we have seen  6 this week with RealAudio, where they had a TRUSTe  7 privacy seal, there were activities, and TRUSTe  8 hasn't come down with their result, but that some  9 people would feel weren't disclosed or honest, so  10 the enforcement level that you're talking about  11 would be the withdrawal of some sort of seal?  12       MS. WANG: Well, I don't know any of  13 the details of that RealJukebox situation other  14 than what I read in the paper. But wouldn't you  15 agree that it was very effective, the self-regulatory  16 mechanism there? The market came down  17 very hard and RealNetwork did the right thing  18 right away. I think to me that's just evidence  19 that it works extremely well, and that's just one  20 of many instances.  21       MR. HILL: I'm not commenting on the  22 benefits, the strengths and the weaknesses. I'm  23 just asking for this organization if that's the  24 desired enforcement mechanism, is the withdrawal  25 of outside audit seals if someone is a bad</p>
<p style="text-align: right;">Page 231</p> <p>1 easier issue for web sites, web publishers, that  2 deliver their own advertising on behalf of  3 advertisers, because the consumer knows whom  4 they're dealing with.  5       In our situation, we went the extra  6 mile, as Dave put it, and allowed for the opt-out of non-  7 personally identifiable information  8 collected in the routine course of delivering an  9 ad or even delivering content to a consumer  10 because of the situation that we find ourselves  11 in, that we are business to business companies  12 and not direct to consumer companies. So I just  13 wanted to clarify that one point, that we are in  14 fact not saying that -- we're not at all  15 expanding on anything that the OPA has put forth  16 in the few years.  17       To your second point, on legal  18 framework for accountability, the very critical  19 part of our principles and one that Dan Jaye  20 mentioned is that we are all going to agree to  21 join third party auditing organizations to make  22 sure that other people agree that we do what we  23 say we do, because certainly we have every  24 intention of following our own principles.  25       In terms of the accountability,</p>	<p style="text-align: right;">Page 233</p> <p>1 player? So a bad player in the network would  2 find themselves without an audit seal? There  3 would be no accountability or redress?  4       MR. HILL: But could a consumer go  5 and hold that company accountable, sue them? Do  6 you guys advocate some sort of framework? If  7 someone says, I don't want to be in NAI, I don't  8 care, I'm going to profile, should there be a  9 framework?  10       MR. ZINMAN: I think there's another  11 method of control that we need to get out here,  12 which came out in the second panel, and I'm not  13 going to articulate it as well as Dan Jaffe, but  14 I'm going to try, which is that the advertisers  15 do not want to be associated with companies that  16 abuse the trust of consumers, and all the  17 companies in our industry, our lifeblood is the  18 respect and responsibility that we hold with our  19 consumers, the advertisers.  20       So every company that represents any  21 significant advertising dollars is going to feel  22 a lot of pressure to make sure that they are  23 responsible to consumers. So I think companies  24 are going to naturally be pushed into a self-regulatory  25 environment with or without</p>

<p style="text-align: right;">Page 234</p> <p>1 regulation.</p> <p>2 MR. MEDINE: I just want to add, of</p> <p>3 course, the Federal Trade Commission's deception</p> <p>4 authority to bring cases against companies that</p> <p>5 don't honor their privacy promises, both to</p> <p>6 consumers and business partners. I also thought</p> <p>7 it might be useful at this point just to hear</p> <p>8 from Paula Bruening from TRUSTe.</p> <p>9 MS. BRUENING: Thank you. I'd like</p> <p>10 to make two points, one that would speak directly</p> <p>11 to the RealNetwork issue and one that probably</p> <p>12 speaks more to the general issue of relationship</p> <p>13 that everyone's been talking about.</p> <p>14 First of all, without going into</p> <p>15 tremendous detail, RealNetworks is a TRUSTe</p> <p>16 licensee and I think the people in this room and</p> <p>17 definitely on this panel are aware of issues that</p> <p>18 were raised earlier last week about the</p> <p>19 collection and transmission of user data via the</p> <p>20 RealJukebox consumer software. As it turned out,</p> <p>21 after we made an initial inquiry it turned out</p> <p>22 that, as our license agreement and program is set</p> <p>23 up right, we were not able to act on that because</p> <p>24 our program governs information that is collected</p> <p>25 through a web site and that was not the kind of</p>	<p style="text-align: right;">Page 236</p> <p>1 I think speaks to what everyone's been talking</p> <p>2 about, relationships with consumers and how that</p> <p>3 pertains to seal programs in general. I think</p> <p>4 one of the things that we work on on a daily</p> <p>5 basis and requires some of the hardest thinking</p> <p>6 that goes on at TRUSTe is looking at these</p> <p>7 relationships that are increasingly growing</p> <p>8 between companies on the Net and are becoming</p> <p>9 increasingly complex.</p> <p>10 I think that our job is to as much as</p> <p>11 possible clarify what those relationships are and</p> <p>12 what their implications are for consumers as it</p> <p>13 pertains to collection and sharing of</p> <p>14 information. We know that companies want to have</p> <p>15 as much as possible seamless and hassle-free</p> <p>16 experiences for their consumers on the web, but</p> <p>17 at the same time we have to assure that there is</p> <p>18 consistent notice that is going on as a consumer</p> <p>19 is traveling through their web experience. And</p> <p>20 we know that they may be going to different URL's</p> <p>21 that may be governed by different privacy</p> <p>22 policies.</p> <p>23 So what we're challenged with is</p> <p>24 making sure that the consumer is clear as their</p> <p>25 taking these travels on the web as to when</p>
<p style="text-align: right;">Page 235</p> <p>1 information that was being transmitted. It was</p> <p>2 not at issue in the RealNetworks instance.</p> <p>3 However, we have taken this as an</p> <p>4 opportunity to look very closely at the issue of</p> <p>5 information that's collected in this manner, and</p> <p>6 this is our opportunity to expand the program to</p> <p>7 include that kind of data collection and</p> <p>8 transmission.</p> <p>9 We do believe that RealNetworks has</p> <p>10 done the right thing. They have taken a lot of</p> <p>11 steps on their own and with TRUSTe to address the</p> <p>12 issue, and we have worked closely with them over</p> <p>13 the last week. We're going to be looking at some</p> <p>14 very specific things that we can work on with</p> <p>15 RealNetworks to assure that our relationship with</p> <p>16 them is good and we can continue to be sure that</p> <p>17 they're doing the right thing and that our</p> <p>18 program is acting optimally.</p> <p>19 I think for the future what we will</p> <p>20 be looking at is a program that deals with this</p> <p>21 kind of consumer software transmitted data, and</p> <p>22 that's going to be our project in the coming</p> <p>23 months. So I just want to get some clarity on</p> <p>24 that as we're going forward.</p> <p>25 The other point that I wanted to make</p>	<p style="text-align: right;">Page 237</p> <p>1 they're in safe space, when they're not, and when</p> <p>2 their privacy policy has changed. So to the</p> <p>3 extent that that mirrors what we're seeing in</p> <p>4 online profiling and to the extent that Dr.</p> <p>5 Westin's findings are an indication of what the</p> <p>6 consumer is looking for is notice and choice, I</p> <p>7 think it's our challenge as we move forward --</p> <p>8 and maybe this is the topic for the next workshop</p> <p>9 -- to figure out what is effective notice.</p> <p>10 It's good to have principles. It's</p> <p>11 very important to have principles and it's a</p> <p>12 wonderful first step, but how do you go about</p> <p>13 implementing those in a very complex kind of</p> <p>14 environment where real estate is very valuable, a</p> <p>15 seamless experience is very valuable?</p> <p>16 So we have to really decide, whose</p> <p>17 responsibility is this? Is it the advertiser's?</p> <p>18 Is it the online business? Is it both? What's</p> <p>19 adequate and effective notice and how do you</p> <p>20 provide for opt-in and opt-out as you're making</p> <p>21 your way on the web?</p> <p>22 MS. BURR: We're going to go to John</p> <p>23 Kamp, then Evan Hendricks.</p> <p>24 MR. KAMP: I don't have anything to</p> <p>25 say.</p>

<p style="text-align: right;">Page 238</p> <p>1 MS. BURR: Thank you.  2 Evan Hendricks.  3 MR. HENDRICKS: Thank you, John.  4 As a matter of clarification, is it  5 my understanding we're only here to ask  6 questions?  7 MS. BURR: I wanted to see if there  8 were any questions about how the program worked.  9 MR. HENDRICKS: Yes, I have one,  10 because \ somebody sitting in this seat at a  11 \Department of Commerce meeting on ratings, when  12 he was giving ratings one to ten, how good is the  13 privacy policy, \, I'd say this one might be up  14 to about a 2.5.  15 One of the issues of fair information  16 practices that everyone agrees on is access to  17 your own information, and I don't see that listed  18 here. So I wanted you to address the access to  19 information.  20 Second of all -- and I have a series  21 of questions, so you might want to jot them down  22 and I'll get them all out of the way so we can  23 move on. Second of all, DoubleClick right now,  24 clearly you're in the business of collecting  25 personally identifiable information. If you're</p>	<p style="text-align: right;">Page 240</p> <p>1 In terms of access, right now we have  2 left it, because there are lots of different  3 business models and not all the companies in NAI  4 gather personally identifiable information. We  5 have not explicitly addressed access at the NAI  6 level. It's something that we're looking at.  7 With regard to non-personally  8 identifiable information, once again, it is not  9 strictly true that access needs to be provided to  10 non-personally identifiable information. That  11 being said, let me comment on why many of the  12 companies do not provide access to non-personally  13 identifiable information-based profiles. The  14 problem is authentication, because we don't know  15 who the consumer is. We have no way of  16 authenticating that a person who's asking for  17 access to a non-personally identifiable profile  18 is in fact the person associated with that  19 profile.  20 Because we've made a commitment to in  21 many cases keep that information secure and not  22 to share it with other people, because we can't  23 authenticate the consumer, we can't display that  24 information. We are very interested, however, in  25 looking at new technologies and new techniques to</p>
<p style="text-align: right;">Page 239</p> <p>1 not, it certainly appears that you are,  2 considering that you've acquired Abacus.  3 So the question in all of our minds -- let  4 me finish the question.  5 It looks like you're in the business  6 of acquiring personally identifiable information.  7 So I wonder, what is your projection? How many  8 files on how many individuals do you expect to  9 gather information? The credit reporting  10 agencies are willing to disclose they have  11 records on 180 million Americans. So considering  12 that your opinion poll that you paid for shows  13 that you got a response that 52 percent of the  14 people support using personally identifiable  15 information for online and offline behavior the  16 tailor ads, so what are your projections on how  17 many individuals you expect to collect  18 information on?  19 MS. WANG: You want to answer the  20 first question?  21 MR. HENDRICKS: The last question is  22 on access to information.  23 MR. JAYE: I would prefer to address  24 the specific question about NAI principles and  25 then I'll hand the mike over.</p>	<p style="text-align: right;">Page 241</p> <p>1 solve this problem, because we would like to  2 provide it if we can find a way to solve the  3 Catch 22 between not knowing who the consumer is  4 and being able to prove that they are who they  5 say they are.  6 MR. MEDINE: Why not just use the  7 consumer's own cookie to give them access to  8 their information?  9 MR. JAYE: The concern is that, once  10 again, cookies are not a strong identification  11 technique. We don't provide typically the  12 profiles out to any third party who has a cookie.  13 So the issue is, if we allow somebody just to  14 enter a cookie and say, show me this profile,  15 there are situations, for example in an office  16 environment, where a co-worker might have easy  17 access to the cookie file of another co-worker.  18 So once again, it's an area that we  19 keep thinking about. We would like to provide it  20 if we can solve the security issues.  21 MS. WANG: To your second question,  22 which has to do with DoubleClick's impending  23 merger of Abacus -- and it's impending because it  24 hasn't happened yet -- we don't own the Abacus  25 database. And it's something that seems to be -- we</p>



<p style="text-align: right;">Page 246</p> <p>1 and saying we understand what we're up to, we  2 plan and we intend to do right. And I suggest  3 that we not worry about creating laws in this  4 area until we have allowed this self-regulation  5 to play itself out.  6 I being a former regulator at the  7 Federal Communications Commission, can tell you  8 that when in 1997 the Federal Trade Commission  9 did its first sweep on privacy policy on sites  10 none of us were particularly surprised to find  11 that under 15 percent of the sites that they  12 visited had privacy policies.  13 But I think more of us were even sort  14 of taken back by how one year later, when there  15 was a similar sweep done after self-regulation  16 had been in place, fully in place for some time,  17 that nearly 80 percent of the sites had privacy  18 policies on them of some type. As a former  19 regulator, I must say that that is something that  20 could not have been achieved by the government.  21 Government regulation mandates could not have  22 sped, gotten the industry there any faster than  23 that. In fact, I don't think it would have gone  24 that fast.  25 So those who are very interested in</p>	<p style="text-align: right;">Page 248</p> <p>1 personally identifiable. But you can't really  2 deny that this information has a very high  3 potential to be potentially identifiable.  4 People have debated back and forth  5 over the course of the day that it may be  6 difficult, maybe, to find the person that this  7 information correlates to, but it can be done.  8 MR. JAYE: It can be done?  9 MR. SHEN: Right.  10 MR. JAYE: If you assume a set of  11 circumstances, at which point we would no longer  12 consider it non-personally identifiable  13 information. In other words, talking about what  14 might happen and what might not happen, there are  15 lots of different possibilities. However, with  16 regard to the information we gather, when we say  17 we gather information and use it in a non-personally  18 identifiable way, that is accurate,  19 that that is how we are going to use it.  20 Now, if our privacy policies change,  21 if we should start to have different practices,  22 there are different ways of interpreting that.  23 But at Engage, at least, the way we would  24 interpret it is the information we gathered under  25 past privacy practices we would need to go out</p>
<p style="text-align: right;">Page 247</p> <p>1 developing laws should recognize that the Federal  2 Trade Commission has taken the right stance in  3 the past by encouraging us to continue to do the  4 kinds of things that the people coming forward  5 with this program have today.  6 MR. MEDINE: Andrew is next. I want  7 to just make it clear to the panel that we're now  8 open to the broad topic of self-regulation.  9 People are free to direct questions, but they can  10 also discuss unrelated issues to the NAI  11 proposal. Andrew.  12 MR. SHEN: I'll go ahead and  13 apologize. I'm going to ask another question  14 about the self-regulatory proposal.  15 VOICE: Move the mike closer.  16 MR. SHEN: I'm sorry. Can everyone  17 hear me?  18 VOICE: No.  19 MR. SHEN: No?  20 MS. BURR: Just talk louder.  21 MR. SHEN: Anyway, a couple people,  22 David and Elizabeth, have said you guys have gone  23 the extra mile to include some partial  24 implementation of fair information practices,  25 even though this information is not necessarily</p>	<p style="text-align: right;">Page 249</p> <p>1 and get proactive consent from a consumer before  2 we started to treat data that we gathered under  3 an assumption that it was non-personally  4 identifiable as personally identifiable.  5 So I take issue with a position that  6 says that there is no such thing as non-personally  7 identifiable, because I think that it  8 holds out the possibility that consumers will not  9 be able to get the advantages out of the  10 Internet, the free services that are advertiser-  11 supported, if we draw a broad brush and say, now  12 anything could be personally identifiable in some  13 circumstances, so let's not create that category  14 for non-personally identifiable information at  15 all.  16 MR. HILL: Just a clarification,  17 Daniel. So are you saying that, does the NAI as  18 a group have a policy on fundamental change of  19 notice? So if you collect data under one  20 practice and then change at a later date, you had  21 mentioned that Engage believes you require  22 consent and an opt-in for that change of  23 practice. Otherwise you have to stay under the  24 previously advertised policy.  25 Does the NAI as a group have a policy</p>

<p style="text-align: right;">Page 250</p> <p>1 on how they approach change of practices, so if  2 they have a merger or an acquisition and it's now  3 in someone's business interest to make it  4 identifiable how would your group suggest dealing  5 with that?  6 MR. JAYE: Well, as David Medine  7 pointed out, when we make a public policy  8 statement his organization certainly has  9 enforcement capabilities if we violate that  10 privacy principle. Now, with regard to changes --  11 MR. HILL: Yes, I'm talking about  12 revision.  13 MR. JAYE: Yes. In terms of revision  14 with regard to prior data collection, that's an  15 area that we have not explicitly called out at  16 this time. What I will say is that this is a  17 process we have gone through over the last, I'd  18 say, about eight or nine months since the initial  19 meetings with the government.  20 There are a number of areas that we  21 will in the coming months as we look to expand  22 the group to include other industry members, we  23 will need to tackle certain issues and we welcome  24 input about particular issues that people think  25 might make a better self-regulatory framework.</p>	<p style="text-align: right;">Page 252</p> <p>1 legal speak that gets put in there by a lot of  2 lawyers, but it's: we reserve the right to  3 change this policy at any time without consent or  4 permission from the user. By agreeing to this  5 policy, you're agreeing to all future privacy  6 policies that this company may issue.  7 That's generally a clause that's in  8 most privacy policies. So I'm asking, is that  9 currently this group's practice, to include it?  10 MS. WANG: I think those members of  11 our group that are members of TRUSTe and other  12 organizations probably have restrictions on what  13 they can say along those lines. Again, I go back  14 to my initial answer, which is that everybody has  15 to comply with general fair information  16 collection practices in how they would view that,  17 and that's really the answer. I think I can't  18 without specifics --  19 MR. MEDINE: Tim has been waiting  20 patiently over here.  21 MS. BURR: And Steve seems to have  22 been pulling the microphone closer.  23 MR. LORDAN: On behalf of the Online  24 Privacy Alliance, I want to applaud the  25 advertising industry for this self-regulatory</p>
<p style="text-align: right;">Page 251</p> <p>1 MR. HILL: Thank you.  2 MS. WANG: I just want to -- you were  3 talking, you say that if notice has been given or  4 choice has been offered and the consumer had done  5 one thing and provided the information, if later  6 on the practice had changed, the answer is -- and  7 it's not an answer that's particular to NAI, it's  8 really an answer particular to fair information  9 collection practices generally -- you need to  10 look at the original notice and see whether or  11 not the new use was contemplated in the original  12 notice, because you had asked the consumer for  13 permission to do a certain thing and if you  14 change that thing or you add to it, then,  15 depending on what that thing is, it could be that  16 you need to go back and provide additional  17 notice.  18 MR. HILL: Just to follow up on that,  19 do most of your guys' privacy policies have the  20 right to change the policy practices without  21 consent or permission currently?  22 MS. WANG: I don't understand the  23 question.  24 MR. HILL: Well, a lot of privacy  25 policies I've seen include -- and I assume it's</p>	<p style="text-align: right;">Page 253</p> <p>1 initiative. It's particularly important and we  2 applaud you. In response to Dan's comment that  3 we look forward to working with you as well, to  4 follow up on what John said with regard to the  5 speed at which self-regulation can work, I think  6 it's remarkable the time it took for this group  7 of companies to come together and put forward  8 this initiative.  9 Lastly, I'd like to ask you, can you  10 comment a little bit further on how you plan to  11 work with your business partners and share your  12 practices with them and how that's going to work  13 as far as notice goes?  14 MS. OAKES: Yes, I'll be happy to  15 answer that question. As an organization, as a  16 group of companies, we individually have  17 participated in solutions that address your  18 question. But as an organization we intend to  19 work with our business partners to put  20 information specifically about the third party  21 ad-serving relationships that they have in their  22 current privacy policy with a link directly  23 either to our individual web sites if there's a  24 one on one relationship or to the NAI web site,  25 so consumers will understand there is a third</p>



Page 254

1 party relationship involved and access to our  
 2 privacy policies as individual companies and as a  
 3 group.  
 4 MS. BURR: We're going to do Steve,  
 5 Jerry, Evan, then Fred. David told me that was  
 6 the right order.  
 7 MR. LUCAS: Thank you.  
 8 I think that no one on this panel  
 9 would deny that today the practice of profiling  
 10 has occurred without any real notice, any of the  
 11 major factors -- notice, choice, access, or  
 12 consent, or the knowledge of consumers for the  
 13 most part. And I think that we too applaud the  
 14 work of this organization.  
 15 But I have some concerns over the  
 16 whole notion of not requiring an opt-in. To me  
 17 an opt-out, if you start with an opt-out and  
 18 information is collected and then later on a  
 19 person decides they don't want that information  
 20 used any more, especially when your privacy  
 21 policy says that we share information with third  
 22 parties, at that point I would argue that an opt-out,  
 23 while it doesn't allow the company to use  
 24 that data any further, you still have a  
 25 proliferation of data.

Page 255

1 MR. JAYE: Steve, could you just  
 2 clarify. Are you talking about PII information?  
 3 MR. LUCAS: Yes.  
 4 MR. JAYE: Okay, but not non-personally  
 5 identifiable information?  
 6 MR. LUCAS: Right. We can get into  
 7 that in a second. But I think that not having  
 8 the consumer opt in first -- I don't see why, if  
 9 we're going to take a positive step, that we  
 10 don't take the whole step and say, let's go to an  
 11 affirmative opt-in at that point as opposed to an  
 12 opt-out. If you take a look at what's  
 13 happening in Europe, that's required as opposed  
 14 to -- an affirmative action as opposed to an opt-out.  
 15 The other thing is, we do, we support  
 16 a self-regulatory model. We believe that a self-  
 17 regulatory model has the potential to be the way  
 18 to go. We think that if the industry doesn't  
 19 step up there may be a need for some legislative  
 20 mandates to establish a framework which we can  
 21 all work on.  
 22 Having said that, we also have  
 23 decided that it's important both to provide consumer  
 24 education as well as the opportunity for  
 25 consumers to be able to go to a site and opt out

Page 256

1 of targeted advertising as well as profiling.  
 2 Today we actually announced the launch of a site  
 3 called Myprivacy.org. The purpose of that site  
 4 is again to provide consumer education, but also  
 5 to provide an opportunity for consumers to  
 6 specifically request not to be targeted, both  
 7 through the use of personally identifiable  
 8 information as well as to be tracked through the  
 9 use of cookies.  
 10 Having said that, we think that all  
 11 these efforts -- we applaud any effort that  
 12 brings the industry closer to a fully  
 13 permissioned model, because we hear all the time  
 14 that the goal of the industry -- in fact, someone  
 15 on the panel said it -- the goal is to send the  
 16 right ad to the right person at the right time  
 17 with the right offer. I think it's time that the  
 18 term "right" is the right of the consumer to  
 19 determine when, where, and how any information  
 20 that's being used, being collected and used --  
 21 they have the ability to control that.  
 22 Having said that, I do have a couple  
 23 of questions. That is, we're seeing a lot more  
 24 of companies out there on the web either  
 25 acquiring companies that have an offline presence

Page 257

1 or we know that there are practices out there  
 2 that sites collect data -- use data that's been  
 3 collected offline. Does your organization plan  
 4 on any disclosure that would require, outside of  
 5 COPPA, which I believe does require some  
 6 disclosure when data is being used from offline  
 7 data sources -- do you plan on disclosing the  
 8 fact that you're using data that's been collected  
 9 from offline sources and that data has been added  
 10 to that profile?  
 11 Without providing the consumer  
 12 access, the consumer has no way of knowing that  
 13 you've created a profile with data that has not  
 14 been collected from the consumer online and data  
 15 that hasn't been permissioned.  
 16 MS. WANG: I guess that's my  
 17 question. Your first question, which had to do  
 18 with consumer choice, and this would be  
 19 DoubleClick specifically.  
 20 MS. BURR: Elizabeth, can you pull  
 21 the mike up.  
 22 MS. WANG: Oh, yes. Thanks, Becky.  
 23 The NAI principle provides for  
 24 consumers to have choice at the time of data  
 25 collection, personally identifiable data

<p style="text-align: right;">Page 258</p> <p>1 collection, and the opportunity to opt out, and  2 you're asking why we would not offer to opt in.  3 Actually, I want to clarify our opt-out, because  4 if at some point a consumer gave me an address in  5 connection with the sweepstakes with the full  6 notice that, oh, we're going to connect offline  7 data to you -- and by the way, in answer to your  8 second question, the answer is yes, DoubleClick  9 would do that, would specify at the point of data  10 collection that that information would be  11 connected, linked with offline data, more data  12 from other sources. So that's the answer to your  13 second question.  14 But in answer to your first question,  15 if later, if I'm the consumer and I signed up, I  16 did not opt out at that point, and then two weeks  17 later it occurs to me, hey, I really didn't want  18 that to happen, you can always come to the  19 DoubleClick site or go back to the site where you  20 originally opted, where you originally provided  21 the information, the sweepstakes site, and get  22 linked to the DoubleClick site and opt out then,  23 and that opt-out would be effective for as long  24 as you have that browser or until you delete your  25 cookie file.</p>	<p style="text-align: right;">Page 260</p> <p>1 category of non-personally identifiable  2 information is the ad delivery data, and that's  3 the data that's used for profiling and targeting,  4 and that we're providing an opt-out for across  5 the network.  6 MR. MEDINE: So, using Elizabeth's  7 example, if I changed my mind and I want to go  8 back, I can opt out of any future use whatsoever  9 of personally identifiable information?  10 MS. WANG: That's correct, yes.  11 MS. BURR: Jerry.  12 MR. CERASALE: Thank you.  13 I wanted to commend NAI for their  14 efforts here. And Lynn, I really was pleased  15 with your statement and I want to make sure I  16 understand it, because I think it agrees with  17 where the DMA is: that the best place for notice  18 is right away and it's really at the initial web  19 site where you go. I guess it's, using a term  20 that's been used here, the publisher.  21 And do I take it that you're going to  22 make efforts, you the NAI are going to make  23 efforts, to ensure that your -- the web sites  24 with whom you work are going to have in their  25 privacy policies a statement that would say: I</p>
<p style="text-align: right;">Page 259</p> <p>1 MR. MEDINE: Can I just ask a  2 clarifying question on that. It wasn't clear at  3 the beginning that the opt-out that applies to  4 personally identifiable information is as broad  5 as the opt-out for non-personally identifiable  6 information, because as I understand it for non-  7 personally identifiable information it's for use,  8 whereas, just to clarify, for personally  9 identifiable information, I thought you could  10 only have a choice over third party transfers but  11 not any control over internal use by your  12 companies.  13 Could you describe if that's the  14 correct interpretation?  15 MR. JAYE: No, that's not correct.  16 The opt-out on PII data, personally identifiable  17 information, is over all use. On non-personally  18 identifiable information there are two  19 categories. There's a category that's  20 effectively the infrastructure of the web. The  21 infrastructure of the web requires us to be able  22 to, for example, be able to report on reach,  23 frequency numbers, etcetera. So we cannot  24 provide an opt-out to that.  25 In that category or the second sub-</p>	<p style="text-align: right;">Page 261</p> <p>1 have an agreement with XYZ company that can  2 collect information and have a hot link to your  3 privacy policy, so that the consumer would then  4 know what the web site's policy is and then what  5 your policy is, so you can then establish the  6 relationship there with the consumer to do the  7 opt-out?  8 MS. OAKES: Couldn't have said it  9 better myself, absolutely correct, and we look  10 forward to working with your organization to make  11 that happen.  12 MR. CERASALE: And then a comment on  13 Austin's question. It's my view if you get a  14 change, at least it's the view I think of the DMA  15 -- and I'll get a pink slip tomorrow if that's  16 not true -- the view of the DMA is if you change  17 your privacy policy, information that you  18 collected under the old privacy policy, and then  19 try and use that old information in your new  20 privacy policy, which has a very material  21 difference, I think that subjects you, that  22 company, to FTC review, because you collected  23 information under one pretense and then start to  24 use it under another pretense, and you have to  25 somehow give notice back to change that.</p>



<p style="text-align: right;">Page 266</p> <p>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</p>	<p style="text-align: right;">Page 268</p> <p>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</p>
<p style="text-align: right;">Page 267</p> <p>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?</p>	<p style="text-align: right;">Page 269</p> <p>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</p>

<p style="text-align: right;">Page 270</p> <p>1 the information that I heard in the last half an 2 hour.</p> <p>3 I think that, first of all, TRUSTe 4 requires compliance with fair information 5 practices and we would welcome working with these 6 companies to the extent that we think these 7 companies are willing to work toward fair 8 information practices. I haven't looked closely 9 at the provisions that you've announced, but that 10 would be very important.</p> <p>11 I think that, to the extent we could 12 work with them, at this point, unless we look at 13 your program and decide something else would be 14 necessary, that this would be such a special 15 case, I think that NAI would probably fall under 16 the same rules that the rest of the licensees 17 fall under where we have a dispute resolution 18 process, that there are inquiries that we can 19 make with companies when there are questions 20 raised by consumers, that we can raise the level 21 of that inquiry of things aren't resolved, that 22 we can require audits. We have the ability to 23 refer to the FTC and we do ultimately have the 24 possibility to revoke a seal if that's necessary. 25 I have to reinforce, and I think that</p>	<p style="text-align: right;">Page 272</p> <p>1 companies who are involved in the fast pace of 2 change can kind of work at doing their best to 3 meet fair information practices and setting up 4 standards for future activities with new 5 technologies.</p> <p>6 MR. HENDRICKS: I don't want to 7 criminalize it. I just want to create a civil 8 right of action so that if their wishes aren't 9 respected they can do something about it.</p> <p>10 MR. CATE: Well, I at this late 11 moment would just like to briefly return to the 12 broader set of issues, although it's difficult to 13 do that without some reference to the discussion 14 that's already been had. So let me be very 15 brief.</p> <p>16 First, self-regulation seems like -- 17 it's fairly unremarkable to say that it's a good 18 thing. That is, without regard to whether a 19 specific piece of self-regulation is, that it's a 20 good thing because it can deliver, backed up by 21 effective enforcement, it can deliver very 22 effective privacy protection. It can be far more 23 specific. It can be far more easily changed in 24 response to changing conditions than, for 25 example, the 60 years it takes Congress to enact</p>
<p style="text-align: right;">Page 271</p> <p>1 the incidents of the last week have made clear, 2 that we're living and we're working in an 3 environment that's evolving and we have to keep 4 evolving this program. So I think that this may 5 well just present another challenge where that's 6 what we have to do.</p> <p>7 MR. ZINMAN: Can I respond to just 8 one of those comments. Just one of Evan's 9 comments about after the RealJukebox thing I 10 think happened. I think we weren't in the 11 offices of RealNetwork, so we can't imagine the 12 scurry and fury that went around there when they 13 found out this was happening, but I do know, 14 being another company in the industry, when you 15 see something like that happen you respond 16 immediately by taking a look at your own 17 practices.</p> <p>18 So I'd say that there was a lot of 19 response that happened within the industry, 20 people making sure that they weren't making any 21 similar mistakes. This is part of the dynamic of 22 a very fast-growing industry. So the challenge 23 is, do we want to criminalize all this behavior 24 or what we need to do is we need to work in a 25 self-regulatory environment where all the</p>	<p style="text-align: right;">Page 273</p> <p>1 a bill or even the time it takes the FTC to act 2 on a matter. So the self-regulatory approach has 3 a tremendous amount to recommend it.</p> <p>4 The second point, of course, goes 5 back really in some ways to the last panel and to 6 the issues more specifically dealing with 7 profiling, which is this issue of treating non- 8 personally identifiable information as having 9 this privacy interest.</p> <p>10 The complexity or the oddity of this 11 is highlighted by the very problem of how do you 12 opt out of its use. I want to tell you not to 13 use information that's not about me or that you 14 don't know if it's about me, and you said, well, 15 we'll put a cookie on your computer. Well, again 16 we're back to where I was in the last panel, 17 which is now my computer has a privacy interest 18 and it's opting out, but if I use my laptop that 19 opt-out is no good.</p> <p>20 This at least raises one potential 21 problem and it's not a novel problem in self-regulation, 22 and that is it's important that it 23 not create confusion. In other words, the goal 24 of self-regulation presumably is to be clear and 25 direct and let people know what they are opting</p>

<p style="text-align: right;">Page 274</p> <p>1 in or opting out of or what have you.  2 This is one of the specific points I  3 would raise with this, to be very clear that if  4 we're letting people -- if we're giving the  5 impression that you can opt out of non-personal  6 information, in fact we don't know realistically  7 what that means.  8 The point was mentioned earlier, opt-in  9 versus opt-out, whether -- I think it was you -- whether  10 this should be an opt-in  11 situation. I just can't let the sort of  12 reference pass without at least noting it's not  13 just six of one or half a dozen of the other.  14 The ramifications of one versus the other are  15 very significant, and even places like the EU,  16 which you mentioned, which have clear opt-in laws  17 on the books, we see increasingly using opt-out  18 as the de facto enforcement mechanisms, the way  19 in which they work.  20 This is particularly true, say, for  21 HR data in Europe. We have not see data  22 protection commissioners saying you have to go to  23 every employee and get them to opt in; they can  24 continue working there but not opt into this  25 system. What we have seen is a requirement that</p>	<p style="text-align: right;">Page 276</p> <p>1 information practices. I think it's important to  2 look at fair information practices not as a goal,  3 not as something we should aspire to reach, but  4 as something that consumers should have now.  5 We're talking about information collected from  6 individuals and, whether companies believe it or  7 not, this is information that they may want  8 control over.  9 I'm not going to refer to Dr.  10 Westin's survey. I'm actually going to refer to  11 a different survey done by Georgia Tech. I have  12 the results from 1997. Sorry I don't have the  13 more current ones, but this is based on more than  14 14,000 respondents, which I believe Dr. Westin's  15 survey was based on about 400.  16 It said that 87 percent of the users  17 believe they should have complete control over  18 the demographic data. Now, I can attest that  19 complete control follows notice, consent, access,  20 and security, not the sort of stripped-down  21 measures that we often see, like notice and opt-out. So  22 I think it's important to keep that in  23 mind, that consumers want more and the government  24 has the ability to provide it to them and that we  25 shouldn't rely on self-regulation as the only</p>
<p style="text-align: right;">Page 275</p> <p>1 you give notice and then give them a chance to  2 opt out. Even though the law says the opposite,  3 in practice opt-in just doesn't work in those  4 situations. That's one of the reasons, of  5 course, why we use opt-out almost exclusively,  6 with the exception for example of dealing with  7 children.  8 Finally, though, and very much on  9 point with the panel, one has to wonder to some  10 extent if technology isn't about to put a lot of  11 these concerns to rest. You know, we saw the  12 presentation earlier. We all know about other  13 types of technologies. We see new technologies  14 debuted all the time which make it increasingly  15 easy and affordable to browse the Internet wholly  16 anonymous, anonymous in every sense of the word.  17 I think as we think about self-regulation  18 one of the components that necessarily  19 has to be thrown in here is thinking about the  20 availability of these technological solutions as  21 well.  22 Thank you.  23 MS. BURR: Andrew.  24 MR. SHEN: I just have a comment  25 about regulation in general and about fair</p>	<p style="text-align: right;">Page 277</p> <p>1 model out there.  2 MR. JAYE: Could I make just one  3 comment? If we're going to bandy surveys about,  4 there's a very interesting result that Professor  5 Westin presented in Cambridge at the U.K. Privacy  6 Laws in Business Conference this summer. He  7 referred to it briefly this afternoon. But one  8 of the interesting results that came out in his  9 presentation was the fact that consumers in the  10 U.K., even though they have regulation, felt that  11 consumers in the United States had better privacy  12 protection than they did.  13 So the interesting anecdote there is  14 that regulation alone isn't a solution, either.  15 I think that self-regulatory frameworks are  16 absolutely essential. We believe at NAI that  17 this industry is so fast-paced, so moving, the  18 things we're talking about now almost no one  19 understood three or four years ago.  20 I think it would be very difficult  21 for regulations to be able to be enacted that  22 wouldn't necessarily hamper the growth of  23 electronic commerce and advertising on the  24 Internet.  25 MR. SHEN: Can I respond to that very</p>

Page 278

1 quickly. I hear that argument a lot, that the  
 2 Internet is moving very fast. We hear the phrase  
 3 "Internet time" all the time, that it's  
 4 impossible for the government to regulate on  
 5 specific issues, like online profiling and the  
 6 collection of information. But the fact is that  
 7 fair information practices are never going to  
 8 change. These are the cornerstones for the  
 9 ability of the consumer to control their  
 10 information -- notice, access, security, consent.  
 11 I mean, these are never going to be  
 12 changed, and these can be enshrined into law.  
 13 The FTC recently did a very good job on the  
 14 Children's Online Privacy Protection Act. It was  
 15 a very complex issue. They're dealing with how  
 16 parents should be involved in the process of  
 17 giving up the information on their children, but  
 18 the FTC did a very good job and it did it within  
 19 one year. So it is possible to do that and do it  
 20 effectively.  
 21 MS. BURR: Steve and then Jerry.  
 22 MR. LUCAS: Just two quick comments.  
 23 We haven't talked much about the economics of  
 24 what we're doing from the perspective that we all  
 25 know that click-throughs are dropping through the

Page 279

1 floor. But yet we see example after example of,  
 2 when permission is asked, the acquisition rates  
 3 dramatically increase. People like Seth Goten in  
 4 his book talk about the fact that when he asked  
 5 permission from his consumers his acquisition  
 6 rate went from less than 2 percent to over 20 and  
 7 his cost of acquiring an individual name, if you  
 8 want to call it that, went, in the case of one of  
 9 the Wall Street firms, from \$300 to \$25.  
 10 So again, I just want to stress the  
 11 notion that there is clear evidence that  
 12 permissioning works from our industry  
 13 perspective.  
 14 Now, we talk about that cookies are  
 15 an essential fabric for the web, but they're an  
 16 essential fabric for maybe certain things and in  
 17 certain people's views. I would argue that  
 18 cookies are an essential fabric for advertisers.  
 19 They are not required for the web to function as  
 20 the web. That's first of all.  
 21 Second of all, I would also argue  
 22 that, even though we're looking at, say, hardware  
 23 negotiations with the EU and if those go through,  
 24 if the fair information practices agreed on don't  
 25 include the idea of an affirmative opt-in and

Page 280

1 don't include the notion of specific and  
 2 unambiguous consent and don't include the notion  
 3 of access, we still have countries outside of the  
 4 EU that have very strict data privacy laws.  
 5 While I'm not suggesting that we fold  
 6 up the tent and agree with every data protection  
 7 law that's out there, most of the other countries  
 8 have similar types of fair information practices.  
 9 There's over \$500 billion worth of e-commerce  
 10 that's at stake here between ourselves and  
 11 Europe, and at some point in time -- we can put  
 12 it off for as long as we want to and we can put  
 13 all the hope we want into safe harbor, and I have  
 14 all the confidence in the world that we'll be  
 15 able to solve this issue.  
 16 But if we don't, at some point we're  
 17 going to have to step up to these issues.  
 18 They're not going to go away.  
 19 MR. MEDINE: We have time for just a  
 20 few more comments, but I know you wanted to  
 21 respond on information-based marketing.  
 22 MR. ZINMAN: That's right. Just  
 23 quickly, I have no doubt that advertisers will do  
 24 whatever is necessary to improve the returns they  
 25 get from advertising. So I don't think we should

Page 281

1 be debating the effectiveness of one method of  
 2 advertising versus another, because advertisers  
 3 are going to direct their money at the one that's  
 4 most effective.  
 5 So if you're right and if we have  
 6 another panel, next time everyone will be doing  
 7 permission-based marketing.  
 8 MS. BURR: Jerry.  
 9 MR. CERASALE: The only thing, don't  
 10 force a specific business model. I think that  
 11 the real key here is to give American consumers  
 12 the knowledge and they're going to make a smart  
 13 choice. They're going to vote with their feet,  
 14 or in this case they're going to vote with their  
 15 mouse clicks.  
 16 That's the real key here, is to have  
 17 some faith in the American public when you give  
 18 them knowledge and you give them choice that  
 19 they're going to make, they're going to make  
 20 their decision. They're going to vote and  
 21 companies are going to fail that don't provide  
 22 what they need.  
 23 I think that's really the important  
 24 thing here, is to try and make sure that we give  
 25 them notice. The problem we had here today is

<p style="text-align: right;">Page 282</p> <p>1 that people didn't know what was there. It  2 wasn't transparent. It wasn't a relationship.  3 So create it and let the marketplace go and put  4 the faith back in the American consumer.  5 MR. KAMP: Jerry just made about half  6 of my points just there. I agree with him, but I  7 also think that one of the things that's going on  8 here is this is an awfully complicated system.  9 Computers for most of us are very fragile devices  10 that crash on us and make us crazy, and one of  11 the ways in which we get to where Jerry is is we  12 make these things a lot simpler than they are  13 today.  14 I think the fact that our law  15 professor was confused this morning doesn't  16 surprise me, and we have to get to that  17 simplicity in this area so that consumers can  18 understand the choices that they're able to make.  19 MS. BURR: The last word.  20 MR. HILL: Just in response to  21 Jerry's comments, I think one of the things we've  22 heard come out of this is this idea that a lot of  23 the privacy initiatives are anti-marketing. I  24 think that nothing could be further from the  25 truth. I know my company's going to spend \$20</p>	<p style="text-align: right;">Page 284</p> <p>1 the auction block ready to be sold to someone.  2 And if customers don't have a way to say, you  3 know what, I never agreed to engage in business  4 with this company, then I think we have a problem  5 with our framework.  6 So I think there are other options.  7 MR. MEDINE: Our apologies to Cookie  8 No. 247. We weren't able to get to your  9 question.  10 MS. BURR: That's emblematic of the  11 day. This has been a very interesting panel and  12 a very interesting day. Clearly, our work in  13 this area is beginning and the companies here  14 have told us that they are continuing to work and  15 want input from the people around the table, and  16 I imagine around the room as well, on the work  17 that they are doing.  18 So thank you for coming forward, and  19 we look forward to working with you on that.  20 We are going to go to some wrap-up  21 comments, but before we do, since everybody likes  22 to scoot out at the end, I'm going to give a few  23 well-deserved thank-you's before we do that.  24 This truly has been a team effort of the Federal  25 Trade Commission and the Department of Commerce.</p>
<p style="text-align: right;">Page 283</p> <p>1 million this year on advertising. Most of that  2 or a large percentage of that will be online.  3 For us, we're looking for partners in  4 our advertising initiatives that can meet the  5 same standard of customer relationship that we  6 have for ourselves. And it's proving somewhat  7 difficult, but there is a growth. This group  8 does not represent all the advertising  9 initiatives. There are groups like Yesmail,  10 Yoyodyne, Alladvantage -- different initiatives  11 that have consent, permission-based.  12 One of the problems with the sole  13 economic "let's let it work itself out" is what  14 we saw with Firefly. Firefly came in and said:  15 We're going to build consent tools, permission  16 tools. And at the end of the day, whether  17 through execution or bad timing, Firefly went  18 almost bankrupt. That technology was acquired by  19 Microsoft and has been turned into the number one  20 profiling tool on the Net.  21 So that's the danger, is if we set up  22 these profiles and there's no redress for  23 consumers, when the companies that do fail  24 because profiling wasn't in the best interest of  25 customers, you've now got 80 million profiles on</p>	<p style="text-align: right;">Page 285</p> <p>1 Whoever said federal agencies don't work together  2 well was wrong.  3 So I'd like to thank -- and this is  4 for both David and myself -- people that we've  5 worked with who have been instrumental and but  6 for their hard work this event would not have  7 happened: Martha Landesberg at the FTC, Laura  8 Mozzarella at the FTC; Wendy Later, Sandra  9 Leonsis, and Christina Speck at NTIA; Don  10 Friedkin and Mary Street at the Office of the  11 General Counsel here at the Department of  12 Commerce. And we've seen a lot of AV guys  13 running around. The only one I recognized was  14 Hershel Gelman, but whoever all the rest of you  15 are, you deserve our thanks. Thank you very much  16 to all those people.  17 We spent a lot of time getting up to  18 speed on this technology and getting all of the  19 various viewpoints that we heard around the  20 table. So to all those people who worked on it,  21 thank you very much.  22 (Applause.)  23 MR. MEDINE: We'd like to ask the  24 panelists to keep their seats, and we'd like to  25 invite up to the podium Jody Bernstein, who is</p>



<p style="text-align: right;">Page 286</p> <p>1 the Director of the Bureau of Protection of the  2 Federal Trade Commission, and Andy Pincus, who is  3 the General Counsel of the Commerce Department,  4 to make their closing remarks.  5 As they're walking up, I will briefly  6 introduce Andy. He's the General Counsel, again,  7 at the U.S. Department of Commerce, and as  8 General Counsel he is the chief legal adviser for  9 the Department. Beyond his legal  10 responsibilities, he also serves as the senior  11 policy adviser for the Secretary and the  12 Department on a broad range of domestic and  13 international issues, including electronic  14 commerce, international trade, banging the  15 microphone, and telecommunications, intellectual  16 property rights, environmental issues, export  17 controls, and technology.  18 REMARKS OF ANDREW J. PINCUS, GENERAL COUNSEL,  19 U.S. DEPARTMENT OF COMMERCE  20 MR. PINCUS: Thank you, David.  21 First of all, I want to reinforce my  22 thanks, not just to the people in the two  23 agencies, but all the people who participated on  24 panels today and the people who came and listened  25 and participated in the audience. I think this</p>	<p style="text-align: right;">Page 288</p> <p>1 obviously care a lot about the growth of  2 electronic commerce. It's a driver of our  3 economy and the President has asked us to look  4 over that issue. But we recognize that that  5 won't happen if consumers don't feel that this is  6 a safe environment in which to do business. So  7 protecting privacy in all its manifestations is  8 critical to that.  9 Just as important, the FTC realizes  10 that in its role as the chief consumer protector  11 of the government, protecting privacy is a  12 critical element of that mission. So it's really  13 an instance where both of our missions point us  14 in the same direction and have really caused us,  15 not just in this endeavor but in the whole  16 privacy issues, to really be working together in  17 lockstep, and it's something that we're very  18 proud of.  19 I don't want to rehash everything  20 that's happened today. It seems to me, as I  21 said, a lot got put on the table and there's a  22 lot for everyone to digest. I think it's also  23 important to remember, as with anything in the  24 world of e-commerce, we're dealing not just with  25 our own domestic situation, we're dealing with a</p>
<p style="text-align: right;">Page 287</p> <p>1 workshop did just what we hoped it would do,  2 which is to focus attention on an issue, a  3 privacy issue that we feel has gotten less  4 attention than it should, to put out there the  5 business community's views, the privacy  6 community's views, some of the technology that's  7 out there, and really to begin a conversation  8 about what to do about it that was helpfully  9 kicked off by some of the initiatives that were  10 announced here by the business community.  11 But that's not the end of it, that's  12 the beginning; and we obviously hope that this  13 dialogue will continue and will result, as other  14 dialogues have that started in workshops such as  15 this, with an approach to protecting privacy that  16 will work for the growth of the Internet and that  17 will also work to provide real and concrete  18 protection to the privacy of consumers.  19 I guess Becky kiddingly said federal  20 agencies don't often cooperate, but we have a  21 very good cooperative relationship with the FTC.  22 I think the reason for that is that both of us  23 realize that addressing this issue in a real and  24 concrete way is critical to both of our missions.  25 For the Department of Commerce, we</p>	<p style="text-align: right;">Page 289</p> <p>1 medium that's international. So to the extent we  2 can devise solutions that work in the cross-border world,  3 we're going to devise solutions  4 that have a much better opportunity of  5 effectively protecting consumers' privacy.  6 That's one of the reasons that we  7 have concluded that self-regulation is an  8 important and effective way to go, because it  9 provides consumers with an ability to protect  10 themselves, not just domestically with respect to  11 laws that may or may not apply to any particular  12 web site, since there's no way to be sure exactly  13 what laws govern any particular web site, but  14 through seal programs and other mechanisms,  15 visual cues, give consumers a way to protect  16 themselves. So we think that's an important  17 methodology to pursue, with the caveat that that  18 protection has to be real.  19 So we look forward to participating  20 with all of you in the continuing discussions  21 both of this issue and the other issues relating  22 to privacy.  23 Now I introduce Jody Bernstein, who  24 is, as David said, our colleague in this  25 endeavor. Jodie is a true path-breaker in public</p>

<p style="text-align: right;">Page 290</p> <p>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.)  12 REMARKS OF JODIE BERNSTEIN, DIRECTOR,  13 BUREAU OF CONSUMER PROTECTION,  14 FEDERAL TRADE COMMISSION  15 MS. BERNSTEIN: Thank you very much,  16 Andy, for a very nice introduction. If I may say  17 also, as others have, what a pleasure it has been  18 to work with you and others at the Department of  19 Commerce on this very, very significant issue. I  20 do thank all of you participants, both on the  21 panels and in the audience as well, because I  22 think, once again, what we set out to do here  23 today we may have achieved. That is to open up a  24 process so that all of us could better understand  25 a very complex issue.</p>	<p style="text-align: right;">Page 292</p> <p>1 the law was to put parents in charge of  2 protecting their own children, they were  3 immediately comfortable with what was happening  4 to them. I think the same thing is probably at  5 issue in this instance.  6 A lot was accomplished today, I  7 think. A lot of sort of consensus issues were  8 addressed that will serve us all well. We were,  9 I think, to be encouraged by DMA and NAI in  10 connection with an effort to achieve what's been  11 achieved in other areas, and that is a self-regulatory  12 program that addresses what the  13 problems were today.  14 I'm looking over at Evan because I  15 never agree with him, either, and he always has --  16 luckily, they always give me a chance after  17 Evan has attacked the FTC to at least be on the  18 platform. In that context, I would just add to  19 Evan and others that, while the FTC has been very  20 supportive of self-regulatory programs, it is not  21 without the FTC's commitment to law enforcement.  22 Those things are coupled together in this area  23 and in other areas, and I think that is in my  24 judgment and I think in others why self-regulation has  25 achieved the amount of</p>
<p style="text-align: right;">Page 291</p> <p>1 Now, I really never dreamed that I  2 would stand here before any audience and say, you  3 know, I agree with Jerry Cerasale about these one  4 or two things. I never agree with Jerry Cerasale  5 at these things, so there has to be a certain  6 uniqueness about any given one of these sessions  7 that we hold.  8 But when Jerry said, and others have  9 said it as well, that the real problem here I  10 think that we were addressing today is no one  11 knew that this was going on, nobody knew -- I  12 mean, us ordinary people didn't know what was  13 happening. And at least from our experience,  14 whenever Americans find out that something is  15 affecting them that they know absolutely nothing  16 about, whether they had any ability to control it  17 or not, they get very upset and they want to know  18 what's going to be done about it and do they have  19 a way of controlling it.  20 I noted that in connection with the  21 children's statute and the rulemaking that,  22 happily, someone did point out that we did it in  23 one year because it needed to be done, and as  24 soon as parents understood that the theory behind  25 the law and the way we were going to implement</p>	<p style="text-align: right;">Page 293</p> <p>1 credibility, particularly in the online  2 environment, that it has.  3 I would make one other point that I  4 don't think had sufficient stress today, and that  5 is that your program also included an education  6 component. We also believe that that's an  7 essential element of achieving an overall  8 comprehensive program that can -- and we've all  9 not seen all the details of everything -- can be  10 a successful one.  11 I think the key word is  12 "transparency," and if we all keep that in mind -- and I  13 think everyone has spoken for that  14 concept -- that we will have moved a long way.  15 We look forward to watching as this  16 program develops as you get more experience with  17 it, as we all get more experience with it. In  18 the end, I think that this forum which the  19 Department and the FTC sponsored will have  20 achieved at least an initial beginning of  21 achieving what has been a very complex, very  22 complex set of issues.  23 I would only add one more thing, and  24 that is that when we talk about notice and  25 opportunity to opt out, among the words that I</p>

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