FEDERAL TRADE COMMISSION

EHAVIORAL ADVERTISING

TRACKING, TARGETING & TECHNOLOGY

Thursday, November 1, 2007

9:00 a.m. to 5:00 p.m.

United States Federal Trade Commission

Conference Center

601 New Jersey Avenue, N.W.

Washington, D.C.

Reported by: Robin E. Boggess

TABLE OF CONTENTS

P R O C E E D I N G S

- - - - -

WELCOME AND INTRODUCTORY REMARKS

MS. BRANDENBURG: Good morning, and welcome to the Ehavioral Town Hall. We're delighted to welcome you to what promises to be a dynamic and informative two-day town hall.

Before we begin, I have a few announcements. There will be time at the end of nearly every session to ask questions. Two microphones will be set up in the aisles and the moderator will indicate when it's time for audience questions. If you'd like to ask a question, you can line up at that time. If you don't mind, please state your name and group affiliation, if any, to assist the court reporter.

Keep your questions short and to the point to allow everybody to have an opportunity to ask their questions.

If you'd like to submit comments on the issues raised in the town hall, you may post a comment on the town hall website, which you can find at www.ftc.gov. The comment deadline is November 16th of this year.

The town hall is being videotaped and will be available for viewing at the FTC website in the future. All PowerPoint presentations can also be downloaded from

that site.

We have a few important housekeeping notes. First, a few reminders about security. If you leave the building for lunch or at any time, you'll need to be rescreened through security to reenter, and for security reasons, please wear your name tags at all times. Of course, if you notice anything suspicious, report it to the guards in the lobby.

You'll find bios in your packets and information on local restaurants for lunch can be found outside on the tables at the check-in.

A few additional remarks, for everyone's enjoyment and safety, right on cue, please turn off or set to vibrate your cell phones, and do not use your cell phones in -- even outside here in the conference center because it can be disruptive for those participating in here. You're more than welcome to use your cell phones out in the lobby where you first came in.

Second, and importantly, the restrooms are located across the lobby beyond the elevators and fire exits are located through the main doors of the front of the building onto New Jersey Avenue and through the pantry area, which is directly behind us, to the G Street corridor and out G Street. In the event of an emergency, please proceed to the building diagonally across from

Massachusetts Avenue.

Finally, I would like to thank the Interactive Advertising Bureau for providing coffee and bagels this morning that I know we've all appreciated.

Now it's time for a special welcome message from Chairman Majoras.

CHAIRMAN MAJORAS: Good morning, and thank you for coming. I am sorry that I cannot welcome you in person to the Federal Trade Commission's Town Hall examining behavioral advertising and consumer protection. I am grateful to everyone who has agreed to participate in this important two-day forum.

We have convened this town hall as a follow-on to our Tech-Ade hearings held last fall to explore in detail those consumer protection issues that behavioral advertising presents.

For more than a decade, the FTC has been committed to protecting consumer privacy and identity, both online and offline. We have used our full range of law enforcement authority, encouraged and supported industry self-regulation, and conducted extensive consumer and business education programs relating to privacy and security.

In the past year, we have considered closely and internally debated the several petitions and

complaints about behavioral advertising that we have received, and FTC staff has met with and interviewed scores of consumer groups, companies and technologists to better understand the advertising technology and the legal and policy questions its use implicates.

Over the past decade, our methods of communicating with one another have changed fundamentally. Thus it is not surprising that we are at a moment in time when the advertising industry is transforming itself, forming new combinations, developing new strategies, simply exploding with activity. Online companies of all types are moving into the advertising space or expanding their presence so as to generate revenue and enhance and complement the many other services provided by their businesses.

Today and tomorrow, as we look at developments in online advertising, we will be exploring the types of information that companies collect about consumers as they travel across the Internet, whether the information collected is anonymous or personally identifiable, how this information is used and shared, what consumers understand about the collection of information online, and finally, whether these practices are resulting in consumer harm and, if so, how this should be addressed.

We recognize that advertising brings many

benefits enabling consumers to make informed choices, as well as providing free online content and a level of personalization that many consumers enjoy.

We also recognize that there are legitimate concerns about whether consumers are aware that their activities are being tracked online and about whether data, once stored and combined with other data, could somehow find its way into the wrong hands.

We are here to learn more about these issues, engage in a robust discussion about current and future developments, and debate the ramifications of those developments in this marketplace.

Again, thank you for your participation and enjoy the forum.

(Applause)

MS. BRANDENBURG: Now I would like to introduce Lydia Parnes, the Director of the Bureau of Consumer Protection for the Federal Trade Commission.

(Applause)

MS. PARNES: Thank you. Thank you all so much. It is really a pleasure for me to be here to welcome you all to the FTC for our Town Hall on Behavioral Advertising. I'd especially like to thank the panelists who are with us today and tomorrow for the time that they have given us and all of their efforts to share their

insights and expertise on behavioral advertising.

Those of you who have been working on privacy issues for the last decade are experiencing a little bit of deja vu, I would imagine, this morning. As many of you know, the Commission examined behavioral advertising, which we then called online profiling, at a public workshop that we held in 1999. Then, as now, we described the practice as the collection of information about a consumer online, including searches the consumer conducts, the webpages visited, the content viewed, geographical information, lifestyle or preference information, all for use in delivering targeted advertising to that consumer.

Because the consumer's own activities are used to target the advertising, the ads are presumed to reflect that consumer's interests and thus increase the effectiveness of the advertising.

More recently, we discussed behavioral advertising at last year's Tech-Ade hearings, which examined the key technological and business developments that are expected to shape consumers' experiences in the coming ten years. What we learned at Tech-Ade, and in preparing for this event today, is that the advertising market has changed dramatically since our earlier workshop in 1999 and that the practices involved in

behavioral advertising have changed along with it.

First, behavioral advertising has become more prevalent and it's expected to become even more widely used in the coming years.

Second, marketers are seeking to expand substantially the information they collect and analyze to increase the precision of their behavioral advertising.

Third, the industry has seen a recent flurry of consolidation, resulting in more consumer information in fewer hands.

At the Tech-Ade hearings, panelists also debated the costs and benefits of behavioral advertising. Some panelists stated that consumers benefit from the practice because the ads they receive are more relevant to their interests. That's a good thing. If you're shopping for a tennis racket, for example, isn't it nice to get an ad showing you where you can buy a tennis racket, or maybe even a coupon giving you a discount for that racket, or maybe a discounted vacation to a tennis resort. Those are all good things.

Others express concern about the increasing collection of consumer information online and the use of this information to develop comprehensive consumer profiles that can be stored indefinitely.

These issues were underscored by several

letters we received from consumer advocates and others expressing their concerns about the effects of behavioral advertising on consumers.

We decided that we really needed to learn more and, so, here we are. Over the next two days, we anticipate some terrific discussions which we've organized into nine panels. Our first panel will provide an overview of behavioral advertising from various perspectives. We have a technologist, a privacy advocate, an industry representative and a representative of the leading self-regulatory organization.

In the second session, we'll hear from industry representatives and outside analysts about current business models, as well as technological and other changes in recent years.

The third panel will present survey data related to consumers' knowledge and attitudes about the collection of data online and the use of cookies, a primary method for collecting data.

After lunch today, the fourth and fifth panels will address the nuts and bolts of behavioral advertising, what type of data is collected, how the data is used, who has access to it, and whether and how the data is secured.

Tomorrow, we'll begin the day by examining what

companies disclose to consumers about behavioral advertising and whether these disclosures are an effective way of communicating with consumers about the practice.

Then, we have a nice little surprise on the second panel, a presentation of the results of a YouTube contest for the best short video explaining what cookies are and how they're used for advertising online. The concept was developed and sponsored independently by Esther Dyson and the Harvard Berkman Center.

During the session, the judges will show the top five videos, discuss the relative merits of each, and select the winning video, and members of the audience will also have a chance to vote for their favorites. We hope that that's a really fun break.

After lunch tomorrow, we'll turn to the regulatory landscape. We'll hear about regulatory and self-regulatory measures governing behavioral advertising, both here and abroad, including the status of the principles put forward by the National Advertising Initiative.

And, finally, our last panel will look to the future. It will explore anticipated changes in the behavioral advertising space and whether and how behavioral advertising is being used across different

technologies.

Before I close, I want to address one issue that I suspect has crossed the minds of a fair number of people here, why a town hall? Why not the good old familiar FTC public workshop? Well, by town hall, we want to signal that we expect a lot of discussion at these two days. On almost every panel, we've left time at the end for audience participation, and because this event really is -- you know, the people sitting here, you are all the who's who in privacy. So, we expect this debate to really be a very active, robust and informative debate for us.

There's just one more thing I'd like to know. As I'm sure you all realize there is a tremendous amount of work that goes into preparing for an event like this and I'd like to acknowledge the folks at the FTC who put this together.

From the Division of Privacy and Identity Protection, there's Lori Garrison, Peder Magee, Jamie Hine, Stacey Brandenburg, Assistant Director Jessica Rich and Associate Director Joel Winston.

From the Division of Advertising Practices, Mamie Kresses, Michelle Rosenthal, Assistant Director Rick Quaresima, Associate Director Mary Engel.

From the Division of Consumer and Business

Education, Callie Ward, Colin Conerton from our Honors Paralegal Program, and Eileen Harrington, who is a Deputy Director in BCP, also played a large role in this.

I want to thank all of you for your absolutely terrific work.

(Applause)

MS. PARNES: The next two days promise to be an education for all of us, filled with spirited debate and constructive dialogue. Thank you all again for coming. And, now, I'm going to turn this over to Lori Garrison for our terrific first panel.

(Applause)

SESSION 1: OVERVIEW OF BEHAVIORAL ADVERTISING

MS. GARRISON: Thank you very much, Lydia, and good morning, everyone, welcome. The first session today to open our town hall is designed to set the stage for our two-day conversation. As Lydia said, we'll have a technology presentation to simply and clearly show how generically ads are delivered online. It's not meant to be comprehensive, but it's meant to kind of set the stage so that we have a common understanding of how this works.

Following that, we're going to have three perspectives on the issues that we're exploring in this town hall.

So, to begin this session, it is my pleasure to introduce Richard Smith, a technologist who will walk us lightly through the online advertising world. Richard hails from that great land to the north, Red Sox nation. Welcome, Richard.

(Applause)

MR. SMITH: Thanks for that nice introduction here. As Lori said, the FTC invited me to come in here to give a general technical overview of the Internet advertising technology, you know, how we see ads on the webpages and the websites that we go to, and my goal is to give sort of a broad overview, not at 50,000 feet but more maybe down on the 5,000 feet level. So, there will

be some technology discussion in here.

I certainly expect a lot of people in the room will know a lot of this stuff, but I hope everybody will learn a little bit. I certainly learned a few things just by putting the presentation together.

I'm going to start off here with a screen shot of an article that I took off the Washington Post website. I chose the Washington Post because obviously we're here in D.C., but the principles and the technologies that I'm going to talk about would equally apply to basically any major metropolitan newspaper.

What we have here is an article about how to get your kids to eat their vegetables or how not to get them to eat it, and it's a long article, it goes for a couple screens here. I only took a screen shot of the top one.

But we can see the article itself as well as a couple ads here, a Neiman Marcus ad, as well as a Lufthansa ad. I think these ads were properly displayed because they had this ad inventory. I don't think I was particularly targeted here for them.

But the point that I wanted to show here is that unlike, say, a printed newspaper, a webpage gets its content from a lot of different places. It's not just the Washington Post that content on the webpage comes

from, and there's more content down at the bottom of the page that comes from other places besides the Washington Post.

I ran a program called a packet sniffer to actually find out where all the content was coming from for this webpage. A packet sniffer is a programmer tool that allows somebody like me, a technologist, to look at all the information that goes between my computer and a website and a web server, and it shows both sides of that conversation. If this tool was used by the FBI, you'd think of this as a wiretap device. But since it's my computer, we call it a packet sniffer.

One of the things that I was surprised to learn was just how many different places content was coming from. First of all, to show that webpage, I counted 131 requests for information between my computer and remote servers, and it ended up going to 17 different servers in order to provide content for that one webpage.

So, as you can imagine, the process of providing that webpage is a bit more complicated than it just looks from the screen that you're looking at.

So, what's going on here? At the most basic level, if we just have a static webpage where there was only content coming from one place, we have the user's computer down at the bottom. It makes a request up to

the publisher's web server which is going to be somewhere in a data center most likely in the United States somewhere, and what it's going to say is, I want this particular webpage and it gives an address, and that's that http:// address that we all are familiar with in the address bar. And it makes that request to the publisher's web server and then the web server will then provide that webpage back down to the user's computer.

Along with it, in many cases, will -- if this is the first time we've visited this website -- will come a cookie. I think the best way to look at a cookie is it's kind of like a little membership card and on that membership card it has an ID number which uniquely identifies the computer and, in many cases, in some sense, the individual who made the request for that particular webpage.

Now, if there are images that need to be shown on that same webpage, they'll be done as separate requests. So, each image that we see displayed on the webpage will be its own request.

Now, for a commercial website that's showing -- you know, like a media website that's showing advertisements, they'll have a second server involved here as a minimum, which will be the ad server, and its job is to provide the image that we see for the banner

ad, as well as the ability to click on that banner ad, then end up at the advertiser's website. So, it handles all that aspect of things.

And, again, all that happens are the user's computer will send out a URL request to the ad server, which will be typically for the image or perhaps script code for the ad, and then that image or script code then is sent back down to the user's computer along with a cookie. In this case, this cookie belongs to the ad server.

There may be a third type of server involved in serving up that page, which is what we call a web analytics server. So, websites want to know, in a lot of cases, you know, what's popular at the website, what articles are getting read, what do people seem to be interested in. So, they'll hire an external company in, many cases, called a web analytics company to do those measurements. What will happen then is a URL will also be sent to the web analytics server with the idea of providing information about where somebody has been on the website.

So, these URLS that go to the ad server and to the web analytics server, those are provided by the web publisher. So, they appear in some manner in the HTML code of the webpage or the script code of the webpage and

they're provided by the publisher and then they make these -- they cause these requested then to go to these other servers.

So, obviously, there's some level of cooperation that goes on between the publisher and these other companies in order to get the proper information being sent to the servers.

Now, one thing I wanted to show here is with the web analytics server, in general, it doesn't really provide any information back to the user's computer. It doesn't provide content. It's sort of a hidden activity that goes on and statistics are gathered and then provided back to the publisher, independent of the user's computer.

But a lot of the information that's being transferred and going around here in this process of showing the webpage is going through the user's computer. It comes from the publisher's website out to these other servers and then back to the -- from these servers back to the user's computer.

When we look at -- you know, we're going to talk a lot about cookies over the next two days here and one type of cookie that I think requires special attention here is the ad network cookies and sometimes they're known as third party cookies because they have

some special characteristics.

In the picture I have here, as we have the user's computer up at the top and going to various media websites -- I have it going to washingtonpost.com, CNN, New York Times and MSN, but it could be many different computers. And at the top of each of these webpages, I'm showing some stylized banner ads. So, the first time -- let's say I have a brand new computer, I just opened it up and I go to the Washington Post as the first webpage that I visit. The ad network server will store a cookie on my computer at the Washington Post website, and then as I go around to these other websites, that cookie gets returned to the ad server each time I request another banner ad.

So, what's special about ad server cookies is they, in essence, get shared across many websites, in cooperation with those websites. It's not just like an ad network can grab a cookie on any arbitrary webpage. But if the different websites cooperate, there's this ability then to retrieve the cookies on different media websites. This is a little bit different than normal. If we take like the Washington Post, it's not allowed to look at the New York Times cookie, or vice versa. They don't share. But within the ad networks because of the way the web browsers operate, cookie sharing is possible

across many different websites, and this is one of the things that -- one of the reasons that we're here today, in essence, is because of the sharing that goes on of cookies.

Another concept that will be showing up here over the next few days that will be talked about to some degree is something called web beacons. They go under a lot of different names. I coined a term, for example, six or seven years ago called web-bugs. They also go under clear pixels, action tags, under many different names, but the most popular name seems to be nowadays web beacons. They're a method that work in conjunction with cookies that allow a publisher website to communicate information off to an ad network or to an analytical server.

What makes them interesting and sort of popular in the media is the fact that they tend to be invisible on the webpage. They're implemented as invisible or hidden images on webpages. But the fact that they're images is just an artifact of the way HTML works. What they're really used for, in the most typical case, is for the publisher website to transfer information to the ad network server or analytic server about the person or the webpage that's being viewed.

So, what happens is in the URL, the web beacon,

you know, because it's an image, it has a URL, there's information that's placed into the URL that the publisher wants to tell the ad server about this person or webpage. And they have many, many different uses and they're basically a tracking device, if you will, for watching what people do on the Internet and they provide the ability to track people even when a banner ad's not being shown.

If we go back to our example of that article I showed you about getting our kids to eat vegetables, I took the packet sniffer output and condensed it down and found all the different servers that are providing content or are involved in that webpage. I broke them into the three categories, what I showed before on the original slide, which is the content server, an ad-related server and analytics servers.

So, we can see a lot of stuff going on here. Obviously, the Washington Post is going to have a server here providing content, you know, it's their website. Well, it turns out they actually have four different ones and, you know, for different uses. Sometimes images tend to load down a server, so they have special high speed servers that just do images.

But there are other websites that are -- other companies who are providing content on that webpage and

their names are Inform, MuseStorm, QuestionMark, and Sphere. And QuestionMark gets involved with doing surveys. Sometimes you'll see on a webpage a pop-up. They'll say, would you like to participate in a survey and it will be a company called QuestionMark. This is one of the power of the Internet is the fact that you can link together a lot of different content from different sources.

There's also the -- I forget exactly, I think MuseStorm was providing some kind of related article service, so that if you were interested in this article, they provided links to other articles that cover the same territory. So, you click on there. You click on the link and go there.

So, the advantage of having an outside service do this is they can specialize in this little niche of providing content and then it can be used across many websites.

We have then, also, in terms of ad-related servers here providing content. We have some of the big players in the business, you know, obviously DoubleClick providing banner ads, Google providing text ads along the bottom or the right side of the page, which I didn't show. Then we also have a company called Revenue Science and they're very much a part of what we're talking about

here today because they're a company that does behavioral tracking and provides behavioral targeting services. So, at the Washington Post, one of the things that's going on is you're being targeted in some way on ads based on the articles you're reading.

For reasons that I don't quite understand, there's four different companies who are providing analytic services at the Washington Post. So, they're really interested over there at the Post of what we're doing at their website. But, you know, analytic type services tend to be gathering aggregate statistics and tend not to be individually targeted.

I mentioned before, you know, we've talked in earlier slides about cookies and I just wanted to give you a sampling of what cookies look like here from the various servers. What I tried to show here is they're kind of -- the analogy that I like to use for cookies is they're like membership cards. When you go to a website, you're given your own personal membership card and you become a member of this club for this website. So, in the case of the Washington Post, you're given an anonymous ID. So, all cookies have names as well as some kind of value associated with them.

Here I show one cookie per server. It turns out you can have 20 or 30. There's really kind of no --

there is an upper limit on the number of cookies you can have associated with one webserver, but you can have many different ones. Typically, you see anywhere from one to about 20.

And the ID numbers will tend to be -- because it's computer stuff, will tend to be mixtures of letters and numbers here. So, we have a cookie ID assigned for the Washington Post, Aggregate Knowledge, DoubleClick, Revenue Science, QuestionMark and MuseStorm are the ones that I found on that webpage. There might have been a couple more. I don't think I had enough room for all of them on the slide. But there were six to eight cookies that were being set on my computer. What I had done was cleared out my cookies and then viewed that page to see them all come down.

And the important thing about cookies -- you know, as I said, there's a membership card. The membership card analogy is that when you come to the website, you're given this unique identifier number, and then when you return back to the website, the number that's on that membership card is sent back to the server every time a request is made. So, that's the essence of the tracking that goes on here.

Now, I want to shift gears a little bit. That's sort of the nuts and bolts of how the Internet

works, if you will, from the perspective of showing a webpage. What I want to get into now is more about how the ad targeting or how ads are presented. The analogy that I'm giving here is we have this funnel that takes in a lot of information and then at the bottom spits out some kind of banner ad that gets displayed on the webpage.

So, there's a lot of information that goes into that decision of what ad to show. And then on the left-hand side here, we have a database of ads that need to be shown and then information that's going into the ad selection funnel gets matched up with what ads that are in the database and, finally, the decision is made of what ad to be shown on the webpage.

This process is done by the ad networks. That's their job. It has to be done pretty quickly, too, because what you don't want to do is have -- it can't take many seconds to happen. It's got to happen instantaneously, more or less. You want to see a webpage. You don't want to see pieces of it pop up more slowly, although that sometimes does happen.

So, what gets put into this ad selection funnel here? Well, when a request is made, a lot of information is sent from your computer up to the ad network and these are all sort of fair game, if you will, for selecting an

ad. One being an IP address, your IP address, which is kind of like the phone number of your computer, and it can help, in many cases, locate where you're at. The time of day. That doesn't really come for your computer but that can help determine the ad. The cookies on your computer, another thing. URL, because that can contain information, although a lot of times it looks like gibberish, sometimes it can contain useful information. Demographic information, which is connected to the cookie. The contents of the page and frequency counter.

So, all those things, and potentially more things, will go into this ad selection funnel and out pops our banner ad.

So, I want to give some concrete examples here then of how this works. Some of these will seem maybe very familiar. Other ones may be something people haven't thought about before.

The most obvious place you can see targeting going on, I think, is at an Internet search engine here. I have a Yahoo! webpage, where the idea that I search for, you know, ID theft, that's in the search box here and you can also see it at the top in the URL in the address bar. So, obviously, that's going off to Yahoo!, and then we get sponsored links here, you know, based on this keyword. So, the idea that people buy the ID theft

keyword and then they get their sponsored links shown on the right-hand side of the screen. So, this is very traditional type Internet advertising.

One time I heard an analogy from people in the ad industry, this is a lot like when you go to the Yellow Pages. You'll see your listings that -- the unpaid listings, as well as the ads that appear in the Yellow Pages. This is a very effective type of advertising because, obviously, if you're searching for something, it's probably a good time to maybe hit you with some advertising related to it.

Speaking of baseball, let's see here, but this is about Cincinnati. Here's an ad at my way, and this is basically an example of contextual-based advertising. This was provided by Google. So, we have a news article about the Cincinnati Reds and we'll see ads down at the bottom, you know, based on information that -- or keywords that appears in that article. So, we see an ad here for a baseball jersey and another one for a Cincinnati car dealer and another one for getting play-off tickets. I don't live in Cincinnati. These ads were shown to me in Boston. So, it gives you an idea of contextual-based targeting.

Here's an example of location-based targeting. I went to the Times of India website here, and I'm not

sure what this article is about, it's probably about some sort of local legal matter. But if you take a look at the ads carefully, you notice some interesting things. The prices are in dollars and I'm being shown an ad for Netflix, which I don't believe has an operation in India. I could be wrong, but I don't believe it does. But what's going on here -- and I get Lending Tree ads here for mortgage and, again, in dollar amounts.

What's going on here is the Times of India, in order to make money in the best possible way off of me, is going to show me American ads when I go to their website. So, they made arrangements with the ad networks in order to do location-based targeting. It's either based on seeing my IP address that they'd know that I'm in America or possibly my browser language.

Another way to target ads if you just ask people about their demographics. Everybody in the room probably knows that if you read stuff at the Washington Post, you must set up an account with them. My account -- I have an email address of nobody@nowhere.com. You don't necessarily have to provide accurate information, but the idea here is they want basic sort of direct mail type demographic information in order to do ad targeting. They simply ask for this information when you sign up.

Here we go to a little more -- sort of another level of sophistication here. I think that -- and it gets more into the behavioral type advertising that we're talking about here where a website watches what we do and then provides feedback to us about what's happening on the website.

This past summer I was looking to upgrade one of our TV sets to a high definition TV and I was looking at the Olevia 37-inch TV, which I actually ended up getting. And if you notice down at the bottom of the screen, while I'm looking at this webpage here, I'm also shown what other people have looked at -- when they've looked at this television set, what other models have they looked at and which they ended up buying. This is an example of what's known as collaborative filtering. The idea is you gather aggregate statistics about what people are doing at your website, you're watching them walk around the store and looking at the different models that they're looking at and then you provide that feedback to help people understand potentially other sets that they may be interested in.

But it's an example here very much of kind of remembering things, not just if we think about the earlier targeting, which is based on the one page. Now, we're getting into targeting based on remembering

information about what people have done.

Another example of this is Netflix. You know, if you're a user of the Netflix services, right after you log in your homepage, they'll bring up a little link that you can click on saying, here's our recommendations. Because you rented this movie, we think you might like this movie. And those recommendations are based on the fact of what other people have rented, you know, they've rented this movie and they've also said, we also like these other three movies, and they provide that information back to you.

This is an example where people are making decisions when they rate movies whether they want to participate in this service or not.

So, if we get back in to more behavioral advertising, which is what we're talking about here, well, what's different about it compared to sort of the more simple targeting or classic targeting I talked about earlier?

What's different is we add in another database off on the side here, which is the behavioral profile. The idea is that as we surf the Internet, information is going into behavioral profile that somehow says these are the things that we're interested in based on what we're doing on the Internet, and we use that now for ad

selection.

So, we use all these other parameters that we were using before, but now we add in sort of the history of what we've been doing to select our ads.

But what is the behavioral profile? Well, I looked at a number of different companies involved in this business and it seems like there's two sort of broad ways that we get rated. One I call a product interest profile and the other one is more of a demographic segment profile.

The idea is that we have -- our profile has different categories in it. I'll start off with the product interest category. We're rated for these different kinds of products we may want to buy, how interested we seem to be in those different things. I have for example here car buyer, house seller, house buyer, apartment renter, so on. And we get rated at some interest level and I have it as percentages. It's really up to companies how they do this.

But this information then when we go to a webpage is then used -- these interest levels are then used to decide what kind of ad we should be shown based on the inventory that we have.

The second way of being rated is putting into demographic categories, and this is more traditional

direct marketing things, where we're -- it's sort of like what gender we are, how old we are, where we live, how much money we have and so on, and that's -- again, we get rated by what we do on the -- in our web travels here. So, I have like soccer mom, retired male, newlyweds, all these different sort of categories.

So, how are these profiles created? Well, if you go back to our original few slides here, as you saw, all these web requests are provided to the ad network and they provide a lot of information about what we're interested in. So, we have a variety of ways that can feed into these profiles. I just give some examples here of -- we have a product interest profile. So, if we clicked on a Home Depot ad at one point, that signals that we might be a DIY or somebody who wants to fix up the house on the weekends.

If we're looking to upgrade our HDTV that may be indicated by the fact that we read four different articles over time about high definition television sets. Another source might be we searched for pricing information about cars. So, all the different things that we potentially on the Internet can feed into this profile and there are a variety of mechanisms then that the publisher websites use in order to take information about their webpages and then pass this off to the

behavioral profiling companies to feed into these profiles. Then the information then gets regenerated back in order to do our ads.

So, I need to wrap things up here. Thank you, everybody, for your attentive listening and I hope it was useful here to try to understand the lay of the land. Thank you.

(Applause)

MS. GARRISON: Thank you very much, Richard. Richard told me that he's never done a PowerPoint drawing before and we were so delighted with some of those earlier slides that we actually created blow-ups. We're going to leave them up as posters on either side so that you'll be able to look at them while we're here and, of course, his PowerPoint, as all the PowerPoint presentations, you will be able to download.

Now, we'd like to hear from three presenters who will each give a different perspective on the issues that we're going to discuss today. We'll start first with Jeff Chester who is from the Center for Digital Democracy. Jeff?

MR. CHESTER: Good morning. I want to thank Richard for that. I've been following the online advertising and the digital communications marketplace now since the early 1990s. Before I talk about privacy

and the remarks I've made, I just want to underscore that the future of online advertising has profound consequences for the future of our democracy and democracies everywhere. The kind of society we are creating right now for ourselves and particularly for our children, in many ways, is being shaped by the forces of advertising and marketing.

Whether or not we're going to have a diverse array of democratic media content services, whether or not all voices reflecting diversity will truly be heard, whether or not we're going to have consumer protection and, yes, whether or not we're going to have privacy is all wrapped up in this issue. And I'm going to focus on privacy, but if you want more background, you can go to democraticmedia.org.

Exactly one year ago, November 1st, 2006, the Center for Digital Democracy and the U.S. Public Interest Research Group filed a 50-page complaint asking the Commission to investigate developments in behavioral targeting. We have grown alarmed, as we've watched since 2000, the ever-growing sophisticated array of techniques that had been deployed to track our every move, not just on individual websites, but through the development of new approaches called re-targeting where we were becoming digitally shadowed wherever we went, site to site, where

the industry has designed, in their own words, immersive rich media applications. That's the content that's used with the ads, designed to get us to give up information and to enter, in a way, through our subconscious minds, a relationship with the marketers and advertisers. The technology, the business models had already exploded and, yet, nothing was being done to protect American consumers and educate them.

But when we filed our complaint last year and we met with Chairman Majoras soon after, it was very evident from her interests, and I deeply appreciate this, that she recognized and still recognizes, because we met with her last week, that we had identified a series of major consumer privacy concerns.

Commissioners Leibowitz and Harbour have also been extremely supportive and I want to say I have come to admire over the last year the hard work and dedication of the FTC Privacy staff, and I thank you.

But we believe the time for fact-finding is over. The Commission is the designated Federal agency which is supposed to safeguard consumer privacy. It must now act to protect Americans from the unfair and deceptive practices that have evolved as part of what the industry calls the digital interactive marketing ecosystem.

Wherever we go, as we said last year, the data collection and interactive marketing system is shaping the entire U.S. electronic media marketplace. Few members of the public understand what is going on, that our every moves, our interests, even our mouse clicks are tracked, tabulated, stored and then used or sold to the highest advertiser's bidder.

Yes, online marketers, you can track, collect and use for commercial purposes when someone searches for a health concern, such as their child's use of Ritalin. But just because you can do it doesn't mean it's right. Yes, digital advertisers, you can behavioral target consumers looking for a sub-prime mortgage and sign them up, but just because you can do it doesn't mean it's right. And, yes, online marketers, you can eavesdrop on the members of social networks, but that doesn't mean it's right.

The online market industry is trying to hide behind a number of things, including the facetious claim of much of what they collect isn't personally identifiable. That is why today -- and I know my time is brief. I did time this as five minutes, but what can I say.

We are filing today a new complaint. I think it's 76 pages, which updates the Commission and the

public about all the developments in the online advertising data collection business that we have been tracking -- we've been tracking them over the last year. We urge you to go to our website or get the press release and read it and you will find out the state of the industry and what the plans are to track and target each and every one of us, to use the power of new technology to engage us in behaviors without our awareness and our consent.

We are showing in our filing how children and teens are the focus of behavioral targeting. We talk about the mortgage of crisis. We talk about MySpace and Facebook and, yes, we document new forms of racial and ethnic profiling that's going on in the online industry and we ask the Commission to launch immediate investigations in these four areas.

We also want to underscore that the privacy threats arising from the Google/DoubleClick merger are the gravest and we urge the Commission to act on the EPIC petition.

I see my time is up. It is time for the Federal Trade Commission to protect consumers by fully implementing and enforcing the fair information practices as proposed by the OECD. Unless the Commission does this, our privacy and the privacy of our children and

youth, who are the principal focus of this machine, which will have a profound impact on their values, on their education, their sense of self and their ability to civically engage. I urge you to go to digitalads.org if you want to just get a sense of how the digital marketing infrastructure has been designed to encourage children to engage in unhealthy dietary behaviors.

The question is, will the FTC act to protect the U.S. public and help ensure that the Internet and other online media are a safe environment for communications in commerce? I await the answer. Thank you.

(Applause)

MS. GARRISON: Thank you very much, Jeff. And, now, I'd like to introduce for another viewpoint, Randy Rothenberg from the Interactive Advertising Bureau. Randy?

(Applause)

MR. ROTHENBERG: Good morning. On behalf of the Interactive Advertising Bureau, the trade association for advertising supported interactive media in the United States, I thank the Commission and the staff for this opportunity to participate in this very important discussion regarding online behavioral advertising.

The IAB's 350 member companies represent the

present and future of marketing in media in the United States. Among our members are the burgeoning new media brands that have entered American consciousness during the past decade, companies such as Google and Yahoo!, MSN and CNET. They are the major media companies that have made two-way communications a significant component of their offerings, from the New York Times to NBC Universal to Conde Nast to CNN.

There are smaller successful information companies serving market niches, such as Cars.com and WebMD. And there are platform specialists in areas such as digital video, online games and social networking with new names like Brightcove and WildTangent and Facebook.

As this indicates, historians will undoubtedly look back on this period as the most dynamic and innovative in the history of American business. Central to this dynamism has been the promise of advertising support. A question for all of us today is what is the best policy framework to maximize such innovation and competition in order to produce the best products, services and diversity for consumers? There is a clear answer supported by copious evidence dating back at least to October 1994, the date when the Netscape Navigator web browser was released, initiating the interactive era.

The unprecedented proliferation of good

services and information diversity that characterized the Internet has been generated within a framework of industry self-regulation and market forces. It is incumbent on the business community to ensure that interactive advertising, marketing and data use practices are responsible. At the same time, government must be prudent in ensuring that no regulation is drawn that would curtail interactive advertising's potential to continue to support this extraordinary pattern of innovation and consumer benefit.

Advertising is the economic foundation underlying the dynamism of the interactive era. With interactive media, it's become a commonplace that marketing spent one of the last three read-outs of imprecision in American business is becoming more accountable and more productive. This is possible because of the availability of mathematical and technological tools that enable the analysis of non-personally identifiable data to detect patterns in people's interests and consumption habits and to allow the matching of advertisements to their needs.

Other analytics tools allow for predictive modeling based on the responses to these well-targeted ads, enabling the development of even better targeted ads. All of these advancements ultimately work to the

benefit of consumers. They not only receive advertisements more relevant to and productive for them, they receive more and better free content and services online.

Because these advertising processes are largely automated, they are taking costs out of and improving results from advertising. In addition, because the Internet allows the seamless aggregation of thousands of websites into online advertising networks, marketing can reach consumers in volumes that rival, even surpass, the audiences of broadcast television. Yet they can do this with a precision that no previous medium can match.

In such ways, are interactive media contributing to the productivity revolution that is driving American business in the 21st Century. For such reasons, interactive advertising spend in the U.S. this year likely will reach $20 billion, according to research by the IAB and Price Waterhouse Coopers. That's nearly one-third the amount marketers spend on television and a sum reached a mere 13 years after this medium's invention.

This revolution is reaching deep into the fabric of communities across the nation. Today, all of us, quite literally, own a press and much, much more. The Internet has torn down barriers to entry in both

content creation and distribution. It is now possible for any individual to publish a national magazine, even program a global television network with the applications that come built into his or her laptop. Never has speech been more open, available and varied.

As of July 2006, some 12 million American adults, about 8 percent of the American population, were publishing their own blogs, which were being read by 57 million other people, according to the Pugh Internet and American Life Project.

If any of the Commissioners or Commission staff or anybody else in the room want a tutorial on how to create your own national media outlet, the IAB would be glad to provide it if you'll promise in return to join the IAB once you begin to sell advertising, for you most assuredly can use advertising and build a business on the web based on little more than your brain, passion and energy. According to Pugh, 32 million American adults have used online classified ads for selling or buying and 35 million American adults have participated in an online auction.

Millions of others are making their living creating and operating media venues that house well-targeted advertisements. The 24/7 real media online advertising network partners with 950 websites. Dakota

numbers 4,000 websites in its online network. Advertising.com, another online network composed of thousands of sites, reaches 160 million unique visitors a month. These sites are the mom and pop grocery stores of the worldwide web, just as the local retailer anchors the geographic community, so these sites anchor communities of interest that span towns, cities, states and even nations. They do this with their content and they finance the content through advertising. Online advertising is a catalyst for a small business renaissance in this country.

I'll give you examples -- I'll conclude, thank you. I will give you examples. If anyone wants copies of the full testimony with the names, dates and businesses developed by real individuals around the United States using these networks and the variations of diversity of communications, just go onto the IAB website and look at the list. Thank you very much.

(Applause)

MS. GARRISON: Thank you very much, Randy. And, now, to round out this morning's first session, here is Trevor Hughes from the Network Advertising Initiative. Thank you.

MR. HUGHES: Thank you, Loretta. Good morning, and I would, too, like to thank the Federal Trade

Commission for pulling together another great event for us to examine important issues in the online marketplace today.

My name is Trevor Hughes. I am the Executive Director of the Network Advertising Initiative. I've been in that role for the past six years. Prior to that, I was Director of Privacy and Corporate Counsel for Engage, one of the original behavioral targeting companies, now long since defunct, but I have been in this space for quite some time, the better part of a decade, and it does feel a little like deja vu coming back to revisit many of these issues.

I'd like to start today by saying that everything old is new again, that the issues that we're talking about where we're hearing shock, shock, that marketers are trying to deliver more relevant messages to consumers really should not be surprising to any of us. Starting in 1872 when Montgomery Ward sent out his first catalog and then going on to Sears and Roebuck, they quickly realized that the expense of printing those catalogs and sending them out to rural America was pretty high and that it made more sense to try and figure out who might be more likely buyers of their products and services. So, they started to target their marketing to those people who were most interested in what they might

want to sell or to buy from those companies.

Marketers, from the beginning of marketing, have been trying to find the most relevant audiences possible and make available services and products that are most relevant to our marketplace. So, it's not a big surprise. And we see it every day. We saw it before the advent of the web.

I'm a soccer coach, soccer player, soccer administrator. I get a lot of soccer catalogs. I didn't have a relationship with either of these two companies when I first got the catalog. They somehow knew, either through my membership in a soccer organization, my subscription to a soccer magazine, my purchase of a soccer-related something from some store that I might be a soccer guy. And you know what? They were right. They were right. This is a form of behavioral targeting.

It's been around for a long time. Behavioral targeting is not new. It's not new at all. Marketers are just doing what marketers have always been doing.

But the web is different, isn't it? The web is most definitely different, and that's why for more than a decade we have been engaged in an ongoing dialogue to build layers of protections into the web, into ecommerce, into our experience online so that we can provide greater trust for consumers so that they will engage in the great

power that is the Internet.

And just like Montgomery Ward and Sears Roebuck, reaching out to disenfranchised rural America back in the late 1800s to offer goods and services that were not available before, the web is a great democratizing agent in society today. It allows us to communicate in ways that we never could before. It allows consumers to find tools and services and goods and products and communities of interest that never existed before.

But data collection, the speed of transaction processing, the ability to dynamically create offers and services for consumers are different, and for that reason, we have layers of protection. We have defense in-depth for consumers with regards to their data and their privacy online.

Let's start at the very top, privacy policies. We don't talk enough about privacy policies anymore, but it's one of the great successes of the past ten years online. Recent stats suggest that 85 percent of the Fortune 500 post privacy policies.

Now, there are many criticisms of privacy policies and I certainly would be one of the people to say that there are many things that we could do better. Layered notices are a great example of a step forward,

but there are great examples of things that we can do better with privacy policies. But, by and large, online organizations today are posting privacy policies and it's not just for notice. It's not just for notice, it's also to create obligations on that organization. Many organizations post privacy policies in the absence of an obligation to do so and in posting a privacy policy create exposure for their organization.

I remember seven, eight, ten years ago many, many companies saying, why would we post a privacy policy when we're not required to do so and when we do so, we expose ourselves to liability to the FTC and State AGs and consumers generally? Privacy policies are out there for notice and for enforceability and they're working.

But we also have technological controls. Every browser in the United States and the world has cookie controls within three clicks. You can switch off third party cookies, you can switch off first party cookies, you can manage cookies in many, many ways. I.E. 6 and I.E. 7 have even more sophisticated tools. The Platform for Privacy Preferences, P3P is embedded into those tools and that, in the default setting in I.E. 6 and I.E. 7, blocks third party cookies that do not have a privacy policy attached.

We also have self-regulatory programs. Most

certainly the Network Advertising Initiative will be discussed many times and I look forward to discussing our thoughts about the NAI and what we have done over the years during tomorrow's self-regulatory session.

But there's more. There's TRUSTe. There's other seal programs. There are downloaded applications like anti spyware, anti malware, privacy enabling tools that consumers have. We have many, many, many layers of control and protection for consumers today.

But let it not be said that we're done because we're not. We certainly have more to do, and I am here today representing the members of the Network Advertising Initiative to say that we definitely look forward to this dialogue and we hope that from this we will be able to improve the consumer protections that we have in place and we hope that collaboratively together we can find better solutions for consumers. Thank you.

(Applause)

MS. GARRISON: Thank you very much. This has been a great start to the day. We're going to ask if you can be back in your seats -- this session won't have questions. All four of these gentlemen will be on subsequent panels and you'll be able to ask questions at all of the later panels. I would like you to be back here if you could at ten to twelve after. We would like

to get started just a little bit earlier for the next session so indeed we can have enough time for questions.

Thank you.

(A brief recess was taken)

REMARKS

MS. BRANDENBURG: We're ready to resume our next session if you could all take your seats.

One brief housekeeping note, for anyone who has noticed the clocks in the back of the room, we apologize that they seem to have automatically advanced themselves or have not kept up with the time change. So, please disregard those. They are an hour back in case you get confused.

Now, it's my pleasure to introduce Commissioner Leibowitz who's going to make a few remarks.

COMMISSIONER LEIBOWITZ: I think I'll wait another minute or two because I see people coming in. Why don't you all try to take your seats. Let's take a minute or two to find your seats. It's an unexpectedly packed house today, but we're very delighted that it is.

(Brief pause)

COMMISSIONER LEIBOWITZ: Good morning. I'm Jon Leibowitz, I'm one of the FTC Commissioners. Usually I'm the Commissioner with the shortest speeches, Commissioner Harbour is the Commissioner with the most substantive speeches, but today this one's going to go a little closer to 15 than five minutes, so I wanted to let you know in advance.

Let me start by thanking the first panel for

setting out some of the really important issues that the workshop is going to grapple with. As you can tell, reasonable people approach behavioral marketing from very, very disparate perspectives.

Let me also thank all the participants in this Town Hall meeting. You are not only a large group, you're an incredibly impressive group and your presence is really a testament to the "white heat" of these issues.

And, finally, a really big thank you to the Commission staff for all of its hard work in organizing this event. I see a number of Commission staffers here who have worked extremely hard on this. So, thank you so much.

We all bring different privacy expectations to the table. It doesn't bother me, for example, that Amazon keeps track of the books I've ordered and recommends new ones, and that's targeted advertising. And it doesn't really bother me that search engines deliver sponsored links based on my queries. That's targeted advertising, too.

Somewhat more disturbing, at least to me, is the new Internet telephone service that uses voice recognition technology to monitor phone conversations and to send, contemporaneously, targeted ads to the

subscriber's computer actually during the call. But this service is opt in, the product is new, and there are plenty of competitors offering telephone service with different and probably higher level of privacy practices.

I am concerned, though, when my personal information is sold to or shared with third parties or when my online conduct is monitored across several websites or across different web-based services, especially when there is no effective notice or consent to these practices. And I think all of us should be concerned, even troubled, that seemingly anonymous searching and surfing can be traced back to individuals, specific individuals, and that not all information that companies have collected about us is secure from data breaches or release.

Don't take my word for it; just ask AOL customers. Last year AOL released a cache of supposedly anonymized search records, but some people were identified based on their queries. The results were somewhat embarrassing, yet it could have been much, much worse.

In my view, all this is a real paradox: you can go online from the privacy of your home and enter searches or surf websites that involve sensitive medical conditions or reveal your deepest darkest secrets or, by

the way, even your most trivial curiosities. You can create a personal profile on a social networking site and reserve access only for your close friends and family. It all seems so private, but because online marketers are tracking our Internet searching, surfing and socializing, it may be more public than we would like to think.

Now, if you have teenagers, you probably know the texting acronym POS, parent over shoulder. Well, I see a lot of you do. And those who have teenagers and don't know this texting acronym, you should learn it.

Well, when you are surfing the Internet, you never know who is peering over your shoulder or how many people or how many companies are watching.

Now, to be fair, most of our web searching and browsing and social networking is free, thanks in large part to advertising, and most consumers seem to like it this way. As the Internet has evolved, the ad targeting has become more sophisticated, arguably bringing greater benefits and a richer Internet experience to consumers.

But the question is, at what cost? Are we paying too high a price in privacy?

In his seminal 1983 book, The Rise of the Computer State, David Burnham worried that detailed data

bases and the expanding network of computerized record systems were enabling large organizations to track the daily lives of individual citizens.

And that was then, sort of the Jurassic Age of big mainframes -- when personal computers were just entering the market, the Internet was still an academic/military experiment, and get this, AT&T was the giant telecommunications behemoth. Of course, some things never change.

And some things never stop changing. Today, the Internet, computerized data collection and targeted advertising are creeping into nearly every aspect of our social interaction and our commercial transactions. Seventy-one percent of U.S. adults use the Internet. Nearly half of all Americans have broadband at home. Internet advertising revenues for the first half of 2007 were nearly $10 billion, a 26 percent increase over the first half of 2006. Make no mistake, the business of online behavioral marketing is big business.

In An Ideal Husband, Oscar Wilde wrote -- and I think this was in 1894 -- “Private information is practically the source of every large modern fortune.” And, today, that’s especially true with online behavioral marketing. Just last week, Microsoft announced a $240 million agreement that gives it exclusive rights to sell

worldwide ads targeting Facebook's 50 million members, and I think Facebook, based on that investment, is estimated to have a value of $15 billion.

Google already invested $900 million in MySpace, which announced that it can tailor ads based on what users write on their profile pages. Meanwhile, Google is trying to buy online ad server DoubleClick -- a little more about that later. Some of you know that we're reviewing that deal.

Microsoft acquired aQuantive, Yahoo! purchased Right Media. With all these big money deals of course comes big-time pressure to push more, and more effective, ads on the Internet down to consumers.

Collectively, all this tracking of our online conduct, our searching, web browsing, social networking, emailing, and telephone chatting, all this massive collection of our private information, purportedly to serve precision-guided ads, can be disconcerting.

Perhaps it is because we don't quite understand what websites and online advertisers are doing or how they are doing it. Perhaps it is because we feel like we don't really have any meaningful choice or control in the matter other than to stay offline, which really isn't a choice at all. Perhaps it is because we don't really know what information websites and others have collected

about us, and perhaps it is because we have no assurance that they will protect the confidentiality of our sensitive personal or financial information.

Now, when the Commission first confronted these issues nearly a decade ago, there was a general acceptance of four core fair information practice principles. It's actually fair information practice principles -- I did that notice with two Ps -- notice, choice, access, and security. Industry efforts to implement these principles resulted in many websites developing and posting so-called privacy policies. And, initially, privacy policies seemed like a good idea, and they are a good idea.

But in practice, as Trevor noted in the last panel, they often leave a lot to be desired. In many cases, consumers don't notice, read or understand the privacy policies. They are often posted inconspicuously via a link at the very bottom of the site's homepage, and if you can actually find them, the policies are filled with sort of fine print legalese and techno talk.

A recent study that was submitted as a comment for this Town Hall examined privacy policies of Fortune 500 companies and found that they were essentially incomprehensible for the majority of Internet users. Only 1 percent of the privacy policies were -- 1 percent

were understandable for those with a high school education or less, and that's obviously like most teens and many consumers. Thirty percent of the privacy policies required a post-graduate education to be fully understood.

The study also found that fewer than 27 percent of the privacy policies allowed consumers to opt out of collection of data. None of the privacy policies surveyed allowed consumers to opt in. Not one. And I think she surveyed 175 privacy policies out of the Fortune 500 companies.

The vast majority of the privacy policies simply state that the consumers signify their acceptance to the collection of data by using the website. So, your only choice really is take it or leave it.

Even the title "privacy policy" is arguably a misnomer in some cases, or in some sense, because many consumers believe that the term "privacy policy" means that the website will protect their privacy and will not share their information. I see I provoked laughter over on the left-hand side of the room.

All this tracking and targeting is especially worrisome when it involves children and teens. A whopping 93 percent of American teens age 12 to 17 -- I guess Americans age 12 to 17 use the Internet and 55

percent of these online teens use social networking sites. Internet use by children even younger is growing exponentially as well.

Now, when Congress passed the Children's Online Privacy Protection Act, it clearly recognized that young children deserve special protections in cyberspace. And I see a lot of people in the room who are very, very involved with COPPA, to their credit. COPPA imposes certain requirements before websites may collect personal information from children under the age of 13.

What you have to ask yourself today is, is that really enough? Now, based on the focus group that I convened over the weekend, and that's my 12-year-old daughter and four of her friends, the online ads that target children aren't always appropriate for their age. They see ads with titles like, "How Long Is Your Next Kiss," and "Touch Me Harder." And then, by the way, I asked my ten-year-old about this last night and she said she had just been served, while she was online, an ad for Clorox. So, go figure.

The FTC's -- and I see I provoked a little laughter over here, but actually it was from Commission staff. So, that doesn't really count.

The FTC's most recent report on marketing entertainment products to children seems to confirm some

disturbing practices in this area. For example, sites like MySpace ran banner ads for R-rated movies, even though the site reaches a large number of children under 17.

We enacted COPPA -- and, again, I see a lot of people in the room who were very, very involved, and to their credit, in enacting COPPA. We enacted COPPA to place a parental buffer between advertisers and our children, but the rise of sophisticated behavioral marketing seems to me to be eroding this parental control, at least to some extent.

So what should the Commission be doing? You know, sometimes the answer to problems in cyberspace is very, very clear, like in the case of deceptive nuisance adware, that is adware sent to consumers' computers without their notice so they can't give true and meaningful consent. You put the malefactors under order. You disgorge their profits. You pass a law -- this is my wish list actually -- giving the FTC the authority to impose fines.

But for behavioral marketing, the solution is not so certain. Behavioral marketing is complicated. In some cases, the privacy trade-off may make sense for some people. But one thing is clear, the current don't ask/don't tell mentality in online tracking and profiling

needs to end.

And while I don't presume to have all of the answers or even many of the answers, I do have a few thoughts. Let's start with providing better information and more meaningful choices for consumers. First, some have called for standardized privacy policies, including former Commissioner Sheila Anthony who is a hero of mine, and some have called for shorter notices. And the take-away from the Commission's recent workshop on negative option marketing was that short, conspicuous online notices just work better for consumers. I think all these ideas are worth exploring in the behavioral marketing context.

Another improvement would be for more firms to allow consumers to opt in when it comes to collecting information, especially when it comes to sharing consumer information with third parties and sharing it across various web-based services. Consider changing the widespread opt-out default for ad-serving cookies. Consider changing that default and why not make it opt in? I mean, as the Chairman and Commissioner Harbour and I have said, and we've said this time and time again, people should have dominion over their computers. And we don't just pay lip service to this approach at the Commission. We really, really mean it. Opt in, I think,

would be much more empowering.

Now, at this point, I am not saying that the government should mandate an opt-in model, but, in my view, it is a far more preferable result.

Third, more competition. And, indeed, in this area there's been some good news here in recent months. With all the attention on online data collection recently, the leading search engines have been literally almost tripping over each other to have the strongest privacy protections.

For example, Google announced in March that it would anonymize its server logs after 18 to 24 months so that search histories -- and I know most of you know this -- can no longer be identified with individual users.

A few months later, Microsoft announced it would make search queries anonymous after 18 months. Within days, Yahoo! announced its plans to make users' search history anonymous within 13 months. Do I hear ten months from the search engine lobbyist in the second row over there? Ten? Do I hear eight over there? Anyway, we're making progress.

Ask.com announced recently that it will offer a new feature, the AskEraser, that will allow users to erase their search histories at will. Let's hope we see more competition to give consumers more understandable

information, more choice, and more control. Indeed, today's Town Hall already inspired a number of creative new ideas, including what I think is a very promising approach, which is the Do Not Track list.

Now, it's always great when the competitive marketplace can solve these types of problems, although my sense here, quite honestly, is that the marketplace alone may not be able to resolve all the issues inherent in behavioral marketing. So, at the Commission, we're going to listen closely to what online marketers are doing, how they are doing it, and who they are doing it to, we will continue to think closely about how to ensure all the wonders of the Internet while respecting consumers' sense of privacy.

But we're also going to continue to monitor industry behavior, and if we see problematic practices, the Commission won't hesitate to bring cases or even break thumbs.

All right, one final point, it's not surprising that a lot of folks, and I mean a lot of folks, have asked me -- and I'm sure my colleagues in recent weeks, what are we going to do about the Google/DoubleClick merger? Well, of course, I can't talk about pending merger reviews. Commissioner Harbour, of course, can't talk about pending merger reviews. She's a real lawyer,

as opposed to me. I just play one in the Federal Trade Commission. Except to say this, our staff is working through the matter as expeditiously as possible given the complexity of the deal, and under the Clayton Act, our analysis of the merger has got to be about competition and potential competition. It can't be about privacy, per se.

But whatever we do, let the deal go through, block it or attach conditions, we are still going to have to address the fundamental privacy issues and data security problems inherent in behavioral marketing. They really do transcend any particular acquisition. Our obligations to the consumers of America require nothing less.

Thank you so much. And I know we're running behind, so I will maybe take one or two questions and then we'll turn it over to this panel so they can get moving. So, thank you so much.

And if we have no questions, that's fine, too.

(Applause)

COMMISSIONER LEIBOWITZ: Any questions? One question from the gentleman all the way over there. Why don't you identify yourself.

(Individual not in front of microphone)

MR. SMITH: My name is Robert Smith from

Privacy Journal. It seems to me the analysis of children's websites has to go much further. It's the manipulation of children who have (inaudible) into the consent, not the collection of information, not the disclosure of information, not opt in or opt out. If children go to websites and if they fail to make the right strokes or don't show up enough, they're somehow punished. They lose coupons and lose benefits. Some develop loyalties to a pet or an animal. The animal will die if you don't return to the site regularly, or worse than that, the animal will be abandoned and the child will be made to feel guilty.

Does the FTC have any handle on that kind of manipulation?

COMMISSIONER LEIBOWITZ: You know, let me get back to you on that. It's an interesting point that you raise about sort of manipulation of children in the context of behavioral marketing, and I'm sure it's something that we are looking at and happy to look at.

One more question and then I'm going to really turn it over to these folks who deserve a chance to go ahead with their panel. No more questions? No more questions.

All right, again, thank you so much and we really appreciate all of you being here.

(Applause)

SESSION 2: BEHAVIORAL ADVERTISING TODAY: UNDERSTANDING THE BUSINESS AND TECHNOLOGY

MS. KRESSES: Thank you, Commissioner Leibowitz. I'm Mamie Kresses and this is Peder Magee of the FTC, and we'd like to move into a nuts and bolts discussion about what several businesses in the industry are actually doing themselves.

Today, we'll hear presentations from Dave Morgan of Tacoda, acquired by AOL; Robert Gratchner of aQuantive, acquired by Microsoft; Mike Walrath of Yahoo!; Tim Armstrong of Google; Chanterria McGilbra of Netmining, who's come all the way from Belgium to be with us; Pam Horan of the Online Publishers Association; Mark Westlake of the website HowStuffWorks.com; Ralph Terkowitz of ABS Capital Partners; and Carlos Jensen from Oregon State University.

And, now, we'll go ahead and turn the mic over first to Dave Morgan.

MR. MORGAN: Good morning. I'm going to talk a little bit in specifics about how targeted ads are delivered on the Internet and also talk a little bit about some of the structure and how the business models operate, and as I think you can suggest by the title of -- or at least as the title of my slides should suggest, it's really ultimately about ads that people

want.

I came out of the newspaper industry and I think one of the things that we all have to understand no matter what our point of view is -- that we're not in charge and you're not in charge anymore. The consumers are running the show.

The marketing and advertising and media industry is learning that very, very slowly and painfully, but we are now entering a world where consumers have significantly more power to take information they want, to choose to accept or reject what they don't want, to buy what they want or what they don't want. This is causing extraordinary fragmentation in the media industry. We're watching the industry that I came from, the newspaper industry, going through a period where we're probably going to see a reduction of the amount of newspapers in this country by about 30 percent in daily newspapers over the course, I would say, of probably the next two to three years.

Probably, we will see a quadrupling of small daily and niche publications that better serve individuals, but the old infrastructure's going to change. We're seeing everything supported by advertising and some of them are tests that would make me uncomfortable, too, that I don't want to personally

participate in, which would be ad-supported phone, but for somebody that doesn't want to have to pay $50 a month for phone services and chooses to do that, you know, there's a lot of experimentation.

We're seeing news, entertainment and information going to people where they want it, when they want it, how they want it. And the thing that anyone that's in a consumer industry or, you know, certainly, I think, also for those in government as well, it's in a world of all about me, and me being not me, but me about the consumers. And it's all about free.

Today, most of us would argue there's too many ads, there's too little relevance and they're in too many places. And if you ask consumers today what they most dislike, what they don't like about their online advertising experience, and I think actually you'll probably see some of this in research that will be presented later, is that they don't like ad clutter on the webpages, they don't like interruptive ads and they don't like irrelevant ads. Those of us that work in the industry listen to that a lot and we're starting to focus and we're starting to see innovation and consumer control.

Certainly, one of the byproducts of this meeting is that I don't think there was a journalist in

this industry or in the business world that didn't have at least 12 embargoed press releases late Tuesday, early Wednesday for innovations that people wanted to announce while there's attention in this space.

So, what do I think this is going to mean? What do companies like Tacoda and others focus on, now part of the AOL family? We do believe in the future we're going to see fewer, more relevant ads. Why? Because I don't know about you, but I've cried over television ads in the past. Not a lot of them, but I've never cried over a web ad. We don't yet -- I mean, who has? We have not yet developed the experience, the potential for the emotional ads that will eventually probably -- that consumers want and that consumers value.

So, what are we doing? We're trying to watch, look and listen. We're trying to tailor ads more for consumer experiences. I came from the newspaper industry, as I mentioned, and if you look at the Sunday newspaper, when you ask consumers why they buy the Sunday newspaper, five of the top ten reasons have to do with the advertising, not the editorial, slick coupons, department store promotions, job ads, car ads and home ads. You need ads people want.

The future of ad blocking, that's going to be part of the future. Consumers will only accept ads they

accept and, quite frankly, they're only going to accept ads that mean something to them.

So, what is the networked behavioral targeting work? What is it that the companies really know? This is -- imagine this person surfing through Shutterbug, NBC, cars.com, the New York Times and Oprah. What is known to the ad server, the behavioral ad server? Nothing more than anonymous information that a browser, not necessarily a person, happens to have looked at these kinds of content.

When they're on a website, let's say, like in this case, HighBeam, an encyclopedia website that cannot generate ad support on its own, but it's quite useful for a lot of people in providing free information. They can get an ad that's more relevant that can actually fund that content.

Well-targeted ads basically rely on knowing a little bit more about what -- you know, how to filter an ad and how not just to put the more relevant data, the targeted ad, how to reduce those ads that aren't relevant, the blinky, flashy ads that you see 50 times a day. It's only through behavioral techniques you can put a cap on that and make sure that any one browser won't see them more than once or twice or, hopefully, won't see them at all.

We believe, and I believe, that privacy protection is going to be a growing and important competitive advantage and we already have even heard that from the Commissioner right before this.

Look at the actions. You know, it's not like who's going to 11 months of data, who's going to be the first to say none? Well, we have AskEraser. We are going to see, as consumers start to value this more and more and understand more, we're going to see more companies taking steps. We're going to see companies taking steps so that they can make this a competitive advantage.

And when it comes to what's this mean for democracy and our future, I grew up in a tiny little town in Western Pennsylvania that was supported by the coal industry and the steel industry, and when I was in high school, we had 20 percent unemployment. In my town, you had two broadcast TV networks, not three, so you couldn't see college football because the mountains from Pittsburgh were too far away and we had one newspaper that came out in the afternoon. Today, in my town, if you want a New York Times in print, it's $5 and you have to order it 48 hours in advance. So, my parents had to do that since I got quoted earlier this week. They had to go and put that order in.

But, no, actually today online the 6,000 people in Clearfield, Pennsylvania, get free NewYorkTimes.com every single day paid for by ads, and that's something that we never had the chance when I was growing up to do. So, I'm quite happy to help support and pay for this free content we have.

Thank you.

(Applause)

MS. KRESSES: Thank you, Dave.

Now, we'll hear from Robert Gratchner of aQuantive.

MR. GRATCHNER: Good morning. It's a pleasure to be here and I appreciate the FTC taking the time and effort to allow me to come today to talk about the aQuantive business model and how we work.

But, first, I want to apologize to the people kind of in the center. My wife hates going to the movies with me because the people behind me always say I can't see the movie, while the people in front -- I'm sorry you can't see the screen because I'm right in the way. So, I apologize for that. Likely, you'll be able to see mine today.

So, what I wanted briefly to talk about today is who is aQuantive, how do we work, how do we operate, what's our business model, and in particular, how does

Atlas, the ad serving technology, work?

My name is Rob Gratchner. I'm the Director of Privacy at aQuantive. We are a recent acquisition of Microsoft. Back in May, they announced our acquisition and everything just recently has gone through as early as late August. So, all my talk today will be on the aQuantive model, not on the Microsoft model.

But aQuantive is -- and one of the reasons why Microsoft was attracted to us, is because we offer three great business models. One is we have a digital marketing service and this is your ad creation, we create the banner ads that go out there, we create websites, we help advertisers with their online marketing strategy.

Our second business unit is our digital marketing services and this is our Atlas Group, which serves the ads out there that you see today.

And then our third business model that we have out there is Drive PM, which is an ad network. We're one of the largest ones out there. But incorporated also within our performance media group, we have Franchise Gator and Franchise Gator is basically a lead generation site which we're trying to grow and expand that business as well.

We've been a small company since I joined two years ago. We were U.S. only. We're now growing

internationally with major sites in mostly Europe, but also in Asia as well. So, we're growing, we're expanding and we hope to continue that into the future.

Now, unfortunately, my presentation today was partially already talked about a bit in understanding technology, and they did, earlier today, an excellent job of explaining how online advertising works and how it goes through, and I'll go through briefly a little bit about the Atlas model and how specifically it works and how does the third party ad server get an ad to a website.

So, basically, when a browser does a request to a publisher's website, it will make a call saying, please send me information to my site, I want to go see a sports page or some other type of information. I was joking with Carlos earlier that my family's from Oregon and we are Oregon State fans, so I'm constantly keeping tabs on the Oregon State football team and where it's going -- and to the Boston fans, I want you to know your star is an Oregon State graduate. So, I'm keeping tabs on the Beavers and what's going on.

As I go to the sites, I want to understand, hey, what -- you know, please send me information. But within that website is also a request that goes to Atlas, the URL, saying, please -- it goes to Atlas and when

Atlas receives this, within the second step it says, okay, great, I see this ad, I see this request coming in, now let's go apply some logic to this request. And we have a whole algorithm -- I have a few minutes today to discuss our model, which I can't go into great detail, but when we see a request coming in, we put some logic behind it. Now, if it's a first party ad or the first time we've seen this cookie or haven't seen a cookie, our cookie on there, and then will deliver an ad and not much logic goes behind that. But if we've seen this cookie, then obviously we're going to apply some sort of logic and apply some sort of ad that this user would like to see. In my case, it might be an Oregon State football jersey or whatever the case may be. I want to go see some sort of relevant ad that comes to me.

Then we will also count that add and we'll say, great, here is this ad, we'll count it for some analytics later, and then when we do those, we don't -- we send a response to the -- back to the browser which then goes to actually a third site, which houses all the advertisement. Now, it doesn't collect the information, it doesn't do anything, it just houses the actual creative ad itself. Then it will go serve that ad onto the website.

So, as you can see, it's not as complex as

everyone makes it out to be, but there is some intricacies that need to be explained and, obviously, hopefully this next few days a lot of this will be flushed out.

But one of the things that we wanted to talk about today also is how do we protect your privacy. I mean, obviously, it's a concern. At aQuantive, we've always been very dedicated to privacy and we were a founding member of the NAI. We think the NAI brings a great self-regulatory group to the industry more so than almost any other type of advertising out there or even type of other industry out there. It's a thought leader. It has some great principles out there that we adhere to and others with NAI adhere to as well.

The only thing we don't do is we don't collect personal information by any means. We don't see email, we don't see any type of really personal information coming to our servers that we save.

And the other thing, part of the NAI, we provide an opt-out cookie. So, if you do not want to be tracked, you can click on or opt out through our privacy policy or through the NAI website.

The other thing is our privacy policy -- I know we talked about legalese and technical. I am neither a lawyer nor a technician, so hopefully our site, you can

go and understand it fully.

Then we want to provide a benefit -- we do not provide benefit to our advertisers based upon users' browser history, which is really important to understand.

Then the other thing, as we get integrated into Microsoft, which has a great privacy team and privacy principles out there, we want to make sure that we incorporate their principles with regards to the recent announcement of Live Search and Online Ad Targeting. We adhere to that, and as we get more incorporated, we hope to leverage out their great resources.

Thank you.

(Applause)

MS. KRESSES: Thank you, Robert.

Now, we'll hear from Mike Walrath of Yahoo!.

MR. WALRATH: Good morning. Thank you very much to the FTC and Mamie and Peder for having us here today.

What I'd like to do here is two things. I'd like to start with a view of the market players and models and then talk a little bit about some of Yahoo!'s businesses in these areas.

So, when we think about the online display ad participants, we should be thinking about advertisers who provide the demand, networks who provide matching and

liquidity between advertisers, and publishers who are aggregating audiences and who are delivering supply that allow targeted advertising to be delivered.

What we often see are, and what we've been seeing recently, are ad networks who are providing the matching technology and the liquidity and a lot of the behind-the-scenes work to bring advertisers and publishers together.

When we think about the models in the display advertising ecosystem, we also think about generally three ways that companies participate -- direct relationship between advertisers and publishers; we think about agencies and ad networks providing intermediation services that create scale and leverage -- not every advertiser and publisher want to interact directly with each other, and so, ad networks and agencies provide intermediation services and really an ecosystem unto themselves; and, more recently, we've seen ad exchanges rise. Ad exchanges promoting competition and increased liquidity increase openness and transparency and efficiency in the market as well, where advertisers and publishers and ad networks can all compete.

So, what I'd like to talk about now is how Yahoo! participates in these markets, and there are really four ways today. As both an advertiser and a

publisher across Yahoo!'s own sites via the Yahoo! Publisher Network, where with partnerships with eBay, Comcast, a consortium of hundreds of newspaper publishers, we provide ad serving and ad management platforms there.

Through our recent acquisition of Blue Lithium, we've increased our scale in the ad network business as an intermediary, and through the acquisition of Right Media, we're exploring new models for openness, efficiency, competition and transparency in these markets. These are really the four businesses that Yahoo! participates in in this area.

I think the FTC has provided a very broad definition of behavioral targeting. What I'd like to do is share our definition and how we think about this. What it means to us is displaying ads or content based on insights derived from past user activity. I'm going to get into that in some more detail.

The other thing I'd point out, and I think we are going to get some new information later in the day on this, users are telling us that they prefer relevant advertising and ads that fit their interests.

To start here, I'd like to talk about what the world might be like if we didn't have the ability to target based on insights. So, when a user comes to

Yahoo!, they'd be prompted to sign in, they would receive generic ads, potentially even Clorox ads, and national news, news that may not be as interesting.

When the user actually does come to Yahoo! today, they often receive a personalized greeting, they receive news that's custom tailored to their interests and they would receive ads that are actually relevant to their interests.

So, how do we do this today? There are really four primary ways that we inform the insights that we use to target advertising and content to users. We use content consumed, ads clicked, search keywords and search clicks. And what that information informs are categories like the ones that you see on this side of the page here. So, the information is used to categorize broadly into these interest segments.

How that categorization works depends upon the segment, but we focus on two things. We focus on recency and we focus on repetitiveness or frequency. One of the things that's worth noting is that in many of these categories, the interest of the consumer changes very quickly and, so, we're constantly refreshing the categories based on the recency and the frequency of the information.

So, one of the questions we get all the time

is, well, you have all this interesting information, what does the user get in return? I'd like to talk a little bit about what the user gets in return. Let's start with the fact that Yahoo! today is in the number one or number two position in 26 different vertical categories. A sampling of those categories you can see here. In almost every case, this content or premium service is being provided absolutely free of charge to the consumer because it's being paid for by targeted advertising.

And we're not just resting on our laurels here either. We have some examples here today, I'm not going to read through the slides, but we're investing tremendous energy in improving the products and services that we provide to consumers and, again, this is paid for by targeted advertising. So, we've had some highly regarded mail releases recently. We can talk about some of the new features in our search business and some newer properties delivering information that consumers are interested in.

In summary, I want to thank the FTC again for having us here today, and I'd like to wrap up by pointing out again that we take the trust that consumers place in Yahoo! incredibly seriously. We believe that there's tremendous value being provided to consumers who are participating in our various properties and this trust,

along with our ability to deliver targeted and relevant advertising to consumers, provides a better consumer experience with less cluttered ad pages and more relevant advertising, as well as better products and services for the consumers.

Thank you very much.

(Applause)

MS. KRESSES: Thank you, Mike. Tim Armstrong from Google will speak next.

MR. ARMSTRONG: So, I just want to thank the FTC for having us here today and I want to do a few things. One is just give a basic overview of Google's ad business and then talk a little bit about DoubleClick since it's already come up multiple times today.

I'm President of North America Ads and Commerce for Google and I've been at Google for about seven years and really before Larry and Sergey were Larry and Sergey.

One of the things I wanted to spend a little bit of time before I get into Google's business is just describing, from our point of view, how important this topic is. I think user trust and loyalty is probably the number one thing that we concentrate on at Google and I'll give you examples in our business of that. In general, for people who have longer memories, I think if you remember back in the year 2000, 2001, 2002, you know,

the web for users was a really tough place to be, mainly due to the advertising that was on the Internet in those days.

One of the competitive advantages Google has had is by focusing on user trust and privacy. I think we've actually been able to grow a nice business in search and we are hoping to get into the display ad business. But our business really does start with that.

One of the concepts that we introduced in that time frame was really about relevancy and really serving less ads, having a better user experience on the Internet, and our businesses today really resolve around a high level of user privacy and trust and a high level of relevance.

Today, Google's business model does actually come down to the word "trust." I think, in essence, our entire business, both on the consumer side and on the business side really is competitive in nature from the fact that any user could basically stop using our services with one click.

The same thing is true on the advertising side of our business, and this is a really important point. The vast majority of advertisers signed up in Google's systems are able to instantly cancel their contracts with us. So, when you take a step back and think about user

privacy and user trust, Google has put a tremendous amount of pressure on ourselves to deliver privacy and trust because if we don't do it, I think we would see a big change in our business and, potentially, overnight. So, how I'm going to describe our business, I would just hope that you would keep that in the back of your mind.

Then the second piece is around how we design our products and services. Our products and services are designed with two main attributes in them. One is a high level of transparency and a high level of transparency meaning you know what you're getting into when you sign up for things. We try to collect the least amount of information in the process, but make it really transparent what you're doing.

The second piece is really user choice. So, even if you do want to sign up for our products and services, what are the user choice elements that you have and are able to opt in and opt out of things?

So, advertising in Google, we have two main products at Google. One is called AdWords and it's for advertisers and one is called AdSense and it's for publishers. We have hundreds of thousands of partners and advertisers on these products and services.

AdWords, in essence, and the simplest way to think about it is very contextually or content-based. In

general, if a user goes to Google Search and types in the term "hybrid SUV," it's likely that we're going to put ads that are very relevant to the term "hybrid SUV" up on those search results pages. And if you use Google, I think you're used to seeing those.

The second piece of our business, the ad business that we launched really around 2002 or 2003, is the Content Network, which is really AdSense for publishers. And, in essence, that same user who might go to a content -- let's say a car review page, who reads about hybrid SUVs, they'll probably see an ad that's been relevantly served from Google based on that content.

So, to be crystal clear about this, the vast majority of Google's business today is based on content and not as much based on the behavioral targeting that has been discussed today.

The web is changing in terms of types of content that's on the web and I think we're continuing to update our products and services around how the web is changing. But we update our products and services really with a basis of privacy and user trust at the core element of those changes.

The DoubleClick piece, in general -- and for Commissioner Leibowitz, I'm glad he brought up competition because I think Google is seen as being a

really large player and in the Internet space, I think we're a very small fish in a very big pond in the display advertising business in general. And the people who were also mentioned who have done acquisitions in this space, some of them are actually larger than us from a market cap and business perspective. I think that we would want to be able to be competitive in the display business. So, we're excited to actually work with the FTC to try to close that deal.

DoubleClick, as platform, really allows customers to do a couple things. One is to basically compete in the display space as a publisher or an advertiser and allows people to, in essence, serve and track advertising. The key point on user privacy and trust here is that DoubleClick does not own the data that it serves, that the customers, publishers and advertisers actually own that data, and DoubleClick relies on the customers, the publishers and advertisers, to use that data and to really work in that.

In closing, I think we have stated publicly many times how strongly we feel about user privacy and trust. I think today, at the FTC, that's really the subject matter. We're happy with it. We think the Internet is a much better place because of that.

And I wanted to just close with four kind of

points. One is that we will continue to work with any group that wants to increase privacy and user trust on the Internet. We've been open about that. So, we are happy to take any proposals and discuss that.

Two is that there's a continuum of practices on the Internet and we hope the FTC basically looks across the continuum and helps companies who are doing it right do it better and helps companies that aren't doing it right figure out how to do it better.

And third is to kind of tread lightly. I think there's a tremendous amount of user benefit. Google has helped hundreds of thousands of content people launch new properties on the web based on these services, and we hope that the FTC recognizes that value and will continue to allow us to do that in a way that's really good for the world.

And the last piece is just on privacy. I've been, again, at Google for seven years. I also have been in the Internet space since 1994. Privacy and trust are probably the two words that are going to make the Internet the healthiest in the future, and as important as that topic is today and the businesses that are up here today, I think it behooves all of us to kind of focus on this issue and really make sure that a healthy web and a trust and safety web is going to be the best

business outcome for all of us long-term, and thanks for having us down here today.

(Applause)

MS. KRESSES: Thank you, Tim.

And, now, Chanterria McGilbra of Netmining will speak to us a little bit about her experience in working in the Belgium markets.

MS. McGILBRA: Good morning, and I'd like to thank the FTC for inviting Netmining here from Belgium. Brussels, you're right.

As I was on my way here, I was wondering, I said, you know, they're probably more interested in the chocolate. So, I didn't want to disappoint, so I did bring some Belgian chocolates.

So, just to get started on why we're really here, basically, because we're a Belgium-based company, we are actually driven under EU directives. What that means for us is that, one, many of the luxuries you experience here in the U.S. in terms of behavioral tracking, we don't have. So, we had to be much more innovative in terms of how we actually participated in this space so that we were not only compliant in the EU, which is obviously our most important compliance since we live in the EU, but we're also compliant here in the U.S., because many of our clients, as you'll see at the

end, are U.S.-based clients.

Some of the ways in which the EU Directives are different, one is no IP tracking. We have to have permission based data collection. We also have informed opt-in and possible opt-out one very piece of data we collect. We also -- although at the national or state level -- there's 28 states now in the EU -- although states can be more restrictive in their regulation of behavioral technology data collection, they cannot be less than the EU Directives. So, if you look at the EU, it's the Federal Government, the national are the state level.

How does this impact our business? Basically, we're restricted to cookie-based profiling. We have no other way to collect data. And, obviously, as many others mentioned before, this can be, and usually in our case, is anonymous data collected.

We also are site specific score-based individual profiling -- it's a mouthful. But basically we are not allowed to bounce around on various websites to collect data because our business model is such in which we collect data only for clients who are paying for it. So, we only collect data on one site at a time.

We also have behavior driven interaction. In the EU, we're not allowed to do pop-ups, random pop-ups.

It has to be interactions that are based on a proven or a demonstrated interest of the online customer.

Here's our business model, and if we could draw up one picture to show you how this all works, this is how we fit into it. Essentially we have the Googles, the Tacodas, the Yahoo!s of the world who do a wonderful job at what they do, bringing people to your website, aggregating that data, analyzing that data. They actually do a wonderful job.

We come in at that point and what we do is we focus on what we call the behavioral selling. So, we really are set up to support the selling aspects of online advertising.

So, once the individual gets to your website, what do you do with that individual? I mean, it's essentially your largest retail store in the world and very many companies don't have a presence once the individual gets online outside of pop-ins, and they hope the pop-ins are right.

Through our score-based profiling, we can determine not only demographic information about the individual through click stream data tracking, but we can also determine primary, secondary and tertiary product interests. Once that information is collected, then our system interacts with that individual online just one

time, sometimes twice, depending on the company, and we motivate the individual to leave their contact information. Every interaction that's presented has a privacy policy on it, unless the client says no. So, because we're EU-based, we move forward based on EU Directives and, so, we place that on each of our interactions unless the client says: "no, we have it on our website, don't bother."

Once the information is collected, then we funnel that directly into your already existing CRM system. From there, your company can then follow up on the lead, and I have a case study on how that was done for a Dodge dealership here in the U.S.

So, this next slide shows very quickly, you have five individuals on your website and you can see immediately we start detecting product interest right away because that can be done anonymously. That's click stream data, we all use it.

Next we have scoring -- what we call real-time buying interest, and like Yahoo! mentioned, we use recency, frequency, but we also track based on monetary value of the product that they're interested in. So, this actually generates what we call a lead qualifying score. This determines if the individual on your website is a qualified lead or not.

Here's an example of what we did for a Dodge dealership. Dealerships are really key for our industry or what we do because they -- up until recently, they have a fairly high cost per sale, and so, they're incredibly motivated to use us and you'll see at the end we have a lot of dealerships as clients currently in the U.S. as well as Europe.

We are essentially an ASP Model, so there's no hardware, software maintenance fees. We provided them score-based profiling and identification of quality leads. We also provided the first, second, third level product interest as well as leads directly sent into their CRM System as stated before.

The outcome: 67 leads detected and followed up by the sales team; 21 closed deals within six months, that's a 32 percent conversion rate. For any company selling items online, that's phenomenal.

What's the ROI to that company, 192 U.S. dollars per every one dollar invested in our company, hits into showroom solution.

I short of came here thinking, wow, we're so limited compared to the American companies, but I haven't heard anyone talk about return on investment and how that actually works here. So, I'm interested -- I hope we can discuss that later. Through all of this advertising,

through all of this privacy conflict and interest that has been generated, I heard it on CNN this morning, it would be very interesting to see how this all rolls up to benefit the actual consumer, which is what we're here to discuss.

So, I'd like to thank you all for your time. Again, thanks to the FTC. I'm going to actually sit these chocolates right out on the table, so you can share. Have a good day.

(Applause)

MS. KRESSES: Thank you, Chanterria.

And, now, we'll hear from Pam Horan of the Online Publishers Association.

MS. HORAN: Thank you. I want to thank the FTC for their time today. My name is Pam Horan. I'm the President of the Online Publishers Association, and the OPA represents and is made up of leading online newspaper, magazine, broadcast, cable and pure play publishers. Mark Westlake here from HowStuffWorks is one of those pure plays. And all of our members uphold themselves to the highest level of editorial quality, integrity and accountability.

By supporting publishing principles that reflect the traditional values of separating editorial and commercial content, OPA members enhance the trust of

the web with consumers that are coming to get information every day.

A recent study showed that 44 percent of 18 to 34-year-olds get their daily news through the web. Internet users naturally are drawn to free content, and that's really the DNA of what the Internet's all about, and we've heard a lot about that today. OPA members have a variety of business models, but the dominant one is an advertising-supported model which allows them to provide all this information for free.

Even outside the realm of advertising, the ability to associate website activity with anonymous users is vital to the online publishing industry. We've heard a bunch of examples this morning, whether it was the Amazon example or whether it was the Washington Post example, but analytics really provide publishers with the necessary understanding of how consumers interact with their website in order to serve up an experience that will allow that individual to have the most positive one, which often is in the form of personalized content or the ability to provide special tools and services.

But a real value exchange exists, as we've talked about, in terms of the consumer recognizing that in exchange for all this free content, whether it is on one of those major media sites that I showed you that are

the members of the OPA or even smaller sites, there's a value exchange that they expect to see advertised in exchange for this information. For many OPA members, targeted and behavior advertising are particularly effective methods in serving appropriate and relevant ads to the consumer.

I think a good example of that is the OPA conducted a study of video users several months ago, and this is one of the fastest growing areas on the web, and what we looked at was the consumer or the individual who's visiting sites aptitude for advertising. So, if you look at that third bar, over 50 percent, so the majority say they prefer watching online ads in exchange for not having to pay to see their favorite online video. So, they recognize that value exchange, as I was talking about.

Fifty-four percent say that advertisements are a fair way for websites to provide free professionally produced video, and then, ultimately, 56 percent really are talking about that relevance of the ad being associated with the content that they're looking at. So, there's a real value exchange that we see.

Technology really is the foundation of the Internet and is the foundation of providing a positive user experience. Members like the OPA collect two

different types of information. One is known, and this is where the individual has actually provided personally identifiable information, so PII, and this can be in the form of an email address or a first name. And then there's the anonymous user, which is really in the form of a web browser, and we've heard that earlier, that that's really the first party cookie. An example would be, for example, with the Washington Post. If you're inside the Beltway, you're going to get a different homepage than if you're outside the Beltway. So, that content is going to be more relevant to you.

All of our members have published privacy policies and, to no offense, I think that the comment that was made earlier about it being buried, I think one of the things that we find consistently, it does always appear at the bottom of the page, so that we've trained the consumer, if they do want to access it, that's where it is. Then if there are any changes that are made to those privacy policies, the user is always notified through email and we never share personal identified information without the user's permission. Ultimately, we do not collect PII from children.

The other things that we don't do is we don't download applications to users' computers without that user's permission. We don't change user's computer

settings without their permission and we certainly do not tolerate spyware.

So, just in closing, I think that as we've talked about that trust is really critical and our members really recognize that. So, there's a respect that's been formed and an understanding of the value exchange. So, we really respect, through the privacy policy, how that information is exchanged. Then, as I said, OPA members don't tolerate unfair or deceptive practices in any aspect.

Thank you very much.

(Applause)

MS. KRESSES: Following on that, Mark Westlake will talk about HowStuffWorks.com and the special market for small content publishers.

MR. WESTLAKE: Thank you very much and thank you to the FTC. I'm Mark Westlake. I'm the EVP of Sales and Content for HowStuffWorks, and I promise you I'm not going to do a presentation on how behavioral targeting works, but I am going to tell you a little bit about us and really what does behavioral targeting mean to us.

We're a small site. We've been picked by Time Magazine for two years in a row as the site you can't live without and we've won a lot of awards, but we're small, you know, much smaller than Google, much smaller

than Yahoo! and some of the other sites up here. We do roughly 60 million pages. We reach 10 million users. Our goal is to help people become smarter and make better decisions through providing them detailed explanations, expert reviews, consumer opinions and price comparison across a wide variety of topics, and it's advertising supported.

What does behavioral targeting mean to us? Well, it means more revenue. It's kind of like a cycle. You know, it drives more revenue for us which drives better content. We use the money to create more content, which drives more value to the consumer, which hopefully they share with their friends that drives more viewers to us which eventually leads back to more revenue because we have more people coming to our site.

So, we look at behavioral targeting as driving incremental revenue. We're one of the few sites here in the marketplace that uses both Tacoda and Revenue Science. But the way we can compete in working with Tacoda on HowStuffWorks, they track our users once they leave our site. As you can see here from this chart, 75 percent of our users are identified by Tacoda outside of HowStuffWorks. So, that gives me that incremental reach that allows me to compete with some of the big, big sites. It also helps me drive more revenue than what I

have in a small site like HowStuffWorks.

Now, we sell our site contextually, which is targeted advertising, putting a teen-targeted ad in front of teen content or an automotive ad in our auto site. That's what our targeted drives, a lot of yields. It's profitable. Then we take our excess inventory and work with the ad networks and basically sell remnant.

What we found with behavioral targeting, it sits in the middle. It gives you -- you know, they drive a lot of good quality advertisers at a very good rate for us, which allows us to capitalize on that. We're also working with them on something unique and different which, you know, with a small site you have limited inventory -- how do we get more inventory? Well, one way is to work with the networks to sell our user off of our site. So, you know, there's a -- the New York Times started this back in the late 1990s -- Surround Session, which when you came to the site, no matter where you went, you would serve the ads. We're experimenting with Tacoda and some of the behavioral targets on how we can do that for a small site so we can compete and be able to provide advertisers with a large amount of -- a bigger buy which drives more revenue to us.

And we also found that working with advertisers that it does help them on the ROI side. You know, we

found that they use it for direct response for branding, for launching promotions and it works very, very well.

We also found that it's also -- behavioral targeting is very good for content development. The data that we collect in working with Tacoda and RevenueScience, we can use that data to learn more about our users so that when they do come to our site, we can provide them a better user experience and try to use that data that, again, provides them kind of the information.

But one of the things I think as a whole for small publishers, since I am representing the small guy here, we look at behavioral targeting as being very, very good for small publishers. It drives revenue for us, it helps us learn more about our users so that we can provide more content. But the concerns are, yes, there is an education for consumers on using cookies and the control of cookies. We think it's important that we educate these consumers because if they take those cookies, that prohibits me from targeting them which prohibits us from driving incremental revenue, so it does hurt us.

And it's important that this data is anonymous. It's also important that the partners we work with adhere to the privacy policies and the industry can stay on top in working with the NAI and so forth. We also need to

make sure at the end of the day that the user experience, that these users come to us, they're not upset -- and we deal a lot in the education market, we deal a lot with international traffic as well as the U.S. traffic, and we make sure that the user experience is the best that it can be because that's what drives incremental pages which, again, drives incremental revenue. So, we've got to make sure the data is used correctly and that if it's not used, that we address it immediately.

The trade-off is for behavioral from a small publisher's perspective is provide the users with free quality content as long as it -- which can drive revenue for us. If that doesn't happen, the small guys like us are going to just be nonexistent.

So, again, thank you to the FTC for having me here, and I hope this was helpful and we'll be here for more questions.

(Applause)

MS. KRESSES: Thank you, Mark. Ralph Terkowitz.

MR. TERKOWITZ: I am not going to do any slides. What I really want to do is not talk to you as someone from ABS Capital where I am an investor in media and communications, but to take sort of my historical perspective in this field. I was the founder and CEO of

washingtonpost.com and I must say, I thought some of the background on the Post was quite accurate earlier today, and take that, combine that with my time as a chairman of TRUSTe, which I got involved in early because as a publisher, I did see the need in value for a set of independent guidelines and trust marks that helped to guide publishers in the industry in general.

Now, you've heard a lot of people and a lot of perspectives on this problem and I think the best thing I can do is try and tie this together in a sense of providing a publisher's perspective of this whole kind of targeting.

So, let me start with a little bit of history, and again, you've heard some of this. Behavioral targeting is really not a new industry. It's been around, as Trevor indicated earlier, as long as there have been various means of reaching consumers. It's been used in direct marketing, it's been used in telemarketing, it's been used through publishers. They use both personally identifiable information and geographic information, whether it's neighborhoods, et cetera, purchase history and other demographics to target advertising and target content.

Why do they do that? Generally, as you've heard from everyone here, they do it because it works.

They do it because, generally speaking, targeted content and targeted advertising is quite appealing to the consumer and it's certainly measured by the response they get. It also has a number of other consumer benefits, which I think become really important as you think about the Internet, generally speaking.

It enables publishers -- and I think you need to start by understanding that publishers aren't simply, well, how do I get a tiny bit of content and wrap all the ads around it? A number of publishers have important things to say, but advertising is an important means for paying for that. Targeted advertising enables them to deliver that message more effectively and with fewer ads, which is really very important for those publishers.

Secondly, if you think about what you've heard today, and we talked about in HowStuffWorks, the value of content-based advertising and how effective it is, how many people do you think would like to advertise around a major story like the Walter Reed situation? It's a very important situation for all of us in this country. It's also, in its own right, not a topic which is particularly contextually relevant to what advertisers want to say. Things like targeted behavioral advertising enable publishers to effectively deliver that kind of content to their audience.

Now, having said that, there are certainly privacy issues that are raised with behavioral targeting, and in my mind, even though we've been talking about this being a PII-based issue, it's much more than PII. There are consumer concerns and valid consumer concerns about invasion of privacy, whether or not any personally identifiable information is used. I think it's time to not consider targeting and PII in the same breath, but rather recognize that any privacy information, whether it's anonymous or, in fact, personally identifiable, can create discomfort on the part of the consumer and, as such, represents a set of privacy issues that we do have to deal with. So, we need to abandon that PII/non-PII distinction.

Consumers do have a right to be left alone if they want to be and we need to provide them with those kinds of capabilities.

Now, I think it really comes down to the notion of consumer control as I think about this, if you will, an editorial decision. Consumers want to be left alone at certain times and other times they don't. If I'm researching a car, to take some of the examples we've seen earlier, I may very much want to see behavioral car ads because it, in fact, is relevant to a purchase I want to make. On the other hand, I may be on a set of

websites where I have much less interest in being tracked, and the consumer needs that editorial control, not the all or nothing.

Let me move forward from this sort of historical base of targeting in general and turn to the Internet. The Internet poses new threats around targeting that doesn't exist elsewhere. At the same time, it provides opportunities for new solutions beyond the kinds of solutions we've used in historic media, beyond the solutions that made sense for direct mail, because the Internet is such a different media.

So, where's the problem? The problem is that the barrier to entry in collecting consumer information is substantially lower online. It was expensive to target people in direct mail because you had to put all those stamps on all those letters. It's essentially much cheaper to be a bad actor online, and that's a problem that we need to deal with. Bad actors can abandon one technique and go on to others. Corporate players are more reined in by reputation, but it is a problem overall.

At the same time, we have new opportunities that arise from this because on the Internet our behavioral information is far more transparent and a consumer is far better empowered to make changes than

they are, in fact, in other kinds of media. So, consumers can, in fact, be informed about targeting in real-time and we've seen suggestions around that.

Cookie deletion and management can be managed by the consumer as opposed to by a third party all or nothing approach. There's an editorial process that could take place.

The result is a far more sophisticated set of models for consumer choice which enables the Internet to, in fact, support the kind of behavior we want in content while providing a rational both economic model and value for the consumer.

(Applause)

MS. KRESSES: Thank you, Ralph.

Carlos Jensen from Oregon State.

MR. JENSEN: Go Beavers.

(Laughter)

MR. JENSEN: I wasn't expecting to come here and talk about Oregon football. It's just one of the weird side effects of actually producing a good football program.

I want to thank the FTC for hosting this event and I want to thank all of you for being here and participating in this very important discussion.

As the final panelist and the only non-industry

representative, I am kind of tasked with bringing a slightly different perspective to what you've been hearing about so far. I put things into more concrete context.

What many of us in academia are concerned with in this space is whether users are treated fairly, whether privacy rights are respected, and ensuring that we have the necessary safeguards in place. That's what I have been working on at Oregon State for the last couple of years.

This is not something that we alone care about, the academics. We have great partners, both on the side of consumer rights and a lot of the industry folks who have worked very hard to make this research possible. TRUSTe and BBB have both bent over backwards whenever we've had any kind of information request to them. So, I don't want to say that what we're doing is different.

What brings me to this town hall is, like I said, to talk about some of the research that I've been doing for the last three years. What we've been focusing on is trying to generate a knowledge base, a database of privacy practices and data collection practices worldwide, what websites are doing with regards to end user privacy.

And what we do is we go out, we index --

starting from the top popular websites, we look at all kinds of technologies that they use and practices that they use including cookies, web-bugs, pop-ups, banner ads, privacy policies, et cetera, and we try to analyze them and come up with some meaningful warnings or statistical trends, things like that.

Some of the things that we're interested in is examining the evolution of practices over time, and I'll give you some examples of that. Also, looking at geographic and industry trends, and I'm very glad that we have Netmining here from Belgium because we do find some very interesting geographic trends. And we also want to look at how technology adoptions changes as new technologies make it into the marketplace.

The whole goal of doing this is not to be obnoxious, but to actually provide useful data to everyone, all the stakeholders involved, consumers, legislatures, ecommerce and other researchers who are designing tools to help end users.

So, this is a very high level -- the summary of some of our findings. We're a research institution so our research is limited. We can't go out and index the whole web like people at Yahoo!, et cetera, can do. So, we have to kind of target our analysis and we start at the top most popular sites.

This just shows you how we've been growing. We're limited in terms of our attention span, but we're growing and we're very serious about offering a very balanced picture of what's going on online.

I don't really have time to talk about all of the findings that we have, but I just want to show some of the most relevant ones here, which is the historical trends that we're seeing in third party cookie use and in web-bug use. Third party cookie use are not all that prevalent, but they're a rapidly growing technology.

Web-bugs among the top most popular sites are incredibly common. Thirty-six percent of sites use them these days.

And the interesting thing is that we actually see a marked difference between what's going on in the U.S. and what's going on in Europe. In Europe, all these trends are reversed. There's a decrease in the use of third party cookies, there's a decrease in the use of web-bugs. And as we've heard from Netmining, that hasn't really hurt their business model at all.

So, think back to the first presentation that we saw this morning. Richard Smith asked you to think about the Washington Post and who was sharing information with the Washington Post or, rather, who the Washington Post was sharing information with. What we've done is

we've taken that model and we've taken it one step further. So, if you don't just do this kind of mapping for a single website, but actually do it for a whole ecosystem of websites, what do you get?

Often, when we ask users to make decisions about whether they want to share information with a specific site, it's accompanied with a disclaimer about and relevant partners or trusted partners and who are these trusted partners.

So, what we've done is we've tried to develop a model of how information is shared over the Internet. And what we've found is that these information sharing networks are not isolated islands; they're interconnected sites. This is an example from our data set from 2005 where we find over a thousand servers, 1,700 servers, collaborating in some way, sharing information in some way.

And I wish you could see some more details. The little boxes are color coded and sized according to the amount of information that's collected at each of these sites.

If you go in here and look at who these people -- or these companies -- actually are, you will find the people that you kind of expect to find. But we can actually provide users with this kind of data now. If

you go to this site, this is the full branch of how your information will spread.

So, for more information, we have a paper that includes a lot of the statistics here, and I want to thank the FTC again for hosting this event and the National Science Foundation for providing funding for this research.

(Applause).

MS. KRESSES: Thank you to all our panelists for all that useful discussion. We're going to ask a few questions, Peder and I, and then we'll open up the floor to audience questions. So, a minute or two before we're ready to do that, we'll let you know so that you can line up at the mics and we can move through smoothly. Thank you.

MR. MAGEE: All right, I'll get the ball rolling here on our moderated discussion. I encourage the panelists to jump in when you have a point, once we get the question out there and someone commenting.

Dave Morgan of Tacoda, Dave, behavioral advertising depends upon drawing distinctions among different groups of people. Obviously, an advertisement for snow blowers is not going to resonate with many people in Miami. My question is, is it problematic to make those kinds of choices for consumers? Are there any

dangers associated with serving different advertisements to different segments of people?

MR. MORGAN: Yes, I think what it comes down to is there's -- the moment to be able to present an ad is a scarce moment in consumer's attention, so I think the question is -- there's going to be an ad because it has to be paid for and someone has to provide the free content. The question is, do you give an ad that is largely meaningless to most people or has a basic amount of meaning to everybody or do you try to find some way to make it more relevant? The snow tires in Miami, that's an easy one. You know, if you can use a very basic technique and you try to guess at where the Internet server might be from, there may be a 60 percent chance that you might know a general regional area like the Washington area. So, you could say, no snow tires there.

You also could determine that the browser, you don't know who the person is, it could be ten people looking at the same browser, but you may have information as browsers look for a lot of information about cooking. So, probably a cooking ad is most appropriate.

I'll tell you, and we've obviously talked about this and pretty open, that where I think there's issues and I think everyone has to tread lightly because I think when you start getting close to where a consumer may have

issues or when you start getting closer to things they might think is creepy and I think then it's the question of, are you getting into information that -- and I sort of use like my mother rule or the common sense rule. If my mother would be uncomfortable with it, then I don't think it's something we should do.

So, it's really being careful around things like health conditions and other areas. And I'll say this is something -- we, in the industry, are always looking for input and guidance on how we can be better. I mean, I've seen some comments about children's advertising. Well, I don't know any companies that are working in children's targeted advertising. We're working with large media companies and large advertisers and there's not a person that doesn't think that's the third rail, I'll say, coming from New York, it's just areas that, you know, you just absolutely keep away from.

So, getting back to the basic question of discrimination, do we try to show different ads to different segments of people? Yes, we do, and we do that because people now want to be -- I said it's all about me. They want to be communicated with some sense of what they're interested in and they're tired of being communicated to as if they are no different than anybody else.

MR. MAGEE: That's an interesting point. Is there a mechanism by which those consumers can access their online profile and say, you know, I realize I live in Miami, but I actually drive up to New England and go skiing and I would like ads on snow tires?

MR. MORGAN: Well, a number of companies are testing things there, and I think that's one of the great things about -- it was talked about earlier. The competition here is very fierce in this industry. There's a lot of money being invested. So, a number of companies are testing techniques where you can make information available to consumers and they can adjust it. A lot of times it's not always as -- you know, it's not always just as clear cut as 'are you in a demographic bucket of people,' but just have browsers that have done similar things to you, your browser, you know, also looked at similar kinds of ads.

But I know companies -- I think WeatherBug is one which has actually tested -- been testing a chance for people to actually opt in to certain kinds of information.

So, I think we're going to see innovations like that. I mean, I think -- you know, we just announced at AOL, providing more and better notice. We think that we can do more than just privacy policies and we can

actually deliver ultimately hundreds of millions of banners a year to give more notice.

MS. KRESSES: Anybody else want to comment on that question?

MR. TERKOWITZ: I would simply add that what makes behavioral targeting work is very often what people do is a better indication of their interests than what they think they do. So, frankly, the snow tires in Miami is almost a non-issue because the odds are that that person in Miami that's looking for snow tires is probably reading ski magazines and other things that predict that behavior. Even if I'm in Maine, if all my reading is in pool and garden supply, the odds are I'm not a good customer for snow tires as well. That plays off, as well, on the content side.

So, I've spent many years looking at the question of how can publishers do a better job of targeting content, and it turns out what you read and what you look at is an awfully good indicator of your interests.

MS. KRESSES: Thank you very much. Let's switch gears a little bit. Chanterria, we'd be very interested to know -- you talked about incentivizing the consumer once they get to the individual site to opt in to provide information. How do you motivate consumers to

provide that opt-in?

MS. McGILBRA: Well, you have to remember that, first of all, we only work one side at the time. So, this means the consumer has voluntarily gone to the site, either through a pop-in or some other form of advertising, and they have chosen to be actively on this site. That is the only way in which we track the consumer's behavior to determine if they are eligible or if they are a good quality lead to receive an interaction.

Once they receive the interaction, as stated before, we actually place a privacy policy on every single interaction unless the company says no. Some companies in Europe, generally they follow the Germany standard of privacy policy. However, there are some countries which are much more stricter. For instance, we had a dealership out of Italy say, no, it's not good enough to just ask them for their name, email and phone number, they have to click that they have read the little privacy policy to actually opt in to leave their information before we will take their data.

So, once that's done, that actually gives us the opt-in -- that's the actual opt-in on many cases. Some countries say the fact that it's on there, we assume they read it. The fact that they've put their

information in says that's the opt-in.

The incentive actually comes from the client. So, if I'm on a car dealership, as Ralph mentioned, I absolutely want to receive interactions which say here is -- come in for a test drive and you can have a rebate of $350 off your car, or come in, schedule a meeting with one of our salespeople and see if you can prequalify for financing. I mean, all of that, that's an incentive to leave your information. Companies can use whatever they choose. It's no different than walking into a department store and seeing 50 percent off of Manolo Blahniks. So, you know, it's whatever incentive the company thinks is necessary.

We don't create the incentive. We just create the interaction.

MS. KRESSES: Great, thank you very much. Given the time, what we thought we'd do is go ahead and open the door to audience questions so that we can --

MR. MAGEE: We've got mics in either corner here, so please just line up and ask whatever questions you have for our panelists.

MR. CHESTER: Jeff Chester. I'd like the panel to reflect on whether or not it's okay to collect all this information. I want to quote from Dave Morgan, a paragraph of Dave Morgan, in a new report, HD Marketing

2010, that the ANA, the IAB in the forays just put out, Dave Morgan is saying -- this is both a quote and paraphrase -- data mining is a great example that enables individual targeting.

Let me quote you from his statement. "Every webpage is individual views. Every word typed in a search query box, every video download and even every word in email may create one more data point that a marketer can leverage and use to more precisely target the audience with customized media placement and messaging."

What content might be off-bounds from individual consumers with behavioral targeting?

MR. MORGAN: Well, I can tell you, as I think has been stated a couple times and I think it's important, this isn't a question of technology capabilities. I think everybody understands that there's an extraordinary amount of technology capability, that you could talk to every person in a personally identifiable way, if you wanted to today, using publicly accessible phone numbers and street lists. I used to work in political campaigns, so I, you know -- but it's not just what's technically possible, I would say it's what's right or what makes people feel comfortable.

So, the point in that research report was to

try to understand -- does understanding consumers' paths make it easier to understand what's the most relevant offer, and the answer is yes.

So, what kinds of information aren't appropriate? Well, I'll tell you the kinds of things we have done at Tacoda, and also, this is part of what AOL's doing. I mean, there's sensitive data we don't think is appropriate to target ads to, even though it's anonymous. First, we started by anonymous and not using any personally identifiable information. So, you can't actually know who the person is, which also actually creates an issue in trying to ever -- I should have thought of this in my last question -- ever expose the browsing behavior because we don't know who the person is, so it's almost impossible to actually verify when someone comes as to what the information is.

So, the guidance that we've gotten, which I think has been really good, is cancer, HIV, medical conditions. Those are things we just keep away from and we have no intention of getting near. And every day, we're reevaluating other things in that area. Children, sexual preference, all of those.

There's probably a number of you -- and I know, Jeff, you're aware of this -- there's a lot of industry efforts going on right now trying to actually bring a

little bit more clarity to what are the appropriate areas of sensitive information. One of the things at Tacoda we don't do is we don't touch search data and we don't touch search data because I think that you have to filter every bit of it to know what's not personal and, therefore, that creates a challenge, and it's something that we've never gotten near.

But, most importantly, and I think this is what we really need to focus on, which is it's not what's possible, it's actually what's happening in the marketplace and what's being done. We don't need to know who a person is, we don't need to know a specific search to be able to deliver a better advertising experience. Advertising on the Internet and advertising in general is so clumsy and is done so poorly that just doing it a little bit better, just making sure that there's fewer blinky, flashy ads that are trying to -- find and reconnect with your high school sweetheart or something like that we all keep seeing, and being able to deliver more relevant ads, I think that's our extraordinary opportunity and I think that's what 99.9 percent of the companies that are operating in this world are doing.

I come back to my Clearfield, Pennsylvania, example. People in my hometown have news and information that was never available when I was small. My hometown

now actually has no pediatricians. They have to drive an hour to get a pediatrician, but there's a free ad supported Web MD in that town now and there's a lot more information. So, that's the kinds of stuff we're focused on.

MS. KRESSES: If you could let us know who you are.

MR. MENDEZ: Yes, A.B. Mendez at FBR Capital Markets, a couple of quick questions for Tim and Mike. Tim, within the premium version of Google Apps, the paid version for SMB customers, I have not seen it personally, do you place targeted ads within the Gmail section of that service or do they have the option to receive or not receive contextual ads?

MR. ARMSTRONG: I don't think we have any current plans in the Apps space to do advertising at this point.

MR. MENDEZ: So no ads are placed within the paid version. So, that kind of brings me to the question, I've heard from numerous different sources that there's a lot of complaining about privacy concerns, but when you give consumers the option to pay for a service as opposed to receiving contextual ads, 99.9 percent of the time consumers are not willing to pay. So, there's a lot of complaining, but people, given the choice between

privacy and free services, people will take the free services.

So, it kind of begs the question, also directed toward Mike, for example, like as a user, I have a Yahoo! Mail account that I've been using since college, which is longer ago than I care to admit, and to me, it's sort of locked up. What if I wanted to download one file -- maybe I can and that's just ignorance on my part -- if I wanted to download all of my historical email and pay a fee and say, okay, I want to be able to put this on my computer, or pay a fee to use it on a host basis and not receive any sort of targeting, not have any of that information shared, is there an option of a paid service that would allow that? I'd direct that to both Tim and Mike. Is there anything currently available or plans to offer that kind of service and, you know, what kind of uptake do you think you would see?

MR. WALRATH: So, I think it's a pretty specific question and I don't have a specific answer for you on what you can do specifically inside Yahoo! Mail. I think that it's critically important to understand that the tradeoff here, the conceptual tradeoff is if the advertising model were to go away, then the model becomes a subscription model. It becomes a pay-for model. And I think your point about consumers tend to choose to trade

-- there's a value exchange there and consumers tend to choose free services, free content.

I'm also a long-time Yahoo! Mail user and one of the things that I've enjoyed over the years is that Yahoo! Mail has consistently been increasing storage limits and building functionality and adding new features that make it a far more valuable experience. I think we invest tremendous resources and time and money in improving all of our services in this way and that is paid for by the targeted ads.

MR. MENDEZ: Okay, but as far as you know, there is no I can pay $20, $50, $100 and download the entire file or pay a subscription fee and basically lock up that data so that nobody but me will ever see it.

MR. WALRATH: We'd have to get someone with a little more specific mail domain --

MR. TERKOWITZ: But you can do that for free. I mean, all you have to do is pop it into another mail account and you can certainly do that with either one of those providers. They don't restrict that.

MR. MENDEZ: Okay, that's all very helpful. Thank you.

MS. KRESSES: Thank you. Yes?

MS. GRANT: Hi, Susan Grant from the National Consumers League. A comment and then a question.

My comment is that the tradeoff between getting something free or giving up personal information to get advertising is kind of a red herring because of the problems that we've heard about before, the issue of consumers really not understanding exactly what the tradeoff is because they can't tell from privacy policies and other information that they may be given about how their information is going to be used.

My question is for really all of the panelists to whom this might be relevant. It was really interesting to hear how behavioral advertising works and works well in the EU with the EU Directives. I wonder if any of the panelists here think that the opt-in model would work well for them and, if not, why not?

MS. KRESSES: Do we have a volunteer to start on that?

MR. MORGAN: I'll jump in first. I've done a lot of work with publishing companies in Europe and, so, I've dealt with the EU restrictions. I've also dealt with the German restrictions. One thing certainly marks a lot of the European markets and online. There is dramatically less free content and free services available to European consumers online than there is in the United States.

I'm not an economist, so I can't isolate each

single piece of it, but it's not because of a lack of technology infrastructure. In fact, in many of those countries today, there's actually more broadband penetration than there is in the United States, and it's not for a lack of mobile telephony either because, in most cases, that's past the United States.

But what I will say is that the companies that can provide free tools, free services, free content are not doing it in most of the European markets at the level they're doing it in the United States. There may be other issues for it, but if you think about it in the United States, as Randy Rothenberg mentioned earlier, the online advertising will generate about $20 billion in revenue or subsidy in the United States this year to content and tools and services.

If you look at the capital investments that companies are making, and in addition, I don't know that number offhand, but it's probably in an incremental $10 billion, it's about $30 billion being invested probably in the United States for free web tools, content and services. That's about $200 per consumer that uses it. So, I would posit -- as I say, I'm not an economist to nail it exactly, but I would posit that one of the biggest differences is that free content is not being created because we're not seeing that $200 subsidy coming

in and I think that some of the restrictions are probably one of the reasons.

MR. TERKOWITZ: I think there's another challenge, too, Dave, which goes to this question of free versus paid, which is really an obligation I think we all have and the FTC has as you look at this going forward, which is we really have to continue to work -- and you see it in some of the proposals, the one that came out of AOL, among others -- to drive transparency, to drive education and to create policies that deal, if you will, with those actors who are not interested in transparency and are not interested in education and ease of use. Because those things have to happen.

If you have an environment where it's free but it's hard to figure out what the tradeoff is, then people can make a bad decision. I do think we have obligations. I think there are ways we've done it. Certainly, we've done it at TRUSTe with websites to make this kind of information far more transparent so consumers understand, in fact, the bargain that they are striking.

MS. KRESSES: Thank you. Yes?

MS. MONTGOMERY: Yes, Kathryn Montgomery, American University.

As a kind of follow-up to what you just said, I'm hearing some kinds of content mentioned here that are

considered off-limits or at least sensitive and troublesome to some companies. I want to know, it looks like that line may move from time to time, that this is a rather dynamic area. How do consumers know what is off-limits and what kinds of content an individual company will not collect? How is that information made clear to consumers and how consistent is it? Beyond what may be stated self-regulatory guidelines, I'm talking about operating procedures, how consistent is it within the industry and across corporations?

MS. HORAN: Well, from the OPA perspective, we do have a range of members with different privacy policies, but I can say generally speaking they all publish the types of content or types of information they are going to collect and how they're going to use that information. Some of them -- if I look at, for example, CNET has very extensive, very clearly written, you do not need a Ph.D. to read this and understand how the information is going to be used.

So, I can say for the members of OPA which represent these big brands, there's a great deal of transparency because, again, as I mentioned during my opening, the trust is so critical to support this business model, that would not exist without having that value exchange.

MR. WESTLAKE: Yes, and I'll add to that. Being a content site and a small site, the most important thing for us is that user experience, especially because we have such a small number of people coming to our site. If we're going to upset them or give them a bad user experience, they're not going to come back and, more importantly, are probably going to tell their friends not to go there.

When we have a problem, we get comments and it's like all through the educational market, you know, we get, hey, I saw this, I saw this, and we address it immediately. But I think it's up to the publishers from a content perspective to adhere to making sure not only what we say, but practice what we say in monitoring the performance, monitoring the content. We have strict guidelines for types of advertising that can even come up on the site because we know we're reaching a wide variety of people and we want to be the highest quality. Therefore, we've got to make sure we adhere to the highest quality standards.

MR. MAGEE: I think we're going to just take one more question. Gentleman?

MR. HEGER: My name is Ollie Heger. I'm German. Here we go. I'm with WunderLoop, a targeting technology provider in Europe basically. I just want to

clarify one thing.

If it comes to targeting without any PII-related data, of course you don't have to opt-in. Netmining needs an opt-in as soon as they generate leads which basically refer to individuals -- first. Second, what's happening right now in Germany, this might be interesting in the way that government -- the government actually decided to allow privacy -- how's the word for that -- privacy authorities that are actually checking on the privacy implications on that, to come up with a certificate that can be issued to publishers as well as to technology providers.

MS. KRESSES: Thank you. Okay, I think -- Carlos, you wanted to comment a minute ago?

MR. JENSEN: It was just a follow-up on the previous question, which is from having done this research, I've been reading a lot of privacy policies and what a fun world that is.

(Laughter)

MR. JENSEN: But from a consumer's perspective, I mean, we've talked about here certain types of tracking or certain types of inferences that we don't want to make, things about health status, it could be religious affiliation, things like that. When you look at the privacy policies, you will very rarely, if ever, see any

mention of the kind of inferences that the companies are not interested in making. If they refer to policies as something they don't do, it's typically about atomic bits of information. So, we will not ask you for your mailing address, we will not ask you for this.

So, there's very little guidance to the consumer as to what may be done with that data, what kind of inferences are off-limits and which are acceptable.

MS. KRESSES: Great, thank you very much. That will end Session 2.

MR. MAGEE: We just want to thank all our panelists.

(Applause)

MS. KRESSES: Let's take a minute to stretch while we move into Session 3. Thank you.

(Brief pause)

SESSION 3: CONSUMER SURVEY DATA

MS. BRANDENBURG: We will now hear two presentations on consumer research in respect to the Internet and behavior and attitudes. So, I would first like to introduce George Milne, an Associate Professor of Marketing at the University of Massachusetts-Amherst.

MR. MILNE: Well, it's always a little dangerous trying to present right before lunch, but I'll try to not hold you too long.

Today I'm going to present some information on three surveys that I've conducted with my colleague, Shalini Bahl at the University of Utah. The title of the talk today is Information Exchange Expectations of Consumers, Marketing Managers and Direct Marketers. So, these are the three groups that I'm going to profile today.

The background -- privacy is very situational and the situational factors that we're looking at today are eight technologies that have been used over the last decade. We're going to try to understand that there are different preferences of consumers out there and we want to know how those consumers react to different technologies, and then we want to know if there's actual differences between different types of marketers, including general marketing managers and those people who

are working in the direct marketing industry.

The survey that I'm going to be presenting was the same for all three groups. The survey consisted of eight scenarios and the scenarios were constructed so they were balanced and they went through some extensive pretesting where we presented the benefits to the consumers, as well as some of the risks that might be involved in terms of the technologies that marketers use.

For all the eight scenarios, they were asked whether they wanted to have the opportunity to not allow the technology to be used on them at all or they preferred prior permission through an opt-in or they wanted an opt-out mechanism or if they felt that the technology was fine as was and permission was not needed.

The consumer data was collected through Harris Interactive and we had 2,007 respondents. Overall, given all the choices they had, 45.3 percent of these people did not want to allow technologies to be used. These are of all the choices they had. You had 34.5 percent opt-in, 13.1 opt-out, 6.9 allow. So, this means that 79.8 percent of the people wanted some type of control in terms of the technologies that were being used by marketers.

Now, when we drill down to the data and look at it by technology, it varies. Overall, the line in yellow

is there which you've seen before. The other technologies that we looked at are -- range from pop-ups all the way down to loyalty cards and they're sorted in the order of control that consumers want. So, consumers wanted the most control over pop-ups and they wanted the least control over loyalty cards.

These technologies were selected because four of them reflect technologies that are primarily used for information gathering and four of the technologies are used primarily for marketing communications. So, the pop-ups, text messaging, spam and telephone marketing are more message deliverers and are for information gathering, and realizing that there's connections between the two of those.

Looking at the data, we then decided to segment consumers and see if there were different groups because not all consumers respond the same way. Across all choices, we came up with four segments. The first group we labeled the permissives and that has an N of 168 individuals, and these people obviously were very much allowing the technologies, either an opt-out or an allow was the top categories.

The largest segment with 871 was called the restrictors. These people obviously wanted not to allow the technologies to be used. The pragmatists, another

big group, were more balanced and they wanted an opt-in mechanism with 47.7 percent.

The last group is interesting, it's not really reflected in the data that I'm presenting here, but they're called the environmental protectors. These are people who make the distinction between the different types of technologies. They were much more restrictive for technologies that would invade their private space or time through kind of a marketing communication, but they would allow technologies that would gather information.

There's information that we can profile these segments a little further, looking at age and percent male is one of the demographics we looked at. We have others as well. But you can see the permissives tend to be the youngest group. They are also the highest percent male. They also are the most affluent of the groups. The restrictors are more female, they tend to be older. They are the least educated and the least affluent of the groups. The pragmatists and the environmental are somewhere in between on those.

We also have, on the last three rows in the slide, looking at the percent of individuals in these segments that did not want to allow three of the technologies that are relevant to our discussion today, pop-ups, cookies and no spam.

And here you can see some very marked differences between the groups, where the permissives, you know, don't mind any type of communications that would be available like pop-ups or -- they're not trying to restrict those. You see the restrictors have -- 87.8 percent want to restrict those.

Now, the pragmatists are the group that prefers the opt-in mechanism and while they have -- about 42 percent of them don't want to have pop-ups used, 24 percent of them only want to restrict cookies. That means 75 percent will allow cookies in some form or shape. The environmental protectors, again, they are restrictive for pop-ups or spam which tend to be more of an evasive technology in terms of the time and space. They are more allowing of cookies as well.

Next we added some surveys that looked at marketers and direct marketers. Now, the marketers we contacted through buying a list of individuals who had the name "marketing managers." So, we used direct marketing to find these people. And none of the individuals had worked in the direct marketing industry. We ended up getting 162 responses of these individuals.

And then we have a sample of direct marketers, and these are individuals who worked in the direct marketing industry who are attending a trade show.

Again, we asked the same survey. The only restriction was that we made them answer the questions from the perspective of a marketer not as from a consumer.

The numbers here are the same things you saw on the graph, but again it's interesting to see that marketing managers, who are not necessarily in the space, really kind of get the message about opt-in being important. The direct marketers still are looking at more of an opt-out/allow type of mechanism for some of the technologies.

Consumers -- one thing that I didn't mention early on and I think is kind of important is that across all eight of the technologies, when it came to a choice between opt-in and opt-out, they wanted to have an opt-in mechanism more than they would have preferred an opt-out.

So, as a quick summary of what we have here, consumers want control both of their environment and their information. The new technologies tended to give them more concern than some of the older ones that had been around for a while.

Consumer groups exist with very specific preferences on how to control the various technologies. So, this means that there's opportunity for marketers that treat consumers differently and to try to understand their preferences and treat them that way.

And, finally, consumers have different expectations than both marketers and direct marketers. We knew that. But it's important to see where the conflicts might exist. They really exist over information gathering because while consumers want to control their information, it's vital for the marketers to get that access to it. They tend to be more aware of invasive time -- like telephone calls and spam and so forth. They're much more responsive in not invading the space.

Then, finally, marketers are not all the same and, so, there should be attention paid to the different ones that are out there. Thank you.

(Applause)

MS. KRESSES: Thank you, George.

I'd now like to introduce Dr. Larry Ponemon who is the Chairman and Founder of the Ponemon Institute.

DR. PONEMON: Thank you for saying my name correctly. I thought it was going to be Pokemon again. Last time I was here it was Larry Pokemon.

(Laughter)

DR. PONEMON: So, I have about, I don't know, five hours of material to share with you and I'm between you and lunch and I feel your stomachs starting to rumble. I could hear it. So, we're going to be fast.

We're going to go through this material quickly.

Really my talk is on two separate themes that I'm going to try to integrate, cookies and consumer permissions, and obviously, they are related. But before we do that, I want to talk a little bit about some of the research that we've done. This is a meta analysis of a lot of studies, and if you're interested in seeing the original research, we're very lonely in Michigan, especially northern Michigan where we live. So, please call us. The phone doesn't ring enough.

Basically, what we find is that the world can be divided or the U.S. consumer universe can be divided into three buckets from a privacy perspective. I know I'm oversimplifying, but in our research about 8 percent of Americans appear to really care deeply about privacy to the point where it changes their behavior. About 70, 72 percent are people who, like us, who probably say privacy's important, but we're not willing to forego any inconvenience. So, it doesn't actually show in behavior studies any meaningful difference from this other group called privacy-complacent people, like my children who are in college and graduate school, who basically -- I know I'm probably going to criticize someone here, but like Facebook, they post all these pictures and stuff. It's amazing, especially when their dad is in the privacy

industry. They kind of go against me. It's terrible. Rebellious kids, just like the way I was as a hippie as a younger man.

(Laughter)

MR. PONEMON: Now, that I revealed something about myself, but you also need to look at not the privacy issue, look at the privacy issue beyond the U.S. and around the world because our friends -- for example, our friend from Germany who asked the question before, we basically have this belief people in different parts of the world really care deeply about privacy and they're going to be out there changing their behavior, and there's no strong evidence of that, although EMEA and Latin Americans tend to be more privacy centric than people in the U.S. and Asia. And still that middle category of privacy sensitive and not willing to forego an inconvenience is kind of the strongest category.

So, in a nutshell, then why should you or marketers be -- why is privacy important to us or specifically to online marketers? Why is it important? Well, I'm going to talk a little bit about some research that shows this, at least we attempt to show it in survey research, and really this is a call for research. For those people that are in the research industry, I think we've exhausted the field of survey research. I think we

need to start moving into behavioral research since what people say in a survey may not be entirely true. We know that, so we want to be able to go from that point to the point where we're actually looking at behavior.

We're starting to do that, other companies are starting to do that, it's really important.

With respect to survey research, research shows that consumers are distrustful of marketers who use aggressive online marketing tactics. Well, duh, of course.

The term "cookie" continues to have negative connotation among consumers. Many consumers still see cookie as -- well, it used to be a good thing, chocolate chip cookies, but now it's like cookie, oh, it's an awful word. Mallomars, that's what we have to use here. Oh, yummy.

(Laughter)

MR. PONEMON: Consumers want to have more control over the privacy of information they share with online marketers. Consumers actually -- this was kind of an interesting finding. Consumers actually prefer personalization when it is relevant and it actually provides interesting content. We'll talk a little bit about that. It may be an anomaly, but we think it's actually more persistent. It's more than an anomaly. It

seems to show up in other studies.

And consumer trust in online marketing practices actually does result in better data being collected about the individual. So, if you actually look at the proposition, when we target people, we actually get better information, it seems to be true.

Now, in one study, this is a 2006 online marketing study. This was independently conducted by Ponemon Institute. It was not outsourced, it was done by us. It's about 1,700 Internet users, consumers who self-report being 18 years of age or older. What we've learned from this is, again, that consumers have a very negative perception about the term "cookie." In fact, just the mere mention of cookie in a privacy policy causes people not to get involved. In other words, if you're looking for opt-in, they see the word "cookie" and they are less likely to opt in. It's so -- just the word, changing the word, coming up with some other word, doughnut, I don't know, some other word, would actually change someone's perception about whether they should participate. So, the word "cookie" has this negative connotation, especially when it's in a policy.

Respondents who said they have a very good understanding about Internet cookies, in comparison to the total sample, are likely to be more responsive to ads

and they're also more responsive to personalization. So, again, knowledge doesn't actually lead to negative behavior from a marketing perspective, but actually leads to greater participation.

Also, knowledgeable respondents appear to be much less concerned about the use of cookies, even persistent cookies. On average, only 48 percent of knowledgeable respondents appear to be concerned about marketers using cookies as opposed to 60 percent for the total sample. So, when you think about it, fear, you know, the flood factor causes a lot of people not to participate, but what we're finding generally is when people have more knowledge, still there's a large percentage of people who won't, but you seem to get higher participation.

Let me tell you about some other interesting findings, and I'm respectful of time here, so I have to move pretty fast. What we find is that about 55 percent of respondents believe that an online ad that targets their individual preference or interest improves or greatly improves their experience. We thought this was kind of a weird finding because while people hate cookies and permissions, people actually like the idea of having someone spend the time trying to understand what they're interested in.

So, there's this weird thing about personalization, especially when it's content that's being delivered versus an ad. People actually like it, which is interesting.

And here's another finding, another duh finding, and yet, even though people like it, no one's willing to pay for it. So, the idea -- this is the other thing about the Internet, this absolute confusion about Internet economics. So, for example, there was a large number of people who went crazy when they heard that -- I think it was Google did not save search terms forever, 18 months or whatever. If you're rational, of course, but if you're irrational, you don't expect it, it actually creates issues. So, in our mind, what we basically find is another problem in knowledgeable is actually getting people to understand Internet economics and how this whole thing works.

Another finding that we thought was actually -- it still may be an anomaly, one I'm going to tell you with full disclosure, this could be one of those survey anomalies. We think we're dealing with a comparison between 2004 and 2006 and you would think that over time people would be smarter about technology, like to delete cookies, right? But we find, in general, that people are less likely, there's a downward trend to cookie deletion,

and it's pretty significant. Again, it could be a sampling anomaly. There are two very large studies. The question was identical. But we find that the frequency, very frequent and frequent and sometimes that category is actually decreasing. It's still a very significant number. So, I think our results are consistent with like a Jupiter research study, but for the most part, we don't understand why this is the case.

There's two possibilities. One, consumers are just more complacent, you know. They worry less about it. You know, the biggest story in privacy, it's no longer that story, and it may be harder for people to remove cookies. Maybe they thought before they were removing cookies, but in reality, they weren't removing cookies or all the cookies that they were trying to remove.

I think I'm going to talk even faster than I've been talking. We conducted this permission study and this is a 2005 study and we've learned a whole bunch of interesting issues. But I think the most important finding is about the relationship between permission and trust. So, what we've learned is that companies seem to be getting better at targeting messages to the most appropriate audiences, so some of this behavioral targeting actually seems to be working better.

Consumers are willing to share more and better personal information about themselves when they have a trusted relationship with a marketer. Consumers want to rule over their online experience and 84 percent want to have more control over the types and frequency of Internet ads that they receive.

It also seems that there's this commitment when a consumer trusts an online, like a company and, therefore, it's marketed, it seems to be a longer term relationship. People are less likely to churn or shift or delete cookies. If you treat the customer, the consumer with respect, they seem to be more likely to share and opt-in.

And consumers do not want to be tracked online. Despite all of the positives, because I almost sound like a slogan for Internet marketing, and I don't want to be, but the reality is only 20 percent still are very concerned or would actually think that this idea of tracking their behavior online is acceptable. They don't like the idea of this tracking that's happening behind the scenes. That could be a lack of knowledge and experience because how do you do that if you're talking and if you lack relevancy? So, it could be a knowledge gap, a big one.

The trust factors that we looked at in this

study -- and by the way, we know that some of these have actually shifted. For example, when we first started to look at this issue, web seals like TRUSTe and BBB Online and others weren't really a factor of consequence. Suddenly, they are, and people are looking for TRUSTe, they're looking for a seal that actually defines a certain level of quality. So, we see that shifting.

But what were the top three factors? One, you have confidence that the merchant will safeguard your personal information. The number one trust factor in the study was the privacy commitment of the merchant.

The frequency of the Internet ad, there's like a line in the mind of the consumer when an advertisement becomes annoying and irrelevant and there's a frequency.

The merchant doesn't share your personal information with third parties was important as well.

Then asking for permission, opt-in versus opt-out, these are important, and even the idea of personalizing messages, saying to you, Dear Larry, I know you're a pilot, so we're interested in blah, blah, blah. That stuff may be important, but it's marginal relative to the first three factors.

So, in essence, what did we learn from all of these studies? Well, we find that people want to have more control over the types and frequency of Internet ads

that they receive, and if they had more control, they would have a higher level of trust. So, it's a ying-yang relationship, maybe tail wagging dog relationship. But the idea is to get to trust, you have to actually think about ways of giving the consumer more control.

Again, another finding in summary right before lunch, we asked the question, Do you believe that an online merchant respects you when it does the following? What are the following things that you can learn from this research? Number one, expends the time to try to understand your interests and, therefore, is better able to market to you. So, the number one factor in terms of getting your respect in the study -- now, we didn't have an exhaustive list of questions, but we basically found that this idea of spending the time trying to know the audience and proving it with good content, not necessarily pop-up ads or ads, but good content, was a way of showing respect.

So, in conclusion, we find that consumers are still generally distrustful of online marketers and are taking steps, we believe, even though the frequency is down, to control cookies on their PCs.

In essence, consumers want to have more control over their online experience and ultimately their privacy.

Consumers do prefer Internet ads that are targeted to their specific tastes and preference, are respectful of their privacy preferences, and permission is important here, and are not overwhelming in their mind on frequency. The problem that we try to get at frequency, and we don't have an answer, is it's all different for each of us. To some it's two. For some, frequency is one. To others, it's positive infinity. So, we don't know what the ideal is.

Permission is important to establishing trust and trust leads ultimately to more and better data being collected about the consumer. So, again, it's beneficial for online marketers to do that.

With that being said, I want to thank you and the FTC for giving me this opportunity to present. Thank you.

(Applause)

MS. BRANDENBURG: Thank you, Dr. Ponemon.

So, we've had a very interesting and full morning, and it is now time for a lunch break. We will begin again promptly at 1:45, and if I could just remind you, when you do return, you'll need to go through security, so if you can factor in time for that it would be helpful. Thank you.

(A lunch recess was taken.)

AFTERNOON SESSION

(1:49 p.m.)

SESSION 4: DATA COLLECTION, USE AND PROTECTION

MS. KRESSES: Good afternoon. In Session 4, we're going to hear from seven people and then we'll move into Session 5 directly and have a roundtable discussion of what we've heard, as well as further points that will be raised.

So, we have with us today Nicole Wong from Google; Diane McDade from Microsoft; Scott Nelson from TruEffect; Chris Kelly from Facebook; Amina Fuzlullah from U.S. PIRG; and Lisa Campbell from the Office of the Privacy Commissioner in Canada. We are, unfortunately, missing Professor Ian Ayres whose flight was canceled without warning.

With that, we'll start with Nicole.

MS. WONG: Thank you for the invitation to participate today. My name is Nicole Wong. I'm the Deputy General Counsel for Google and one of my responsibilities is privacy at our company. I'm going to cover today our approach to privacy generally as well as the types of data we collect for purposes of serving relevant advertising to our users.

At Google, we spend a lot of time studying our own business because the entire industry is changing so

rapidly. In the online advertising world, we found two things to be true. First, advertising is a critical component of the web ecosystem. When we do our job well, we connect consumers with information they want at the time they want it. Online advertisers and publishers, including small businesses and bloggers, are flourishing because of the ability to reach their consumers in an effective and efficient way. And billions of dollars of services and information are provided today for free, or nearly free, because of online advertising.

The second thing we found to be true is that our users' trust and their privacy are critical to our business. Because we support open platforms, as Tim Armstrong was describing to you this morning, our users are free to pick up and leave, and because of that, we have to work every day on every product to earn their trust and their business.

In advertising, we've created a very robust ad platform without having to use much information about a user at all in order to effectively target the ads, and I'll describe those systems in more detail.

Our business depends on getting this balance right and we're committed to continuing to provide the benefits of online advertising in a way that protects user privacy.

Let me spend just one minute talking about our team. I am enormously fortunate to work at a company where privacy isn't just the lawyers' problem. Instead, it's a value that's affirmed throughout the company from our engineers through our executives. For that reason, our approach to privacy is not to solve a privacy problem by having a well-worded privacy policy, although I'll tell you that we spend a lot of time on those policies and on things like our recently released videos about what a log file is or what a cookie is, and I hope you will check out our new Google privacy channel on YouTube. But in addition to that, we work really hard at designing privacy protections into the product itself.

The team that drives the process looks like this, with a lot of experienced leadership at the top and, importantly, attorneys who are embedded with the products to make sure that the products are designed with privacy in mind. We also have, of course, support teams and security teams who are experts at what they do.

So, let me turn to our advertising offerings. There are basically two. We try to connect with consumers when they search, known as our AdWords product, and consumers when they visit websites where we also display ads or in our AdSense product. This is a simplification, but it's necessary given the time

constraints. Both of these offerings are contextual advertising, so they give results based mostly on the current context of the user, not on a user's past behavior or a profile.

So, first, to look at AdWords. We're connecting consumers when they search, and a Google AdWords advertiser will purchase text ads, which you can see up here, the mutual funds ad, that are provided in response to a search query that's entered into our search engine. So, the advertiser will design that text ad, choose a keyword that triggers the ad, in this case it's mutual funds. The advertiser picks a language and a geography it wants to target, and then the advertiser decides how much it wants to pay when a user clicks on that ad.

With this inventory of ads, Google will then match the ad to the chosen keyword. We check for the language preference of the user, we check for the IP address in order to get the geo location, and then we algorithmically rank the ads for relevancy to the users based on a quality score that has to do with whether the landing page is of quality, whether there's a lot of click through rate on that ad. And then, finally, we run the auction. The advertiser then pays when a user clicks on their ad.

Importantly, we are targeting here based on the user's search term, not on a profile. So, in our experience, ads are more useful and thus more effective when we can correctly identify what the user's looking for in that moment. This is in contrast to behavioral targeting that's based on a profile built on past activity in order to target an ad.

Our AdSense service works very much the same, except in using keywords to target, we use the content of the page. So, this is a page by SeatGuru, which is used to tell you what the best seats on the airplane are and we take terms based on that in order to target the ads, much in the way the keyword's used. Again, importantly here, we're matching on very limited information.

To be really specific about what we collect, when a user comes to our site, they never have to register to use Google. You can go up to any Internet kiosk, any computer and type in a search without registering with us, and at that time, the only thing we collect is standard log information, URL, IP address, basic information about your computer and a cookie ID.

The same is true when you view an ad on one of our AdSense network partners, IP address, URL, time and date, and the ad viewed.

By the way, descriptions of the type of stuff

that's in a log file is actually in our privacy policy and also in a recently released video that describes what it is.

So, let me finally end with how we protect user privacy. As I was saying, we deliver timely, relevant ads with very little user information. We use contextual targeting. We were also the first major search engine to announce a finite logs policy of 18 months, after which we anonymize the IP addresses and cookies and our cookies expire after two years.

We limit the disclosure of data. We don't transfer PII to advertisers. We have a team that's dedicated to reviewing all requests for user information from the government or any other third party, and we have strong expert teams for network security, software engineering, physical security to protect all of these systems.

Leaving you with a final word, this is a very important discussion for us to be having across the industry. This is a very complex business with many stakeholders. And the third thing we found to be true is that the online advertising industry is evolving. So, it's appropriate for us to be reviewing our practices in light of those changes with an eye to continued health of the web ecosystem and to the trust and privacy of our

users. Thank you very much.

(Applause)

MS. KRESSES: Thank you.

And, now, we'll hear from Diane McDade, Microsoft Trustworthy Computing.

MS. McDADE: Thank you very much and to the Commission and the staff, thanks very much. It's been a privilege to attend today and to learn from the other panelists and presenters and I'm looking forward to both sessions.

Microsoft has grappled with the hard problem of privacy and protection on the online space for many, many years. We started our services in the mid-nineties. I came onboard in '98, and we named our first chief privacy officer in the year 2000.

What we've learned in those years is that what you have to look at when you look at privacy is you have to first think seriously about the technology and how to embed privacy protections by design from the get-go in the architecture.

The second thing you need to do is make sure that you have very solid policies that are understood by every member of the design team, all the employees across the company, and we engage in very rigorous training in our employee workforce around those policies. We've

articulated our policies publicly and they're very well articulated internally.

The third thing that we need to do is to make sure that our practices follow and that there's an internal compliance and implementation program that's followed up by audits, third party and internal, and that we open ourselves up to scrutiny by outside organizations, voluntary seal organizations and the like. Microsoft has done all of these things for a number of years and we've learned a lot through that process.

One of the things that we've had to be challenged by from the beginning is to have a global adherence to the privacy laws around the world as our products are worldwide. So, in doing that, we've learned that our leadership really depends upon our understanding of the larger environment and the expectation of consumers worldwide. We feel, as a leader in the industry, we have a special duty to go the extra mile and really make this easier for customers to take the burden off of them and to put more of the burden on us, as a company, to do the right thing.

I'm going to move probably pretty fast through these slides. I'm going to quickly summarize the information in our online space. Microsoft, in accordance with our privacy statement, does collect both

personal and non-personal information, and when we collect personal information, we only do so after the customer has actively accepted our privacy statement and they've had an opportunity to peruse and examine that.

We do, in turn, with that information, provide our customers with, oftentimes, personalized or customized services. Normally, they are free of charge. So, we're using the information for that primary use.

In addition, we may go ahead and build segments, profiles that target customers with appropriate personalization in advertising and use that information in a secondary manner.

Now, we, about five or six years ago, wanted to think forward about behavioral targeting and recognized that if we were going to do that, we wanted to make sure that any segments that we built that contain what is sometimes Internet data about surfing and searching, that people feel might be sensitive, was segregated from account information entirely so that one wouldn't feel that Microsoft was linking the personal account known PII data, data that can personally and directly identify you, with a profile that might be fleeting as your interest changes from cars to baby gifts to, you know, a trip to Hawaii.

So, we've architected our system from the

ground up to make sure that we separate those two things. And, of course, we also have had a lot of experience in making sure that we're thinking about security from the beginning. I'm going to go into that a little bit later.

One of the things I'm most proud of to work at Microsoft has been the evolvement of our disclosures and notice. We started out like everybody else, with a really long privacy statement. I think it was 14 pages. And in the last few years, we've done customer research and we've understood that customers are really looking for something better, and we adopted a layered notice a couple of years ago after we researched customers worldwide and they told us that they like the idea of a short layer that gives the basic information that they can click down then into a lower layer and really follow up on their interest in the particular areas.

A number of other companies have adopted the layer notice and we'd encourage everyone to take a look at that as it provides a very easy-to-understand format for privacy disclosures.

Another item, and I've got some props, is our public release of our privacy guidelines for software development. It covers web server and client applications so that we're able to be public about the privacy and security safeguards we build into our

products and we welcome other industry players to work with us in moving forward these standards across the entire industry.

In July of this year, we released our principles for this area for Online Search and Advertising and those are available out front. These principles articulated a lot of the practices that we engaged in over the last few years, but they put it all together into one document. I encourage you to take a look at that.

Finally, today, we released a De-identification White Paper that really goes into details about how we segment and separate those two data streams that I referred to a moment ago.

What are our online privacy principles that we outlined in July? Basically, I'm just going to cover the highlights and the progress that we've made on them since we announced our commitment to these in July.

One, we felt that we could do a better job with more detailed privacy notice disclosures as it relates to behavioral advertising, and we've released that and that's live on our new privacy statement this week.

We've also made some engineering investments, and as we move forward as becoming a full NAI member with the addition of aQuantive, we're going to be offering an

opt-out is roamable if you were signed in as an identified individual through our Window Live services, and what that will do is allow someone to maintain their opted-out status whether they're at a different computer at home or at work as long as they're signed in.

We've also gone ahead and made the decision to offer that opt-out capability across Microsoft sites and services, as well as any third party ad serving that we move forward.

Finally, we've taken very seriously working worldwide with regulators and industry about how we can identify best practices together in a collaborative approach because we believe these questions really can be resolved and moved forward with a lot of sharing of information. We think facts are friendly and we like talking to other companies and regulators to understand better their concerns and their practices.

Finally, we've taken security as our partner. I like to say, as a privacy person, that security's the handmaiden of privacy. We really can't have privacy without strong security practices. And, so, one of the things that we've been doing is thinking about -- I'm sorry, I'm on the wrong slide, excuse me. This slide is about how we're going to move forward with aQuantive. What we're interested in here is to make sure that we

move forward to work with NAI and the industry on our third party ad serving, that we innovate with NAI and with other industry partners as we all look for better ways to give consumers that feeling of control and choice that they deserve and ought to have.

My last slide is on security and what I wanted to let you know is we're always looking for better ways to secure the data that our customers entrust to us and, so, we're moving forward with scrubbing all search terms, all search queries from credit card data and Social Security numbers, to remove these items right from the get-go out of search storage. We also have a very elaborate program that's been in place for a number of years that's risk-based so it moves -- our security program is always evolving as we recognize new threats.

So, we take the security very, very seriously whether it's the data that's held pseudo anonymously or anonymously or the data that's personal to make sure that it's not in harm's way from either internal or external intruders. This program is very formalized and mature and it's been audited by external organizations and we do apply a comprehensive policy across our entire suite of services. I can go into more detail about this probably later if we want to get to it.

Thank you.

(Applause)

MS. KRESSES: Thank you very much, Diane.

And, now, we'll go to Scott Nelson from TruEffect.

MR. NELSON: Thank you. Before I get started, I'd like to just throw down to Richard Smith because he had to raise the Red Sox this morning, and I'm probably the only panelist here from Colorado. So, I want to let Richard know that I had set aside time for game seven tonight, which is available, and I could sure use a steak and a shot of whiskey to solve this headache or this brick wall we ran into called the Red Sox. So, I do have time this evening.

Thanks to the Commission and the staff of the Federal Trade Commission for inviting me to participate today. Frankly, about half my presentation has already been given three times today. So, I'm going to jump through some slides quickly and get to the meat of the discussion. What I'd like to is credentialize TruEffect a little bit -- who are we?

MatchLogic is a predecessor company that was actually one of the seminal ad serving companies back in the mid-nineties that founded this space, basically with DoubleClick. We are, I guess, a restart of that company. TruEffect is from the people in IP that was born out of

MatchLogic. So, we've been in the space for ten years. We've worked with large advertisers, primarily on the buy side with ad serving.

Today what I'm going to talk about is a little bit of a shift in the paradigm of the data model. We believe at TruEffect that it's time for a change to this data model and we want to remove the ad server from the data equation in online advertising. We want to place the advertiser and the consumer into a direct relationship and eliminate or even potentially eliminate the collection of cookie data altogether.

Before I dive into this, let me just quickly show you guys, if you don't know, in ten seconds how to read your cookies, look and see what's going on. I'm using Firefox here. Go to Tools, Options, Privacy and Show Cookies, and you can actually go in and see the data that's being collected on any given website. If you go in and refresh your browser, you can see any new information dynamically that's being inserted there. So, that's a little gift from me to you guys.

Now, one quick point here is not anyone can read any cookie, okay? You can't just read and write cookies in consumer's browsers. Browsers abide by protocols and all of us live by those protocols. Servers delivering content to a browser, including ads, are

limited to a specific domain. I've got it up here as the fully qualified host domain represented by URL. Only servers registered within that domain in the DNS system, the domain name system, can read or write cookies into the browser. Traditional third party ad servers leverage cookie technology by using a proprietary domain, so a domain that they own, and it writes cookie test files only their servers can read or write. The advertiser for whom the campaign is being conducted is walled off from reading that information.

Now, furthermore, the consumer views ads, let's say, from Amazon and clicks on one and is redirected to the Amazon website where they proceed to purchase a toy for their child. Now, you've already seen several times today and I represented a series of transactions that would be recorded by the ad server in the process of delivering banners and tracking the clicks and the landings. The consumer has no idea, they've never heard of adserver.com. They've seen an ad from Amazon, they are in the process of navigating our website and making a purchase, perhaps, and that's the trusted merchant with whom they think they have a relationship.

Now, the conundrum of the third party model was really addressed in 1999 with the formation of the NAI and the adoption of the NAI principles. But that's --

that's a big step in the right direction, but it's eight years ago which is actually about two lifetimes in our space.

I'm going to jump through this quickly. Ad servers gather almost all the same data you've seen before. We're talking IP address, browser type, time and date stamp, cookie name, cookie data, so on and so forth.

But what does adserver.com do with the data? Well, one of the things we do is we provide reports. The records are aggregated into reports, the counts, if you will, depicting the performance of the media and the message. The census-based performance reporting made possible by this process has been one of the key drivers in the success of Internet advertising.

An advertiser can see in hours how an offer or a piece of media on a website is performing and make immediate optimization decisions. Now, this alone has put Internet advertising into the marketing hall of fame, but adserver.com doesn't stop there. The raw logs can be segmented, scored, analyzed and modeled and from this a cookie ID can be fingerprinted and those attributes used for targeting, as we've talked about all day.

I'm going to jump through the example because you've already heard all about these examples.

Consumers have voted with their wallet and

created an industry of anti-adware companies, the software makes it easy for the consumers to block or delete cookies and, therefore, they've severely jeopardized the model I just illustrated for adserver.com. When a consumer deletes cookies, the value of that profile in the database is wiped out and the investment to build a profile is lost.

That fact, paired with the disharmony of inserting an unknown third party between the consumer and the known and trusted merchant has prompted TruEffect to introduce a new model, one based on extending ad delivery for an advertiser to that advertiser's domain effectively removing the third party from third party ad serving.

The reality is enterprise level ad serving is complicated, it's expensive, and it's a headache if you don't have extensive experience doing it. Nobody wants to do it, including some of the largest corporations in the world. They've been shackled, large advertisers, with fur-lined handcuffs to the existing third party data model and precluded from developing a direct relationship with consumers when online.

Now, posit this, when you quench the desire to develop an anonymous cookie profiling database, the door opens to a wealth of possibilities in managing the data derived from the serving of ads. We've named this

capability directserve, and directserve is a patent-pending technology that allows an advertiser to deliver their online ad campaigns entirely from their proprietary domain without sacrificing the effectiveness of an enterprise caliber ad serving platform.

With directserve, we can deliver campaigns anywhere on the web from the advertiser's domain using only the advertiser's cookie and creating a database of log records only meaningful to the advertiser. The data is not aggregated and re-purposed for other clients. Now, know, the companies represented here are for illustration and they're not TruEffect clients.

Now, a profiling database is only possible within the confines of the advertiser. Now, TruEffect, as an agent, does not benefit from the data by creating derivative works. I equate this or it's analogous to the U.S. Postal Service delivering the mail anywhere in the United States despite rain, sleet or snow. In other words, it's difficult. But we have no rule on the information shared between the sender and the recipient.

So, what about the consumer and what impact does the technology have on behavioral targeting, which is what we're here to talk about today? First, it creates an opportunity for the known and trusted merchant to extend the functionality and logical relationship with

the consumer that mirrors their website. Wherever they buy a piece of media, anywhere on the web, the consumer is presented with an advertisement that is a function of their relationship with a merchant and the behaviors they've shared.

For the first time, consumers can rest assured that the privacy principles ascribed to by the merchant will not only be employed when visiting the website, but they retain full force wherever the merchants purchase media inventory anywhere on the web.

Quickly, one extension of directserve that we launched this month, or in October, is called safeserve, and it's the only solution that blends the traditional benefits of ad serving with the more rigorous standard of no unique tracking, anonymous or otherwise. Advertisers targeting young web servers or those persons researching sensitive subjects, like medical conditions, do not have to abandon the benefits of consolidated trafficking, optimization and reporting.

So, what about tomorrow? We've been asked to comment on what's happening. I spent several minutes talking about cookies and browsers, but the Internet is no longer defined by servers and browsers exchanging information across copper and fiber. Going forward, data about the consumer behavior will not be mediated by the

cookie facility embedded in browsers. With the explosive growth of digitally addressable media, our company is being pushed to extend census-based measurement and dynamic targeting technology from the browser to other channels. We're redefining what it is to be an ad server.

We, in the industry, have to work closely with the carriers, the networks and the infrastructure providers to guide them in the consumer-centric use of this technology over time.

Thank you.

(Applause)

MS. KRESSES: Thank you, Scott.

Now we'll hear from Chris Kelly of Facebook.

MR. KELLY: Thank you very much, members of the Federal Trade Commission and staff and everybody else who's come out today. I'm Chris Kelly. I'm the Chief Privacy Officer of Facebook, a technology company based in Palo Alto.

I'm going to go through a number of the particulars of how we handle collection use and security of data on Facebook, but I want to start with a couple of principles. You know, one that we followed from the beginning and that we think is very important for every step going forward, which is to have privacy by design

and built into the architecture to empower consumers to make their own choices about data, how they share it, what they do with it and how they share it with their friends.

And, secondly, I want to reach way back to the Network Advertising Initiative principles and we've had a lot of discussion today about the NAI and where things go, but one of the things that the NAI did very well early on was to establish a pretty clear separation between non-personally identifiable information as it is collected and when it could ever be associated with personally identifiable information and put a clear firewall up between them where you had a conspicuous notice and choice. We think it's very important where anyone seeks to or thinks about associating non-personally identifiable information with personally identifiable information, that that principle of clear and conspicuous notice be followed going forward.

Facebook has tried -- obviously, we've based our business on primarily personally identifiable information. We've been very upfront about users and how we collect and use that information, and that's what I want to go through now.

So, let's talk a few facts about Facebook. Facebook, there's a lot of talk about, you know, are you

a media company, are you a technology company? We're a technology company. We build great technology that enables people to share information with their confirmed friends. You know, a fun fact you hear often about kind of online social networking sites and sharing information willy-nilly, it's available to everyone on the web. The average user on Facebook has access to less than .15 percent of the profiles on Facebook. So, privacy has been built into our design from the beginning.

We like to think of ourselves as a social utility to share information with your confirmed friends. We have a bit more than 300 employees in offices in Palo Alto, New York, Chicago, Detroit and now London.

So, collection of data is obviously a key part of this, and I have tried to illustrate this with the key profile page which every user, they validate into the system, they confirm that they have access to the email address that they've signed up from, and then they can enter these pieces of information in their profile.

So, this gives a real-time user control over the collection of information, what's collected and what's not collected. The privacy settings, which I'll show you in just a minute, enable you to say exactly who sees it and who doesn't, but it's also very important to stress there actually is no setting on Facebook to reveal

my profile information to the world.

The goal here is user empowerment and empowerment is sharing information within your real world social context. So, you can share as much or as little as you choose and only with whom you choose.

So, the use of data -- and the principles you probably can't read very well, the principles that we set out here. But while we go into the details about how data sharing works and what we empower users to share, and how we do it, we wanted to set forth two very clear principles. One is that you should always have control over your personal information and you should always be able to choose who you share with and how, but you should also have access to the information that others want to share. If they want to share it with you, you should be able to get it.

Now, that requires a lot of architecture and a lot of thought about privacy and the way that it works. So, the purpose of our site is sharing information primarily with your confirmed friends in the real world. The user controls who sees that profile and receives that information.

Now, we've built a system called News Feed that enables that information to be aggregated but, you know, in another we had obviously a pretty big privacy dust-up

over News Feed when we launched it. But once people understood -- and News Feed is probably now the most popular feature of the site. Once people understood that it was only their friends' information and -- they were only sharing their information with their friends and their friends were only sharing information with them, people got very used to the idea of aggregating all of this information and presenting it in a useful and meaningful fashion. And, of course, advertising is, in fact, targeted based on that information that you provide which we've had a very clear statement in the privacy policy about for two years.

What it says is essentially if a movie company -- we give an example. If a movie company wants to promote the fact that a given movie that they have coming out is going to be playing in your town and you have a movie in your profile that may match what they think the movie that's coming out would be a good one for you to see, you might see an ad for that, but we don't tell the movie company who you are. We don't think you'd want to share that with them. If you want to in some other way, if you want to sign up for an email list or things like that, that's fine with us. But we're not going to do it on your behalf. We just don't think that that meets with the control principles that we're articulating.

And I also wanted to go through our basic security principles and, obviously, we've had this registration system all around. There's not wide availability of profiles in general. We do confirm it based on friendship and on network rules. So, we do have these broader environments that you can choose to join, but yet again, on average, you still only get to this .15 percent of profiles being available to a Facebook user where we're collecting sensitive data, where, for instance, if you want to send a virtual gift to your friends, which is something that we've enabled for about a year now, we collect your credit card, that information is encrypted. When you sign in, you get an SSL encryption layer that handles that data. So, any place where anything sensitive that might be easily misused in a detrimental way is encrypted at that point.

We also have a deployment of what we like to call anomaly-based systems on the network where people are undertaking activities where they're messaging too many people who aren't their friends, not just sending friend requests but sending a whole bunch of messages, usually spam, attempts at spam. We actually capture that very quickly and that helps contribute to the sense that Facebook users have that is a relatively spam-free environment. That's obviously a very, very important

part of being able to control your own experience on a network.

So, overall, this principle of privacy by design has animated Facebook both in its basic operation of the service and in the serving and targeting of advertising.

So, with that, I'll wrap it up and we'll have it open for discussion further.

(Applause)

MS. KRESSES: Thank you, Chris.

And, now, we'll hear from Amina Fuzlullah from U.S. PIRG.

MS. FUZLULLAH: Do you need me to move over because I am actually not from a technology company, so I'm not here with a fancy PowerPoint to show you all. So, if you guys can all see me from here, you're going to have to listen and try the old-fashioned way of just looking at my face and not something fancy on the screen. Is that all right? Thank you.

I'm going to start with a little bit of a story. I think the online advertising marketplace has changed consumers' experiences online in a significant way. I think the best way to describe that is to talk about something we're all familiar with in the brick-and-mortar world and that's the used car lot.

So, if we go on to the used car lot, we're going to know that the guy on the other side that's trying to sell you a car is trying to sell you maybe a lemon, maybe a good deal, you don't know. But you're not going to tell them every single thing about you. You're not going to want them to know how much you have to spend, you don't want them to know how many other places you've gone to, and you definitely don't want them to know what you think of the car sitting right behind that guy. So, that's much what the online world is now becoming.

As users are being tracked and followed and data is being profiled in PII form, non-PII form, all this information can affect consumer experience. So, today, I am here to talk about the consumer experience and how things are changing online for them as a result of all the data that's being tracked.

The folks here today are talking about all the various ways that they're trying to make sure that they can protect consumers, and despite those moves, I think there's still some serious problems out there for consumers as they go online, and I'd like to start with the issue of choices and price.

When you're being followed online and you're trying to make a transaction, you're going to be giving

up information, dropping cookies or giving up bytes of information maybe after you've scanned through a privacy policy that you clicked and just moved on just so you can access the content online and be able to see all your choices and see the prices and maybe even purchase something.

Well, you know, to do that, you've already changed your experience. You've given up lots of information. Now, remember, in the used car lot, you wouldn't have done that. You would be waiting to see what that guy would tell you before you would give up any kind of information and you're not allowed to do that in the online world. In fact, if you are given those opt-outs, it's really difficult to know how your experience is going to change when you do opt out. Are you going to be banned from using the site in a functional way? Are you going to now experience a lack of choices? And, for the most part, it takes a really savvy consumer to be able to actually navigate those opt-out systems. So, it makes it somewhat difficult if there's like a hodgepodge world of opt-outs or privacy policies. So, for the most part, consumers are going to give up their data and move forward, and that affects their -- like I said, their choices and their prices.

The next piece that I'd like to talk about a

little bit is privacy. I think one thing that everyone's noted is the difference between PII and personally identifiable information, non-personally identifiable information.

What's important to note is that it doesn't take PII to find someone. It's pretty easy for all of us to gather a lot of non-PII data and then start to put together a picture of a person, a picture of what they're doing, what their habits are, and that's why it's so valuable to sellers and that's why it's so valuable to the online advertising market and that's why it's so valuable to the folks up here.

So, I mean, I think that it's important that we start with that understanding, that all information that's being tracked actually is valuable to both the consumer and to the folks on the other side. So, there should be strict policies in place that give the consumer an idea of what's happening with your information. How is it going to be used and how is it going to change their experience and how long is going to be kept and who else is going to see this? It's good to hear that there are changes taking place.

But what would be really helpful is that if there wasn't a hodgepodge world out there. If there was actually a uniform system so that folks could actually go

on to one website and go on to the next website and have the same experience, that you wouldn't have to worry, oh, okay, well, now I'm looking at Website B, so am I being tracked? Oh, no, now I'm looking at Website C. I think I'm safe now. It's a lot to keep track of and I think it's difficult for consumers to understand that.

There's one last thing that I did want to talk about and that's the lack of transparency and consumer control. I briefly mentioned it in my example, but I think I'd like to highlight it mostly because in the brick-and-mortar world, when you're asked for information, you can say no.

So, this just happened to me the other day. I was in a store and they asked me for my telephone number. Basically, they're trying to figure out what kind of consumer I'm going to be. Am I going to return that shirt a week later? Am I only a sales shopper? What am I going to do? And we're all familiar with the marketing gurus' descriptions of what are the ideal consumers and which ones are the devils or which ones are the ones that you really want to keep. I refused to give them this data. Well, I didn't get refused service after that. The woman looked at me and kind of looked startled and then she said, well, okay, are you sure? I said, yes. Then we had a nice conversation. I got my pair of jeans

and then I moved on.

I can't do that online because there isn't that transparency. People don't know what's going on with their information, and if they do and if they're smart enough to catch it, it's really difficult for them to, you know, as I said before, know how to get out of the situation and, if anything, what will change.

The online environment has a lot of positives for consumers as well. As online advertisers have told you today, they can direct you to products that, you know, you enjoy and they can show you more targeted ads that won't get you a sweater ad in the middle of the summer. But that kind of utility often drops off with the amount of consumer data that's actually being taken up.

So, it's important that as we go forward, we understand that we place a fine line in between how much consumer data we're actually taking and what we're actually offering consumers in return. Thanks.

MS. KRESSES: Thank you very much, Amina.

(Applause)

MS. KRESSES: Now we'll hear from Lisa Campbell, Office of the Privacy Commissioner in Canada.

MS. CAMPBELL: Good afternoon, everybody. My name is Lisa Campbell. I'm Senior Counsel with the

Office of the Privacy Commissioner in Canada. I want to thank the FTC for inviting me to be here today.

Our office is an agent of Parliament, which means that we are non-partisan and we report to the whole House of Commons and Senate. We oversee two laws. One is the Privacy Act, which covers public entities. I'm not going to talk much about it today because it doesn't apply to what we're doing. It's safe to say that it's 20 years old and badly need reforming.

The other act that we administer has a long title, it's called the Personal Information and Protection of Electronic Documents Act or PIPEDA. I'm going to call it the private sector law because that's what I want to talk to you about today. It's much more recent and it applies to our commercial private sector.

Our office investigates complaints that are brought to us and also ones that we initiate ourselves. We mediate disputes, we audit compliance with our legislation, and sometimes we make our investigation findings public, even naming, if we think it's in the public interest, the parties that were involved.

In some cases, we also go to court for remedies. Our federal court can order companies to comply with our private sector law and can also award monetary damages.

I just want to make brief mention of the differences between the U.S., Canada and Europe. The European Union and Canada, both centrally supervise the private sector's use of personal information and, as most of you know, in the U.S., the regulation of the private sector on this issue is much more dispersed.

Our office has taken the position in a couple of cases already that an IP address is personal information within the meaning of our law, to the extent that it can be linked to an identifiable individual. So, all of the web analytics data that we've talked about that's such a rich trove, such as the referring site, the referring search engine, the keyword and phrase, the time of day of the visit, the machine properties, such as the IP address and browser settings, as well as the complete individual click stream data -- the extent that all of this data can be associated with a person, we take the view that it's personal information and that our law applies.

We've heard, and I must say I think it's excellent that the discussion's going on that people are thinking about how to anonymize the data. It's important because it's now because of the capacity of technology much cheaper and easier to just keep the data. It takes effort and thought to actually anonymize it and dispose

of it. And I see a few folks nodding. You've obviously had to deal with that.

So, the servers of search engines generally record the search, the request, the URL, the IP address, the browser type and language, the date and time of the request, and cookies that can uniquely identify a user's browser.

It's going to be important for companies, I think, to render the data anonymous. There have been examples where people have tried to do that, but when it was released the information they thought was anonymous could then be matched with publicly available data and lead to identifying individuals. So, actually, it's a bit of a task.

I want to talk to you a bit about trans-border data flow. A company in Canada that outsources information processing to a company that operates elsewhere has to tell customers, under our law, that other information that's being processed elsewhere may be available to the law enforcement agencies, for example, of that other country, and our law demands that organizations be transparent about their personal information handling practices so that when a company is contracting out, they have to try, by contractual or other means to the extent possible, to get that

subcontractor to abide by the requirements of our law.

For example, in a case that we investigated and that went to our federal court, a telecommunications company was found to have violated our law when it failed to tell customers when they first signed up that it was going to sell their listing information to third parties.

Our office has investigated many complaints that involve international companies. Most recently, the Society for Worldwide Innerbanc Financial Telecommunications, or SWIFT, and also a case that some of you will probably be familiar with, the TJX Winners and Home Sense case. In the Winners case, we issued a joint report about a month ago with the Province of Alberta, and in that case, which we've made public and it's on our website, we found that the company collected too much personal information, didn't adequately safeguard it and kept it for longer than they needed to do for their business purposes.

Many of you will know that that case involves the data breach of over 45 million credit and debit cards and driver's license numbers in the U.S., Canada and Puerto Rico.

Canadian Courts have held, and we've taken the position, that our private sector law gives Canadians the right to have their personal information protected,

whether the business is collecting using the information in provincial context, nationally or internationally so that the privacy commissioner has jurisdiction to investigate complaints relating to trans-border data flow.

The examples that I'm giving you, I think, show the complexity both for regulators and for industry. Consider, for example, 3D online mapping or Google's StreetView and Microsoft's Virtual Earth. Similar to many other applications that we're seeing now, this software, many of you have seen it, displays the street level photographs that were taken in cities across North American and appears on the maps function. When our office learned that this was going to be deployed in Canada, we wrote to the company saying, just a minute, the photos appear to have been taken without the consent or knowledge of the individuals who appear in them, and we understand that if they're going to deploy it in Canada, they'll do it in a way that will anonymize the data, so either a low resolution or blurring of images.

What the online debate and online advertising shows is that there's really three aspects to the privacy. Up until now, we've mostly been talking about informational privacy or the notion of control over one's own information. But there are two other important parts

to it. One is accessibility or the ability to control who has access to you and to what extent they have access to you. And the other part is expressive privacy or the chance to freely express yourself and associate with others.

There's a case in Canada that's been in the news a lot lately of some young folks working at our border services agency who said some unfortunate things on Facebook and subsequently lost their jobs. So, they have now learned about sort of the intersect.

In closing, I think I'd echo what some of my co-panelists have said. Your personal information, your data, has huge economic value and technology makes it easy to gather vast amounts of data about individuals in real time.

What I see for the future is that developments like developments in nanotechnology, which are going to exponentially increase the capacity of computers to store and process information in real time, make these kinds of debates even more important.

Thank you for your time.

(Applause)

MS. KRESSES: Thank you. We have a couple questions up here, but it will be just a moment and we'll open the mic. So, if you want to go ahead and stand up,

if you have a question you want to ask, that would be great.

I would target this question to Amina, but also I'd be happy to hear from anyone else who has thoughts on this issue. That is, Amina mentioned the worry that there's a potential that the data collected would be used for price differentiation or some other sort of discriminatory practice and I want to get a sense if what you're saying -- are there signs of these secondary ill uses already in effect or that they're likely in the short term? What are you specifically seeing?

MS. FUZLULLAH: Well, I mean, I think that it's rather difficult for consumers to know -- I mean, I hope I made it clear that one of the problems is that it's just not a transparent system. Consumers aren't aware of the price their neighbor is getting inside of their home, at their computer, that's different from the one that's at their own.

So, it's really difficult to even track this kind of behavior because it's not like you're standing in a store and you just heard somebody say, oh, you get this shirt for $4.95, and then you walk up and they're like, well, that's $15.95. So, it's actually rather difficult. I think that's part of why we want more transparency in the process so that we can actually have consumers aware

that if there is this kind of changing, that they're actually aware that it's happening and are okay with it.

Thank you.

MS. KRESSES: Does anyone else have anything to say?

(No response)

MS. KRESSES: I think I just want to move to data retention for just a second. It's something that I hope we'll get into as the panel enlarges in just a minute, but I would ask this of Microsoft and Google and Facebook. There's been discussion of how companies are moving to a shorter time for keeping their data and a shorter time until they anonymize the data. Why is it important to keep the data tied to an IP and date and time for as long as a year to two years? What does that serve?

MS. WONG: I'll try first. Here we go. So, as I was saying, we are always engaged in a discussion with our users, with regulators, with privacy advocates about privacy issues generally and logs retention became one of the issues that we were having a more frequent conversation about, and that's why recently we were one of the first to announce or were the first to announce that we were going to have a logs retention policy of 18 months. So, the question is why 18 and how did we come

to that?

There were a number of factors that went into it. One was making sure that we were providing the most robust system that we could in terms of the services that we offer, and let me come back to that. Another was obviously the concerns about users about having a definite time period that they would know when things were retained and then when they would be let go. The third was security for our system, and I'll talk a little bit more about that, as well as avoiding fraud and spam to our index. Then there were just like the mundane obligations. Remember that all of these clicks on our services, including the clicks on our ads, are the record of how we earn money. The clicks to the ads is how we record it. It's our auditing trail. So, there are tax auditing/SOX compliance issues around keeping that kind of data as well.

Let me talk a little bit about the robustness of our services. When we use our search logs, we do a lot of different things for quality. So, if you've used Google Search and sometimes you get a little tag at the top that says, did you mean X, because you put in a typo. That's actually generated based on the research we do in our search logs so that we can identify when a unique user is typing in something and then corrects it

immediately because that's a typo.

So, we have to have a certain volume of queries in order to be able to identify that. Well, in fact, we actually have to have a larger volume because we have a lot of English users, but in order to serve our users who are viewing our site in Lithuanian or Thai, we actually need a much longer period of time to get the right volume of queries to develop the same robustness.

That works the same, and probably more importantly for us, actually, in the area of things like security or click fraud in order to identify people who are trying to hack our system or defraud our index, in other words, try and send us signals that make us believe certain sites are more relevant than others. We actually need to know not just what is the region that these clicks are coming from, but is it a single computer or a group of computers that's continually trying to attack the system. So, that's the reason that we came to 18 months.

MS. KRESSES: But for the average person, does the 18 months -- I can understand the security thing where it really is that computer, and is it not possible to flag those sorts of items? What does the IP and the time and stuff give you over the 18 months in particular?

MS. WONG: In a security setting, one of the

things to know is you may be having a security attack at a particular point in time, but the problem is that someone was probably practicing that attack for many months prior to that. So, one of the things about having a long period of time is being able to go back and look for the same pattern and try and identify again who the bad actor was in order to stop the current attack.

MS. KRESSES: Thank you very much.

Diane, do you have anything further to add on that?

MS. McDADE: Sure. Microsoft also wanted to take a closer look at retention time frames and we recently had a long examination on that, and our first area to look at was search because we felt that was data that many people equate as sort of like their stream of consciousness and they're very sensitive about it. I think everyone in the industry wanted to make sure that we were able to anonymize fully search queries associated with a single unique identifier and not have that data fall into the wrong hands and also not be available through a government subpoena. So, we really wanted to bring down the time that we held search query data in an identifiable format.

We looked, and many of the same concerns that Nicole just raised, we found were also true in our

environment. I'm going to speak -- she spoke a little bit about the relevance factor, that's also true for our search service, but we also know from a security side that -- and that's where really the length of time is needed, is that it isn't just useful to understand the security threats that have happened in the past, but often looking at the past data helps us to look and predict new attacks. We really need that data to be able to look at seasonality and normalize for that because of our patterns and Internet commerce, Botnets and the click fraudsters highlight different seasons when they know people are going to be most active in ecommerce. So, we really did feel the need for the 18 months.

Most importantly, though, I want to emphasize that we made the decision that after that 18 months was over, that we would sever all unique identifers, all cookies, any other identifier besides the IP address so that data then, our search query data, would be completely aggregate, thus anonymous and could never be pieced back together internally at Microsoft or, when a request might come in, handed over to any other authority. So, we feel we've accomplished this. We think this policy will go into effect in the spring. It's actually a stronger policy than the one Google adopted and we feel that this might be an example where

others in the industry are making sure that search queries really are anonymous after that 18-month period.

MS. KRESSES: Thank you. And we'll move into questions.

MR. CHESTER: Jeff Chester. This is for Ms. Wong. I do want to say that it's very important, I wonder if you would agree with me, Ms. Wong, that the reason that Google and even Microsoft has reduced the retention period to 18 months is because of the extraordinary activity by the Article 49 Working Group of the European Commission which specifically criticized Google for how long it was retaining IP addresses and the extraordinary situation right now with the merger review of Google/DoubleClick, as well as a review of Microsoft/aQuantive.

But, could you speculate then, Ms. Wong, because you talked about the Google practices, you didn't talk about personalized search and when people sign in, but DoubleClick, how do you envision the DoubleClick privacy policies to be? Right now, DoubleClick is perhaps the largest provider of cookies on the planet, billions and billions of cookies. It has a behavioral targeting product, Boomerang; it has a retargeting product. It collects 100 different ways we interact with video online, through its Motif product.

How will all that data be treated by Google, do you envision?

MS. WONG: So, obviously, as you know, we're still in the review process and part of that means that because of gun-jumping rules you don't speculate ahead of what your combined entity will look like, but let me talk a little bit more in detail about DoubleClick.

So, one of the things about the data that DoubleClick has -- and you're right, they issue cookies, they collect data based on advertiser activity or clicking on ads and none of that data is actually owned by DoubleClick. DoubleClick holds it for its advertisers and publishers. Under its contracts with its advertisers and publishers, it actually has no right to access that data or use that data in a non-aggregated, individual form, except with the permission of its customers, and those obligations will flow to a DoubleClick/Google entity if that review is passed and we actually are able to acquire the company.

So, that's an important thing because we can't actually change -- we will own those obligations as well and we will not be able to access or use that data in a non-aggregated individual format either.

Separate from that, we actually haven't figured out, because there is no combined entity, whether it is

technically possible to use that data in combination with anything we have now.

And, finally, and probably most importantly from my perspective, is we don't know if it would be the right thing to do by our users, and I think that's all something -- I wouldn't speculate on that. I think that's an important conversation for us all to have as an industry as well as for us to have as a company.

MS. KRESSES: Thank you. Do we have any other questions at this point? Okay, great, we're going to move right -- oh, I'm sorry.

MR. SMITH: I'm Robert Smith, Privacy Journal. FTC workshops tend to invite corporate people who say that their company is not engaged in the very practice that is being investigated. It's a wonderful phenomenon and we've heard that today. So, let me try another way of trying to get the information out.

You all monitor what your competitors are doing and what's going on on the Net. Are there practices that you see that you disapprove of that ought to be discouraged? Are there practices that the FTC ought to take a very close look at? And if you look around and you don't see any such practices, let us know that, too.

MS. McDADE: Well, I'll speak to two things. One is I do believe that all sites obviously ought to

have privacy statements. I wasn't aware that 15 percent still don't of the top 200. I learned that this morning. I was surprised to hear that.

Second of all, if there are discriminatory -- adverse discriminatory practices in advertising, Microsoft would certainly be in favor of looking more closely at a contractual requirement that advertisers not engage in adverse discrimination and advertising based on behavioral targeting profiles.

Thirdly, I think that we feel pretty strongly that there are always, in every industry, outliers and that we want to work to help those folks understand that to make this environment work best, they're going to bring down the rest of the goodness from the online space. So, certainly, if there are people who aren't in compliance with NAI guidelines, for instance, we think they ought to join NAI and get involved. So, it's in our interest to make sure that those outliers come into line with generally accepted practices.

MR. KELLY: I think anything that's actively deceptive in getting people to reveal personal data and to share it broadly is pretty obviously well beyond the pale, and we do still see that on the web today and that's completely unacceptable from our perspective. I think most other companies up here would say that, too.

MS. CAMPBELL: I'd just offer one comment and I made it in my remarks. But transparency, I think the industry as a whole needs to be more clear with the users exactly what's happening with their data, who it's being sold to, why it's being marketed, especially if you look at the average age of the users of many of the social networking sites, for example. Many of them just see, oh, it's a free site, I can use it, and they're surprised by the ads that pop up in their email or on their mobile phone a few days later.

So, particularly with younger audiences who may not be as aware, it would be a good idea, I think, for industry to be open with them about what's happening with their data and the value that it has.

MS. KRESSES: Any else want to comment?

MS. WONG: I agree with all the other comments, including the deceptive practices, which I think we all agree is inappropriate. I think that the biggest challenge for us is not that there are -- not conquering the bad practices because I think the FTC is looking at that very carefully, but I think that the harder challenge is whether or not how we approach it in light of the current technologies is still up to date, and that is, I think as Trevor may have talked about earlier and some others, there are so many more tools available to us

from a technological perspective on getting this right, and I think that that's why we're trying to engage in an industry discussion about what does Phase II look like.

MS. KRESSES: Thank you.

(A brief recess was taken)

SESSION 5: ROUNDTABLE DISCUSSION OF DATA COLLECTION, USE AND PROTECTION

MS. HARRINGTON: We have our discussants poised to discuss. We have the audience members sitting down and being quiet. We're ready to go. This session will have a different format. First of all, it's billed as a round table discussion, so imagine round. But we will be involving all of our attendees or the possibility of attendee involvement throughout this discussion. We're not going to necessarily wait until the end of this session to have questions and comments from those of you who are here.

There are no presentations at all in this session. We have an hour and 45 minutes unplugged, unscripted. And I think that the objective is to focus on key questions, really where the rubber meets the road. So maybe the first question is, what's all this fuss about collecting information? Let's get down to it. What is being collected? What is it that's being collected? How is it being used and how can it be used to identify the person about whom the information is being collected and stored?

So, the first question that I have, and I'm going to, I think, throw this to Nicole -- is -- and Jamie's saying I should introduce the discussants. But

actually I think what we'll do is have the discussants introduce themselves as they discuss. So, we'll just go.

Nicole, we met you in the last session. What's involved in taking an IP address and perhaps the other items that you collect on every search and reverse engineering those to identify the individual whose information is being logged and collected?

MS. WONG: So let me go back to what's in that log file --

MS. HARRINGTON: Yes.

MS. WONG: -- because I think that's what you're asking me. And, again, for those of you who have never seen a log file, we actually have what it looks like in our privacy policy FAQs as well as a really great video describing what it is and breaking down all the component parts. But, basically, it's this.

If you go up to our site and you're not logged in with us as a registered user, then the thing that we will capture is, of course, your query because that's your question to us. That comes with certain information about your computer so that we render the screen back to you appropriately so your browser, the language preference that you have, the IP address, and the cookie, and those are the two things that people concentrate

most on in terms of being unique identifiers.

Let's talk about what those are uniquely identifying. An IP address will identify a computer connected to the Internet at that time and date. So, it's very specific. And, currently, many Internet users still have dynamically assigned IP addresses. So, if you're an AOL user, when you sign on to AOL, AOL is going to assign you a unique number for your session. When you log out and then go back on, you're going to have another IP address. So, again, it's not identifying you as a person, it's identifying your computer at that time for that session.

A cookie identifies the computer browser. So, again, not identifying a person, but the browser that the cookie has been set on. It's a file that goes into the browser. That is unique, perhaps, to the computer, and so that means that if you have a laptop, and you have one browser and you don't change it, you're going to have the same cookie over and over again. If you switch around to different computers, you're going to have multiple cookies that you're coming in at different times. If you go to an Internet café, obviously that's only identifying the browser on that Internet café computer. So, those are the two identifiers.

MS. HARRINGTON: What's involved in taking

those records and running them against other databases to identify the individual who generated those records?

MS. WONG: It's a bit of a data chain. So, the cookie you would need to seize the person's computer and be able to match what Google has as a cookie to what's on that computer. An IP address, you would have to go back to the ISP and ask them who was the user logged on at this date and time, have them go through that record, and then if they are an ISP that charges someone, they theoretically have that connected to a credit card or something like that.

But, remember, that means that an IP address is really like the license plate on your car, so it can identify the car, but it's not identifying the person driving.

MS. HARRINGTON: But it can be a juicy piece of information, the license plate number on your car.

MS. WONG: The IP address. Absolutely. I think a police officer would tell you, yes, if I've got a license plate number, that's a good piece of information for me.

MS. HARRINGTON: Okay, Richard, I'm going to ask -- where are you, Richard? I want to ask the same question of you. You've heard the discussion of what it is that, for example, is routinely captured, logged, by

search engines. How do you see that information as being used perhaps to identify individuals?

MR. SMITH: Well, it's sort of a complicated question, but I think with Google, I will have to take issue with what I just heard. If you sign up with Gmail, of course you identify yourself, you provide a name, and the last time I checked, you even had to provide a cell phone number where they could do verification back that you're a real person signing up for Gmail. So, there's an association there with personal information, which is an e-mail address, a name, and potentially some other information that's associated with the Google cookie.

And you can really see this if you go to the personal history feature of Google and you have that turned on, it will keep a record of all the searches you've ever done on Google since you've turned it on and been logged in to your Gmail account.

So, the association with an individual is a little bit different than a license plate. It's a much stronger thing. A cookie is identified with personal information if that information is provided to someone. So, to say that they're anonymous is extremely misleading in my opinion.

As far as IP addresses go, the same thing can happen. If you have an IP address and you say, okay,

let's imagine a Google search engine which would allow someone to search the Google surfer logs, which probably exist since they're a search engine company, and say, okay, let me see where all this IP address has been to. It kind of depends on whether this is a static or semi-static or a proxy address. There's a lot of different things. But you can tie an IP address to an individual without being the ISP, and this is done all the time, by comparing different pieces of data together.

So, the idea that these things are anonymous or they can only be identified by the vendors I think is not an accurate situation.

MS. WONG: I need to correct something, which is that if you sign up for a Google account, a Gmail account or some other account with us, then the data that is associated with your account is held in a separate database than the log's information that's held when you do searches when you are not authenticated with our servers. Those are two different databases, two different cookies. They are not put together. That's really important to understand.

MR. SMITH: I guess I'm confused because if I look at search history for my Gmail account I see everything I've searched for.

MS. WONG: It's just because you signed up for

an account.

MR. SMITH: Yeah.

MS. WONG: Right.

MR. SMITH: But it does make this connection, and maybe it's two separate databases, and that's something that can be connected at any time that's needed.

MS. WONG: But they aren't. The second thing, because you had mentioned like anybody could go in and surf the IP addresses, just to be very clear, our IP logs are extraordinarily sensitive to us. They are absolutely locked down with the highest level of security and only people with a need to know access to them, for purposes of maintaining those logs, have access to them, and they are specifically trained in terms of security and privacy.

MS. HARRINGTON: And I'm going to come back to you and others in a moment with a question about your 18-month log retention and the security benefit or need for that. So, hold that thought.

But I want to turn to you, Diane, with a similar question. What about the information that is routinely collected on searches and the ways in which it can be matched against other information sources to identify individuals?

MS. McDADE: Okay.

MS. HARRINGTON: And the ease with which that can be done.

MS. McDADE: Microsoft doesn't offer a personalized search service today in the way that we just described with Google. With our search engine, we retain the search queries, and we will use the search queries in research purposes to see if we can return a better set of results to that user based on the fact that they recently searched -- let's use the example of a vacation. If they were searching before for a particular set of terms and they click, then we want to be able to know that that information was useful to them.

So, for relevance purposes we'll look at cross-session searches, but we're not using that information to identify the individual per se. We're using that information simply to provide and furnish the best relevant results.

MS. HARRINGTON: You may not be, but how easy would it be for someone else to use that?

MS. McDADE: For someone else?

MS. HARRINGTON: How possible is it for someone else, some other party?

MS. McDADE: Outside of Microsoft, outside of our search service, it would be very difficult, if not

impossible, for someone else to obtain that data. That data is secured very carefully. And as we talked earlier, it's retained in an identifiable format for 18 months and then it's rendered completely anonymous after those 18 months.

But the search data is not shared. It's not available to employees on any kind of routine basis. That data is handled very, very carefully with a lot of security protocols around it to ensure that we never compromise that integrity of maintaining the confidentiality of it.

MS. HARRINGTON: Joel, did you have a question? I'm looking -- and people in the audience, please.

MR. WINSTON: I think there was a little bit of a disconnect. I think the question is, could another company that is doing a search that isn't under the same policy constraints that Microsoft might be take that data and combine it with other data and come up with an identification of that individual?

MS. McDADE: No. We wouldn't share somebody's data without their explicit permission.

MR. WINSTON: That's not my question.

MS. McDADE: Okay, well, when you say another company, I don't understand.

MR. WINSTON: Theoretically, take Company X

that runs a search engine and it tracks what search terms people use and collects what other information they might collect. Putting Microsoft aside, could they take that information and reverse engineer it and identify that individual?

MS. McDADE: Well, I think as Nicole mentioned, if someone has an IP address and they have a reason to approach lawfully the Internet service provider, they can ask and, of course, the Internet service provider needs to follow their guidelines and follow the law, but they could ask to find out who that person is. But that's the only way you would trace it back to a known identifiable subscriber.

MR. WINSTON: Thank you.

MS. HARRINGTON: Yes?

MS. HARRIS: You know, we're talking about --

MS. HARRINGTON: Can you introduce yourself?

MS. HARRIS: Yes, I'm sorry. Leslie Harris from the Center for Democracy and Technology.

MS. HARRINGTON: Thanks, Leslie.

MS. HARRIS: We're talking about this as if the only model is a cookie-based model that is one step removed from an ISP, and I think it's important for us to put on the table not just sort of what today and yesterday's models, but where we're going. We know there

are companies now whose business model is to work with ISPs through DPAC and inspection directly pull out a consumer data stream and, you know, exactly what they're pulling out. So, we're not one step away from the ISP, we are the ISP. We're not in a model where there's some cookie to get out of the data collection.

I think the question is, where are we going? Those models continue to assert that those are anonymous because they're, quote, "throwing things away." We don't know what they're throwing away, but we know that both the ISP and the tracking company have pulled somebody's entire data stream out. There's certainly going to be a lot of -- if not personally identifiable under old definitions, I would say personally identifiable under definitions we need to start thinking about. I think there's almost nothing that's anonymous and a minimum that's pseudo-anonymous, and we have to start thinking about it that way in policy.

MS. HARRINGTON: Kathryn?

MS. MONTGOMERY: Yes. I just want to sort of broaden the discussion --

MS. HARRINGTON: Can you introduce yourself, Kathryn?

MS. MONTGOMERY: I'm sorry. Kathryn Montgomery, American University.

I just want to broaden the discussion a little bit beyond the specific operations of individual companies and companies who came here really to show us how they are not engaging in any kind of behavior that should alarm policymakers or consumers because we really need to look at, as Leslie was just saying, where these practices are going and what the general trends are in the industry and what a lot of existing companies and new companies are doing and planning to do in the future, and that is the bigger story here.

I would also encourage people to take a look at the complaint filed by the Center for Digital Democracy and U.S. PIRG this morning, which outlines a lot of these current developments and plans for the future. I'm finding myself frustrated to hear about individual corporate policies and promises, and I don't get a sense that we're moving toward industry-wide operationally sound policies that I think we will need in order to create a level playing field for both the consumers and for this industry. This is what we needed with children and what we were able to get with COPPA ten years ago.

MS. HARRINGTON: Kathryn, I think what we're trying to do, though, is to be as concrete as we possibly can be here to focus and flesh out facts. I'm interested in -- I think it's a very good point that you make that

we also need to look at emerging models and at future directions, and I'm wondering if there is any particular emerging model or trend or if there are any particular ones that you can point to as being of particular concern here, and if you can explain, as concretely as you can, what the concern is, what is the information, how is it - -

MS. MONTGOMERY: Okay.

MS. HARRINGTON: Thanks.

MS. MONTGOMERY: I'm concerned about a whole range of things, but I have been looking at what's going on in the teen marketplace and the emergence and growth of social networking software platforms and a lot of other things targeted at teens. And it's not just banner ads, by the way, because we're looking at user-generated video, we're looking at viral, we're looking at a whole other set of things that go beyond these examples of banner ads.

But what is emerging in that market is a system whereby everything that these young people do and say is fair game to marketers. They may be able to cordon it off to their friends with that kind of privacy, but the model that's emerging is that the data that they provide in their conversations, in their behavior, among their friends, in their user-generated video and the videos

they watch, all of that is compiled into the profiles that become the fodder for behavioral targeting. And, again, if you look at what the industry itself is saying, that's where it is going.

MS. HARRINGTON: Chris, do you disagree with that?

MR. KELLY: Well, Facebook is setting policies that basically restrict this and give users control over it. I mean, that's a situation where we're trying to lead and to set these rules up in advance. What we want is a race to the top around this. If you start to talk about industry standards that are the lowest common denominator, that's not good enough for us.

MS. HARRINGTON: Now, Kathryn, when you listen to Chris, what are the harms that you're concerned about?

MS. MONTGOMERY: When I listen to Chris the harms are that he's the good guy, or at least he's presenting himself as the good guy, in a very volatile industry where a lot of money is going to be made, and there are no rules. There are no rules. Also, my concern is that we're talking about a medium that young teenagers, and teenager is 13 because COPPA only protects under 13, are on there living their social lives and their personal lives.

They are online on search engines and in social

networking platforms exploring who they are, sometimes looking for sensitive information and help with very difficult personal problems. Their lives are, in some ways, to the industry, to the marketing industry and to this apparatus we've created, they're open books. I think it's a wonderful medium for these kids. I'm not saying we should take them offline, but I'm saying that -- and I'm not saying we shouldn't advertise to them, but I'm saying that we need some rules. And if Facebook wants to lead in this area and we can use that as a model to create some rules that could be enacted, that's what I'd love to see.

MR. KELLY: This is why we've set quite a number of rules around how data gets accessed on Facebook and how it doesn't get accessed most of the time. We've made promises in our privacy policy about the availability of personal data and how it just doesn't -- I mean, we collect a lot of personal data. We let users know that it's associated with their profiles. We don't resell it to advertisers. We enable advertisers to target advertising based on it, but we're not selling it to create these broad industry profiles the way that is speculated.

We're setting rules. We think that they're responsible.

MS. HARRINGTON: I have a couple questions back, Kathryn. Are there particular ads now that you're concerned about that are being served up to teens on Facebook? You talk about a need for rules more broadly in this industry. Tell me what you think those rules ought to be.

MS. MONTGOMERY: No, there aren't specific ads. That's not the issue, really. But I do think there need to be some rules about clearer disclosure to young people. I don't think kids have a clue what's actually going on online. I mean, they may know how they can protect their own spaces and only share them with their friends, but they don't understand how online advertising works, they don't understand behavioral targeting.

And the other thing is that there need to be some limits on the information that is collected and the kinds of information. We heard a little bit earlier this morning about some areas that are troubling and difficult. There are no clear lines about what is being collected and what isn't being collected. And I think that they need to have access to the information that's being collected on them, and even if it's not being sold to advertisers, it is being pulled together to facilitate advertising so that targeted advertising can take place, and that's often based on psycho-graphic information.

We just learned from some of the research we've been doing that there's even information about whether they smoke or drink or behavioral kinds of things that can be pulled together into profiles that can be used even within the company.

MR. KELLY: I would stress it's also being used to keep inappropriate advertising from kids.

MS. HARRINGTON: Okay, here are the next two questions.

MS. MONTGOMERY: That’s not a model.

MS. HARRINGTON: First, a question for Larry.

I'm going to get back to her, okay?

Larry, following on this stream, if you could answer what is it that teens know about what's being collected, if you've got data on that? And then back to Chris, and perhaps Diane, what kinds of ads is Microsoft going to be serving up on Facebook, what will the rules for that be? And then, Pam, we'll get to you after that.

DR. PONEMON: Okay, so, I know that we're talking about a lot of different things, a lot of moving parts. I'm going to focus on consumer-based research findings and, specifically, we'll talk about something that we refer to as the privacy age gap. Because it appears that younger people, people with the demographic below 25 years of age, and especially those below the

demographic of 18 years of age, view privacy differently. It's not that they see it as less important, but they see it as something different than we old fogies, like my age demographic, the way we see it.

And the reality is that for younger folks anonymity is, in their mind, whether it’s right or wrong, is a substitute for their privacy. They also look at privacy issues from a kind of physical space issue. Like, for example, I don't want you to know that I'm here physically or I don't want you to listen into my cell phone conversation, I especially don't want you to read the contents of my Ipod or my Iphone. So, to them, it's a different set of issues.

Most people aren't even thinking about privacy-related issues when they're in a social networking site like Facebook or MySpace or you choose your favorite tool. So, from their perspective, these privacy issues are not salient, which gets to the point that if we have a risk, there needs to be some way of communicating and educating.

Now, with respect to disclosure, we've been through this. I've been at this table for many, many decades and definitely participated in FTC workshops for the last ten years, and I will safely say that no one reads a privacy policy, except my mother who's 86 years

old and she reads also food labels. That's her full-time job. Since we know that as a reality, I don't think a good solution is to assume that a clearly written, well-articulated privacy policy will have any meaning at all.

Then the third issue I'd like to say -- and this is because of my background in information ethics -- the solution that we impose on an organization, if we believe the organization is evil and sinister, is different than the solution that we impose on organizations that we believe to be good. If we have a belief that Google is evil and there's some large conspiracy, then basically rules will have to emerge and very clearly articulated rules. But if we believe that organizations like Google, Microsoft, and others are trying to do the best thing that they can and keep this information age moving, then sometimes rules get in the way of progress and all sorts of things.

So, we have to think about the need for rules because rules exist and many rules aren't followed, it requires a lot of enforcement, and at the end of the day there could be real serious economic consequences that could harm an industry that is generating billions of dollars in jobs and all sorts of good things.

Anyway, that's my spiel. I'm sorry for taking so much time.

MS. HARRINGTON: Okay, thanks, Larry.

Now, Chris, back to you, and perhaps Diane. What kinds of ads are Microsoft going to be serving up on Facebook? What will the rules be for that?

MR. KELLY: Microsoft will be serving a portion of our ads on Facebook. Facebook will still be serving quite a number of its own ads as well. But Ad Center will be a placement agent for a number of different ads on Facebook going forward. There's not a data sharing arrangement between the two entities, there's not a whole bunch of options. They are going to be a standard third party advertising network. We're very excited to be in a partnership with them now.

MS. HARRINGTON: Okay, Pam?

MS. DIXON: Thank you. I'd like to respond to your point. I really felt like there needs to be a period put at the end of that sentence. Oh, I'm supposed to introduce myself. Pam Dixon, World Privacy Forum.

So, if a consumer chooses to give associative information that is then tied to their IP address, then they may become identifiable to that company. It's just very simple. Period.

I'd like to address the issue that seems to be floating up to the surface fairly frequently throughout the day, which is the issue of sensitive information.

The companies who are here today have made it very clear that they do not keep or want to keep or have anywhere near them, quote, unquote, "sensitive information." There's an article where a large company said they do not keep records on more sensitive topics like specific medical conditions. Okay, so that's good, right?

But here's the tough thing about that. What constitutes a sensitive medical condition? All of us know there are thousands of diseases. Which diseases do we pick? Is it HIV/AIDS, is it Huntington's Disease, is it that we take vitamins? The health care sector is very broad. So, what constitutes sensitive information, I think, is a very difficult question that we need to tackle.

I think in the financial sector, we have prohibited factors under ECOA, Equal Credit Opportunity Act. So, for example, you cannot deny someone a mortgage based on their race. So, how do these kinds of standards apply to sensitive information in this space? And I think that that would be a very intriguing discussion and an important discussion as well.

Finally, what I would say is that if you have information that's being stored and the information is somehow breached or released or involved with a secondary use, we all know, and I think can accede very easily,

that consumers may be exposed to harm. For example, I've heard some discussion about discriminatory practices, et cetera, et cetera.

I think that a lot of this can be limited by simply defining what constitutes sensitive information.

MS. HARRINGTON: Okay, thank you, Pam.

Lisa, this is an issue that I know there's been some focus on in Canada. Do you have any comment on the health profile issue and how you're dealing with it?

MS. CAMPBELL: Yes. I talked to a couple of folks here. We hosted in September a conference of data protection commissioners from around the world, 600 people were in attendance, and a lot of the conference focused on health professionals' users of personal information. They've got a great need -- interestingly, there are some similarities. They want aggregate data, they want to be able to collect it in real-time and look at it over time to predict all sorts of things, like the movement of diseases across populations, when epidemics are going to occur, what are the geographic factors, that sort of thing.

So, they're quite interested in finding ways to anonymize data so that it can be accessed by researchers around the world and kept in a secure environment, and so that they can generate user trust. In other words, get

people to give them the data because really without that data, they can't do their work, they can't get grants, they can't cure diseases. So, we learned quite a bit from the health professionals.

One interesting concept that they came up with, and I think it's probably a reasonable one, is that you probably can never completely anonymize data. That's a difficult pill to swallow for some folks, but they've arrived at a standard, a definition that says that if it becomes either impossible -- I think, Diane, you said it, either nearly impossible or extremely difficult to identify someone from the data, then you've achieved a standard of anonymization that's workable for the industry.

Does that answer your question, Eileen?

MS. HARRINGTON: I think it does.

MS. DIXON: Can I follow up?

MS. HARRINGTON: Yes, Pam.

MS. DIXON: We have a similar standard, of course, in HIPAA where there's a fairly detailed standard of what constitutes identifiable, what constitutes de-identifiable. I should say, though, that IP address is going to be a very tricky factor under this kind of a standard because if it's in a health record and it's in there at all, we're talking name, we're talking anything,

it is considered protected health information. So, it's a much deeper standard.

But I do think that the pieces that could apply here are that there is a very detailed specific standard. And the process you're referring to, at least under the HIPAA standard, there's a specific percentage of confidence that it cannot be identified. I believe it's approximately 1.7 percent that you could not possibly identify it. So, I think that works, too.

MS. HARRINGTON: Pam, you make a good point that HIPAA certainly applies here, but also maybe the health area is a good one to look at for a minute for purposes of this discussion to talk about sort of how lines are drawn.

We've heard a lot of talk about contextual advertising today. When a consumer searches for information about particular health conditions or goes to a website that is about health or disease, how do companies draw lines about serving ads and what kind of information is collected and how is that -- what are the policies for retention and anonymization of that information? Maybe we can open that subject up here as one that may be illustrative.

Again, if we can be as concrete as possible in this discussion. We don't want to hear about broad

concerns, but rather what are the specific harms that we're concerned about? What are the concrete practices that are used? That would help us greatly.

Some of our discussants we have not yet heard from or recognized and, so, we may be be looking to you to get this rolling and -- Amina --

MS. CAMPBELL: Sorry, if I could just add one point on that.

MS. HARRINGTON: Sure.

MS. CAMPBELL: The health analogy is an important one because initially they'll collect, for example, a sample of DNA for one purpose. The data is then collected and stored over time and, obviously, it's a rich store and they'll find other uses, other things that they want to search in the data, and we see the same thing happening with advertising.

One piece of information about a person collected for one purpose then becomes quite interesting and useful down the road for many other purposes other than the ones for which it was provided.

MS. HARRINGTON: For purposes of directing advertisement or --

MS. CAMPBELL: Yes, quite possibly. So, you've collected one bit of information about a person that they consented to and understood. You then store it. But

later on you find that it would be useful to know that for targeting them for something else entirely.

MS. HARRINGTON: Let me ask the question. If the use to which it is put is serving ads, what's the harm?

MS. CAMPBELL: Well, it depends. What were the terms of the contract, if you will, that you entered into with that individual in the first place? Do they really want to have the other ten ads that the company has decided to give to them?

MS. HARRIS: Eileen, can I respond to that?

MS. HARRINGTON: Sure.

MS. HARRIS: I think in the health area where as a nation we've made some policy decisions about wanting to increase the liquidity of health data, data exchange, we're building online PHRs. The biggest concerns that consumers have is privacy. And there is no set of data more personal than health data.

So, if you're on a health site searching for diabetes, you may not be uncomfortable with the fact that an ad is served up in real-time for things related to diabetes. But if that became a profile about your illness that ads were served to you across the web, I mean, the privacy harm to that I think is enormous, also because I think none of this ultimately is anonymous and

that you could get to the point of building sufficiently rich profiles.

I mean, with my apologies to AOL, we were able to identify people simply on search pretty quickly, that if we start creating these profiles with health data -- so, there's a question about the harm from serving the data, but then there's also the question about if they become part of or very specifically intentionally a profile about somebody's health data.

First of all, I think we've set back the possibility of using this technology for good, for health care, considerably. But, secondly, I think that would be an extraordinary breach of privacy.

MS. CAMPBELL: The only parallel I was drawing was simply that they have been wrestling with how to anonymize data for some time, and that's a good lesson.

MS. HARRIS: I understand the anonymize data for research, but when you get into advertising, you're in another -- I am really curious to hear how companies are doing it.

MS. HARRINGTON: I want to see if Amina has anything that she wants to say on this. You don't have to, we'll come back to you, but just --

MS. FUZLULLAH: I'd actually agree with the difficulty of anonymizing data. I was sitting here

earlier and I meant to say one thing, I'm wondering why we have special programs just for children, why we have special programs just for health care. Data is important to each individual user in a number of ways. So, if we can do it for children, if we can do it for purposes of health care, then why don't we have these protections for consumers broadly?

I'd like seeing tightened scrutiny over that type of data, but it's really important that everybody benefits from any kind of protection that we're going to throw out there.

MS. HARRINGTON: Okay. We're going to hear from Scott, and then Diane, particularly on the question of how the lines get drawn in serving up ads, and Kathryn wanted to add something to this as well.

MR. NELSON: I think there's an intersection that we're just old enough, as an industry, to start understanding exists. We're talking about behavioral and advertising, and advertising functions as a commerce vehicle that is driven by ROI. Advertisers behaviorally target because they want to make better, more effective use of their media and publishers behaviorally target because they want to sell their inventory for the most money possible.

We're getting to a point where the cost and the

benefit of behavioral targeting is starting to intersect. There's going to be a moment where we can build $10,000 solutions for $100 problems all day long with the technology we have. It's extraordinarily potent, and we're extraordinarily bad at using it. And there's a point where we can get the incremental lift we need for the media value without violating the concerns of consumers and their privacy.

I think it was brought up this morning. If we get a 1 or 2 percent lift across the network with some level of targeting, that can pay for a lot. And we don't need to go deep into some of the data that we've talked about here today to do that because, frankly, the technology just is not managed that well.

MS. HARRINGTON: What do you think about whether we may have gone past the point of necessity, for example, on the 18-month log retention?

MR. NELSON: Log retention. Our experience is that consumer behavior online is relevant for several days, okay? Log retention is great for the reasons assessed. Security, makes a lot of sense.

MS. HARRINGTON: Eighteen months for security?

MR. NELSON: I don't know. I don’t know their businesses well.

MS. HARRINGTON: Less?

MR. NELSON: I'm not a security expert. From a standpoint of targeting, people's behavior online unless they're buying a car or thinking about moving to another state, the purchase window is relatively short. And online has primarily been driven by direct marketing. Somebody can transact immediately in that session or within a couple of days, and then the data becomes very, very less viable.

So, the log retention for ancillary purposes, particularly post-campaign analytics to enhance performance going forward, which Google does well, makes a lot of sense. It doesn't have to be specific to the IP address or the cookie. That’s where we get into aggregate. Frankly, we get rid of data -- about six hours from now today's data for us is going to be garbage. We don’t need it anymore. We aggregate it, we get counts and we’re done. That's what the bulk of the Internet marketing and the actual advertising and technology does.

So, yeah, log retention, there are some reasons for it, but it's grossly overestimated what's really being done with those logs.

MS. HARRINGTON: Okay, I want to get back to -- Chanterria, do you want to say something about data retention?

MS. McGILBRA: Absolutely. I don't know if I mentioned it earlier, but at Netmining we actually have a three-month deadline on all the data we collect for our clients, and that's because we collect our data specifically for the client, and we feed that data immediately to the client. So, now the client has two databases, ours and the client's database where that information is stored. And at Netmining we made a personal decision that it doesn't need to be stored in two places.

Now, we do have clients that ask us to hold on to that data for historical reporting purposes, and even then, we charge them an additional fee to do that. So, we incentivize our clients to utilize that data for the sales cycle in their company immediately and then move on to the next.

So, I think it's just a different way to take a look at data storage, and really if you need to store data for 18 months, you're not really using it in the purpose of selling or, as you said, Scott, for a return on investment.

Who is the return on investment for if you're holding it for 18 months? It's definitely not the consumer.

MS. HARRINGTON: Diane doesn't want to comment

right now on line drawing, but I may come back to you with that question. We have a question from the audience

MR. GIVOTOSKY: My name is Nick Givotosky. I'm with Datasphere Interactive and I've been researching digital identity technologies for a certain period of time. I think that it seems inevitable that regardless of the point that was just made about the utility or the lack thereof of existing data that's being acquired, that there seems an inevitability about the further and further aggregation of data around individual identities or profiles, however they're characterized, simply because that's where advertising wants to reach users, is around their interests, across environments, over time.

This mantra of interoperability and cross-platform interoperability just suggests to me that it's not just about the web at all, and that point's come up a couple of times. But it leads to my question, which is even in the language itself we talk about your profile on Facebook, for example, or your profile. Well, in what sense is a profile yours or Facebook's? Who owns that data? Sometimes we're talking about privacy, but are we not really in fact talking about property?

MR. KELLY: I'll be happy to address it. You control that profile, full lock, stock and barrel. If you want to take away any piece of information from that

profile at any given time, go right ahead. We retain information for about 90 days.

MR. GIVOTOSKY: So, you can export that profile in a format that you can reapply in another environment or you can integrate it?

MR. KELLY: We're working on ways -- the worry about full export and sort of take it willy-nilly is that what often that means is other people outside of the environment want to get access to that profile. And we're working on ways to empower users to actually have control. The problem is that when you have a friends network, for instance, you're also looking at taking a bunch of your friends' data because you have those connections with them and a list of them, for instance, and things like that. So, we're working on a number of ways in which we can empower actual users to make those choices.

A lot of the talk about kind of complete openness in social networking platforms gets into other parties who want access to your friends' networks, and that just doesn't work from a spam perspective, it doesn't work from a privacy perspective, but we're working on this problem.

MR. GIVOTOSKY: So, an infrastructure that enabled user-focused export and management of user-

related data you think would be a positive step forward?

MR. KELLY: Absolutely. I mean, user empowerment in this field is the way to go.

MS. HARRINGTON: Leslie, you had something.

MS. HARRIS: Well, just a brief point, which is, yes, you can export the data out, but if the company is holding the data, under our laws you don't have a privacy interest in it and whether it's the government or a litigator coming to whoever's holding that data, I think most Americans don't understand that they really don't own that data. And that’s just a -- well, it is true.

If you're going to hold that data and the government's going to come to you, they've got to come to the website to get that data.

MR. GIVOTOSKY: Which is exactly my point.

MS. HARRIS: They may have to get a higher level of warrant. I'm not saying they're walking out without process.

MR. THOMPSON: This is where I’ll disagree with you. As soon as a company makes a promise, the FTC will be sure that if they don't meet that promise they'll be in here tomorrow. First -- let me finish.

Second is that what a company decides to do in terms of how it complies with -- when it gives up

information to the government is an important question that everybody should look at whatever that website's policy is.

MS. HARRIS: All I said was what was legal, legally required.

MR. THOMPSON: Okay, and what I'm saying to you is that some companies require that you deliver them a lawfully issued subpoena. I personally think those are the websites I would like to do business with. Okay? And I look for that.

So, when you're talking about what's lawful and what's not lawful, I wouldn't want to leave the impression that in the U.S. it's more or less a lawless land because it isn't.

MS. HARRIS: I don't think that that was my intention. It's just in terms of who has cognizable privacy interests under U.S. law, it ought to be the user, but it isn't. And, yes, there is legal process and, yes, some companies, if they're allowed to by law, will notify. In a lot of criminal cases, you can't. But at the end of the day, we don't have a law that requires that notification, et cetera. That's all I'm saying.

I'm not telling you that I think everybody's turning the data over without legal process. It's a pretty low legal standard for a lot of the data.

MS. HARRINGTON: Okay, we're going to -- thank you. We'll move on. Esther?

MS. DYSON: I want to go back to more of the -- Esther Dyson. I'm going to be on the panel tomorrow, so I will try and be brief now.

But I just want to make this distinction between what is promised, what the website says it will do, what is understood, which I think is the biggest problem, most people don't understand what the promises are in the first place, and then the third thing, what is delivered, whether those promises are actually kept. And if you promise I'm taking your DNA only for this purpose and then you go and use it for advertising, that promise isn't being kept. So, if we can make the distinction between the promise and the delivery, that would be useful.

The second issue is I've heard this word "protection," like protection from advertising. I think -- there is sort of two orthogonal points of view, which is, one, consumers need to be protected from bad things, and now we need to sit here and figure out what bad things are, which may be disclosure of medical information or whatever, versus consumers' need to have their rights and their contracts protected, so that if they understand what's going on, that's actually being

delivered.

So, I'm trying to turn this into a question, and the only question I can think of is the one that's in my mind which, unfortunately, is for Chris Kelly

MR. KELLY: I don't think that's necessarily unfortunate.

(Laughter)

MS. DYSON: Well, you might when you hear the question.

(Laughter)

MS. DYSON: I just came in from Russia, so I don't know whether this thing surfaced and disappeared. But last week I read that some of your employees had been poking around in some of your users' data, which clearly is not what you promised. So, a lot of the fear around this is that these promises won't be delivered because how do we know?

MR. KELLY: So, let's be clear about what happened and what happens in companies everywhere that have customer service to deliver to users. There have to be people at companies that have access to users' accounts. That's just the way it is. It's true of any ISP, it's true of Google, it's true of Microsoft, it's true of every company on the planet that operates in the Internet space.

There are rules around that access. Sometimes those rules are violated, and we've had policies in place around who gets access and what those rules are for quite some time. When users violate those rules, they're disciplined or terminated. That's what happens at Facebook

MS. DYSON: So, what did happen?

MR. KELLY: There were a lot of allegations made, a lot of sort of iffy connections to facts. But have there been any incidents of the misuse of internal user data, sure, and have we taken action against those employees, yes.

MS. HARRINGTON: Declan, I have a question for you, and then, Carlos, we'll get to your question. What is your sense of the meaning of the 18-month log retention policy to consumers and account holders? I think you've done some research and writing on that question.

MR. McCULLAGH: Sure. Declan McCullagh. We've done a series of privacy-related surveys, three or four of them, for news.com, which is part of CNET -- and by way of disclosure, I should say that my spouse works for Google, started recently, though I did not discuss my testimony or presentation with her nor do I think she's really all that interested.

(Laughter)

MR. McCULLAGH: But we did two surveys -- and I'm on the morning panel tomorrow and I can go into some detail there -- and we found out that in terms of data retention, Ask Eraser, when that becomes available I guess in December, will keep data for just hours, AOL 13 months, Google 18 months, Microsoft 18 months, and Yahoo! 13 months, and there's differences in deletion versus anonymization.

In terms of what that means to users, that's probably more important than the cookie data retention issue or the cookie expiration issue because the cookie is constantly reset. But when we did those surveys, our readers seemed more interested in how long the data was retained and what data was retained than actual behavioral targeting and opting out of behavioral targeting.

At the time we did the second survey in August, behavioral targeting wasn't as important an issue based on reader feedback and comments as the length of data retention. I'm not sure if that answers your question.

MR. HARRINGTON: Okay, thank you. And, Carlos, before I get to your question, I just have one more question, Reijo, for you. How would this discussion look different if we were having it in your country? How

would it be different if we were having it? What would the discussion be? On harms from, if any, from collection of Internet user information and the service of advertising based on the collection of the information that's collected?

MR. AARNIO: Well, thank you. I'm Reijo Aarnio. I'm the Finnish Data Protection Ombudsman for my eleventh year now. As you know, we have a lot of directives in Europe, not direct marketing directives anyway. So, the question is if this is about personal data or not. And our approach is that if it's not personal data, for instance, this data collected by using cookies, then how can we call this data, and according to the Electronic Communication Directive, it's called traffic data.

So, traffic data is one part of confidentiality of communication. And, now, we have to consider whether this use of cookies violates the confidentiality of communication or how is it according to the Data Protection Directive.

So, this system means that -- well, sorry. First of all, we define data protection as a cluster of rights, right to know, right to make a decision, of use your self-determination, right to object, and so on. And the basic system is such that if some data processing

violates some other rights, for instance, consumer protection rights, then this kind of data processing cannot be acceptable according to the data protection rules.

So, this would be a much more simple discussion in Europe in some sense. Sorry to say this.

(Laughter)

MR. AARNIO: Then there's one aspect and that aspect is that when we speak about direct marketing and profiling and so on, at least in some countries, we divide the situations into two groups. The other one is how can you process the data of your customers, and the other concept is how are you allowed to process data of known customers? And these are completely two different situations since the purpose limitation is different concerning your customers or known customers.

Well, we have to ask why do we have these directives, and my answer would be that we need to have some kind of regulation of how to solve this legal dispute if the consumer says that, no, I do not want my data to be collected too much, and the data controller says that, yes, we need to have your data. So, we need to have rules for solving that kind of legal dispute.

Why we have this system I suppose is therefore that now that we're living in an information society or we are

heading to a ubiquitous computing society and so on, we need to have some tools how to create trust between business and consumers, or data controllers and data subjects, and we are working on this very hard.

If I may, I'll go back to this definition of personal data. This is absolutely no easy task since it took only 12 years of Article 29 working party to make this definition which was adopted last June 2007.

MS. HARRINGTON: Thank you. Carlos, you've been waiting patiently with a question.

MR. JENSEN: Carlos Jensen, Oregon State University. I wanted to pose a question to the panel. I'm not entirely sure who to pose the question to, but I'll let you guys fight over who gets to dodge the question.

Our current model for communicating with the user and getting consent is through the privacy policy, and we know no one reads privacy policies except Larry's mom. But assuming for a moment that people did read privacy policies, how valid is this form of a contract or this form of a disclosure given that, when we're talking about behavioral tracking, we're talking about prolonged periods of time that users have followed? Attention spans are increasingly short. How do you remember what you agreed to? How can you become aware of how much

information has accumulated about you when you give consent or don't give consent?

MS. HARRINGTON: Who wants to -- Pam?

MS. DIXON: I heard a couple different questions in there, so I'm going to kind of pick it apart a little bit.

So, I heard a question about access. How do we know what someone has? But I'll get to that later. I think that the FTC has profoundly made a case for how important privacy policies are. I think they're an extremely important contract, and I promote the use of privacy policies, and I support them strongly. Period.

And then I would like to refer you to a company called Ominet, which is an advertising company, and each time that they present an ad to a consumer, that ad contains "powered by Ominet" on the face of that ad, and the user can then click on that ad and be taken directly to an opt-out. Ominet has a detailed privacy policy, but they also are presenting ads which, on their face, have a direct link to an op-out. I think this is a very intriguing possibility and I think it does constitute additional notice that's appropriate, and since it's contextual, I think it's helpful for consumers. So, that's one thing.

You mentioned access. I think it's really an

important question and one we need to get at here, which is if I go to, for example, a large company or a midsize company or a small company, how may I have access to the profiles that the company holds on me? For example, we've learned that Axiom is starting to do behavioral targeting. Do I have access to the particular consumer segment I've been placed in? Am I a second city person or am I digital urban elite? Do we have access to that kind of data? I think we need to.

Thank you.

DR. PONEMON: Can I chime in since you spoke about my mother by the way?

(Laughter)

DR. PONEMON: Oh, after this meeting, them there are fighting words. But, look, there are lots of concepts floating around here and, unfortunately, I don't think we've nailed one. I think the issue is -- it goes back to the concept of how smart is the public? Is the public just completely unaware of these issues until there's a problem, in which case maybe then you would read a policy or an end user license agreement. But until something happens to you, most people aren't going to spend the time doing that.

So, I think, although Pam makes a good point, the lack of a policy is a bad thing and I think policies

are commitments, probably more important for the organization so that they can rally behind it and create procedures and all of the good stuff, but at the end of the day from the consumer's point of view, there is no empirical evidence whatsoever that a policy makes a difference, that people will not use something because the policy isn't good enough. That policy may become salient to an individual when there's a problem and then they may have legal issue.

I think another comment that's related to Carlos, the question you asked, is about ownership. Remember I told you about the privacy age gap study. We asked the question, who owns your data, and we found that most people believed that they own their data, but younger people basically believe or are more likely to believe -- the majority say that they own the data. So, it's a statistically significant lower percentage. So, younger people are starting to understand that maybe they don't own it.

But then we asked the question, how would this influence your judgment, and we found that it really didn't have an effect on their judgment. Whether a company or you owned the data, they would still do things like download their favorite tool. The tool that we were looking at, to pick on Google, was Google Desktop.

Everyone loves it. It's a great product. But we basically asked the question specifically around specific free software products.

So, again, what does it mean? It means that, yeah, policies are nice. No one reads them. There must be another way to communicate and educate the public other than a policy, and I'm not sure we've looked at all of those different issues. I also think that we need to have probably more accountability for the consumer as well. Consumers need to take responsibility, too. It's not that we're all so dumb and so lame that we can't take responsibility to say no to something that is dangerous. So, we need to step in and take more responsibility as well. Anyway, that's my other spiel. Thanks, Carlos.

MS. WONG: So, maybe I'll just step in from a company perspective because we struggle with this a lot, and I'm glad you raised it. Being a lawyer and trying to draft a privacy policy that doesn't sound like it came from a lawyer is an exercise in creative writing I have not had since I was in grad school. And, so, we try to figure out, well, how are we going to reach these users who, I think Larry's absolutely right, aren't really interested in reading a long, single-spaced 9-page or, in some cases, I think some people have said 14-page privacy policy?

So, we're experimenting. We experimented with the layered notice format, which is what we currently have up on our site, and we started to do some really innovative things like creating user-generated -- or having contests of our user-generated videos. There's one currently that's being hosted by Berkman and that we co-sponsor for, tell us what a cookie does, and some of them are really great. There's one with a guy who like runs from room to room and puts a post-it on himself every time he hits another room.

(Laughter)

MS. WONG: We also have our own videos that come from Google, and as I was describing during my presentation one that sort of in depth describes what is a log file and how do we use it. We have some more queued up that we're going to do. We just started a Google privacy channel on YouTube which, again, is intended to sort of try and educate, but in a different way than a long legalistic privacy policy.

This is our challenge, right? Because -- and let me go back to the thing that I said in my presentation. If we don't get this right, if users don't trust us because we haven't been transparent with them, we haven't at least educated them about what is happening with their data, then we'll lose the users. They'll go

to somebody else.

MR. KELLY: I actually want to take on a little bit of personal risk here and suggest maybe that we have Larry's mom do ratings and go from there.

(Laughter)

MS. FUZLULLAH: I'd love to talk a little bit about notice as well if we have time.

MS. HARRINGTON: Okay, if you can keep it short. And then let me tell you where we're going next and what's going to happen with the remaining 40 minutes that we have.

Scott has a question. I want to ask the panel about something that we read about in the Wall Street Journal just a couple weeks ago, and that is online data combined with offline data to enhance consumer segmentation. I want to hear some discussion on that.

And then I'm going to give you a sneak preview of the last question, and the answers need to be very succinct and every panelist needs to provide one, and the question will be -- and let me just tell you, what we're most concerned about at the FTC is harm. So, we will end with each panelist answering these questions. What is the most serious harm, if any, that you see arising from behavioral advertising? And what action should be taken and by whom to address this harm? Everybody, that's your

homework question, and no one skips.

Okay, Scott?

MR. KLELAND: Scott Kleland from Precursor, and thank you, Larry, for mentioning the word "accountability." I think it was the first time I heard that word, and to piggyback what Esther -- I think that was the concept behind her question. So, let me piggyback the accountability issue.

And if I could ask the large companies, given that the online advertising business is not a direct business where you are getting paid for by the consumer, the question is simple. In what ways are firms accountable in online advertising and to whom?

MS. HARRINGTON: In what ways are firms accountable and to whom?

MF. KLELAND: And to whom.

MR. KELLY: I mean, I'll jump in and say you're accountable to the customer experience. One of the things that I think that innovative companies in advertising are trying to do is be less interruptive and more sort of immersive, allow commercial messages to be part of the experience instead of basically slamming a piece of interruptive media in front of people. I think that if you do that too much, you risk turning the customer away.

So, companies are ultimately accountable to -- particularly companies that are serving online advertising, if their traffic goes down, they can serve less advertising and the market makes them accountable.

MS. HARRINGTON: Does anyone have a different answer than that? The response here is we're accountable to the marketplace really, I think.

MR. KELLY: Well, but the customers drive the marketplace.

MS. HARRINGTON: Right, right.

MR. KELLY: So, you're ultimately -- or if your privacy policies are inadequate and your customers think that, they run away from you.

MS. McDADE: I think we're accountable in the sense of the experience that the customer has on our site. We have a very strong creative acceptance policy and we look really carefully to make sure that ads aren't misleading, that ads aren't themselves collecting PII or involved in nefarious activities. So, I think part of the accountability is that the users feel safe in your site and that the experience they're having with your advertising is one that they're comfortable with or they will not -- we all learned about pop-ups and other kinds of advertising. It was unacceptable to consumers.

So, I think, in fact, research will show that

consumers are in the driver's seat around the types of ads that they prefer.

MS. HARRINGTON: Okay, I want to --

MS. FUZLULLAH: Can I add something? I'm a little bit confused actually because I thought the question that was posed was actually asking since consumers aren't the ones driving your revenue really -- I mean, if you're selling advertising, it's the advertisers that are your customers, right?

So then who are these users? How are they going to be protected by the marketplace?

MS. WONG: But I think the advertisers will go to sites which have a lot of customers and, so, the primary relationship is with that customer. As a company, you're attractive because your customers are willing to come to you.

MS. FUZLULLAH: So, kind of like an indirect A plus B.

MR. NELSON: Well, there's really a three-legged stool there that we haven't talked much about that quality content drives quality users drives quality advertisers. It sounds too simple, but it's something we have a tendency to forget. Most of the people you're talking about that advertise, they're putting their reputation out there on the line in that banner ad or in

that text link saying, I want to develop a relationship with you, Mr. Consumer and Mrs. Consumer, and if they fail doing that effectively, it's detrimental to their business. And that's their interest primarily.

MS. HARRINGTON: Okay, one last audience question for right now. Can you introduce yourself?

MR. MENDEZ: Yeah, it's A.B. Mendez again with FBR Capital. One thing that this calls to mind for me is, I think it's certainly true that consumers and users appreciate more information, even if they won't use it. For example, I noticed a layered privacy statement on a Microsoft page recently, and although I didn't go and click through to the second layer, I appreciated that it was a one-pager format, that if I were concerned at that moment I could take the time, and I had confidence that it would be something I could understand. So, I appreciated that.

I think people do appreciate consistency in where you place a privacy statement, having a privacy statement placed in a place easy to find and then in an easier-to-read format. I find it very difficult to get the information from public companies. If they're working with a third party BT provider and what exactly they're doing, I think most consumers would like -- you know, there's your privacy statement.

Here's the third party behavioral targeting firm that we work with. Here's the kinds of data they may be collecting, we may be collecting about you, and here's the places in our site that we're doing that. If you'd like to get more information, you can go to this, that and the other resource. But there's not much transparency. It seems to be sort of a playing dumb and just any reaction. And could there not be more of a standardization, a voluntary standardization among Google, Yahoo!, and other large Internet media companies?

MS. McDADE: I'd really like to pick up on that. We have a project at Microsoft we call Trust UX. It's sort of in its infancy, but it's something we're passionate about, which is to help develop more standards about the type of notice and the type of information according to the need for the customer to have that information at the time when they're making a decision.

In this book I held up, which is available on the web, we outlined some of the different categories of consent. One we call just in time. So, you're presented with the information at the time you're about to make a decision whether to make a download or to send information back to Microsoft.

Another would be in your first run experience. Information that you absolutely need to know before you

install something. This gets out of the web world in some ways, but I think it's relevant potentially to this area, as you brought up. I think the industry doesn't have yet a good taxonomy and vocabulary for the types of things that we're describing. We have a tough time ourselves following it.

And I think that one of the things we need to have is more industry collaboration around what different definitions mean, what the taxonomy is, and how we should maybe have mutual best practices around conveying that information to the customers in more uniform ways. That's why we did the layered format in the first place.

I just want to pick up on that for a second because notice is something --

MS. HARRINGTON: Okay, I want to jump in here. We have a whole session on notice tomorrow, so I'd really like to move us off of that. This session is about the collection of information and its use. And we really want to focus on identifiable harm. Harm, harm, harm. That's what we care about here at the FTC. Harm that's actually occurring or harm that you think is going to occur in some application or some strategy that is about to be rolled out or that you think is likely to occur in the future. So, let’s refocus on that.

I have one --

MS. McGILBRA: Eileen, I'd like to just ask a question, actually, of the other panelists. Coming from Europe now, working in Europe, understanding some of the regulatory issues we have in Europe and how it shapes business in Europe, many American companies, like Microsoft and Google, are doing lots of business in Europe.

What are you doing to sort of address some of the differences in the regulatory structure of the EU versus the U.S. in terms of how you use data, how you collect it, and how you store it for later use?

MS. HARRINGTON: We also have a session tomorrow on that subject. Okay? So, I really want to keep us focused on information collection and use in the United States market right now because we're going to do the international focus tomorrow, and that will be the key question. So, you're very prescient.

Now, I would like to ask about online data combined with offline data. We read in the Wall Street Journal on October 17th about a new Axiom collaboration with Microsoft and Yahoo!. When a consumer who makes a purchase or registers with a site or fills out a survey and provides an address is then checked against an address that's maintained by an Axiom database, that's an example of this kind of online/offline.

I guess a question that I have is whether any of our discussants know that you are using those kinds of combinations or aggregations of online/offline data. Anybody? Anybody want to volunteer that they're doing that, or does anyone want to say that they know anything about it? Diane?

MS. McDADE: Okay, I'm not aware of what you just referred to and I apologize for that more recent development. I'll research that. But, in general, our privacy statement does permit us to purchase publicly available information that we might append then to a segment.

So, we might take --

MS. HARRINGTON: So why do you do that?

MS. McDADE: So that we might know that a zip code has a particular educational level, a typical income level, so that we can tell advertisers they might be able to reach folks in that zip code. It's just more information for the advertiser.

MS. HARRINGTON: And further segmentation of your --

MS. McDADE: Right.

MS. HARRINGTON: Okay. So, you're doing that to enhance segmentation for advertisers.

MS. McDADE: Correct.

MS. HARRIS: Does that mean you're doing it on an individual basis or you're -- I'm a little confused by what you're bringing together offline with the online data. I mean, are you bringing my offline data together or are you --

MS. McDADE: I believe that what we purchase is like zip code level data so we would know that -- a customer will often give us their zip code, that's part of our registration process, then we would match up that zip code with other publicly available information. People are looking for segments, they're not looking for individuals. Individuals aren't that interesting to advertisers.

MS. HARRIS: Okay. But they are becoming increasingly important to advertisers. I mean, that's really what this behavioral targeting is all about. I find it hard to believe -- it's sounding as if companies don't keep information for very long and really aren't interested in it. That is not what I've been reading in the trade publications about how behavioral marketing works. It really is about this 360 degrees. It's across platforms, retaining information over periods of time. And I would challenge anybody to say that that's not where it's going.

MS. DIXON: My understanding was that the

segmentation was household level even when it is by zip code.

MS. HARRINGTON: Do you have a source on that?

MS. DIXON: Yeah, that would be Axiom and Claritas.

MS. HARRINGTON: Is that where they are moving from -- I think some of them are getting into the advertising business and moving from offline to online. Do you know about that? Are you involved in that? Any of our panelists, anything on that?

MR. NELSON: We are involved in that, but there seems to be some confusion around offline and online. It's digitized data. If I give you my phone number in the store, it goes into a database. Just because I typed it into a browser, it ends up in the same database. And marketers are using digitized data to behaviorally target and to better buy media, to better respond to customer requests.

So, we get this online/offline thing going. Folks, it’s just all digital data whether you gather it for a browser or from mailing in a postcard is irrelevant.

MS. HARRINGTON: But that data is being collected perhaps offline and then combined to serve ads online.

MR. NELSON: But I think the issue is anonymous data I didn't expect you to associate with personally identifiable data. That's the harm, the rub. If I gave you my name and address through a browser or I gave you my name and address through a visit to your retail outlet, I'm fine with that. I chose to do that. But when I find out you're tracking me on another website anonymously and then associating that to the fact that I gave you my name and address in the store, I've got a problem with that as a consumer.

MS. HARRINGTON: And that's happening?

MR. NELSON: No, I don't know that. Could it happen? Yes -- technologically, you bet. I have no personal experience. Our company doesn't know of anybody doing that.

MS. HARRINGTON: Lisa first and then Kathryn.

MS. CAMPBELL: There's a really worthwhile TV show called L'Afacture (phonetic) that tracked 200 companies in the province of Quebec and Canada that their only industry is to trade in personal data. They cater mostly to lawyers and creditors, but all they do is search information on the net and offline that can be matched to provide a rich profile of individuals.

MS. HARRINGTON: Kathryn?

MS. MONTGOMERY: Well, I'd just like to make

one comment. It seems to me that a lot of the way this has been characterized is that consumers go online to shop. I mean, that's sort of what it sounds like. In fact, consumers and users go online to do a lot of other things -- to find information, to do research, as we were talking about earlier, sometimes to research very sensitive, difficult kinds of personal issues. I haven't heard any assurances that that kind of information is not part of the mix.

So, we were talking earlier about this idea of looking up a disease or a symptom or any other thing I might decide to look up online, and that information being used for advertising purposes when, in fact, that's not really what I might expect to happen as a user online.

I guess the second part of my point and perhaps my question is, how much do consumers really know about how all of this works, and I suspect they don't know very much. I suspect that really they're fairly clueless about what works behind the scenes.

MS. HARRINGTON: And tomorrow we're going to be talking about what consumers know and how they might find out or not. But today, again, we're focused on what is it that's actually happening or that we think is going to happen and what are the harms that are associated with

that.

MS. McGILBRA: Eileen, I'd like to just share an experience I had literally just yesterday and see if anyone on the panel wants to kind of -- they may not actually once I tell it. So I went on to a website, X website, and I just perused to look up some information. I closed the browser, I was done, and I went about my day.

A couple of hours later I got an email -- excuse me, a text message, SMS message on my mobile phone saying, we know you're interested in this product, here is an opportunity to do this. And I said, now how on earth did they find me within two hours of going onto this website? Anyone want to reply to that?

I did nothing. I didn't provide any information other than go on the website and peruse.

MS. CAMPBELL: It's called mobile convergence and I think Google and many other companies are interested in buying VOIP and other voiceover Internet service providers that can do just that -- target people beyond browsers. So, it's not just your browser. Your browser would be one of many aspects through which you'll be targeted.

MR. McCULLAGH: Well, let me try to answer that. I mean, we know and there are plenty of published

Internet standards that go back to the mid-1990s, what information your browser presents when you go to a website. It does not give your email address, it does not give your phone number. It gives things like your IP address, your operating system, your browser type, Firefox versus IE, your browser version, and really not much beyond that. The website can set a cookie, but that doesn't really help it very much if this is the first time you were there.

So, based on what you said -- and our current understanding of Internet protocols, that doesn't seem to make much sense. So, then there has to be another explanation like you -- it was a chance coincidence, random spam, or maybe there was another website involved that was brought in via Javascript.

But the most simple explanation is that Interest standards don't allow what you described.

MS. HARRINGTON: Richard, do you have a thought on that?

MR. SMITH: I'm really confused. If you go to the Washington Post and you look at a cookie, it's got your e-mail address in there. You don't put anything in there.

MR. McCULLAGH: But that's because you typed it in at some point. If you go there for the first time

ever it doesn't know that, obviously. Come on, Richard.

MR. SMITH: Yeah, but there could be another site involved. I don't know the specifics of this, but to present this black and white picture without understanding some of the details, I just can't say. I can't make a judgment on this. It's an interesting situation. But to say Internet protocols don't have e-mail addresses or phone numbers is simply not true.

MS. HARRINGTON: Okay, Reijo, you had something you wanted to say. Esther, we'll take a question from you, and then we're to move to our homework.

MR. AARNIO: Yes, thanks. About this segmentation, as we know there is major databases for data mining and data roughing and for that kind of purposes, and these results of this data mining might be an application for an automated decision making system, and this has an impact on our lives.

We've got loan offers made by automated systems or these applications can be found on health care sector, insurance sector, and so on. Therefore, we have a special prohibition about these automated systems in the European Data Protection Directive.

MS. WONG: Before we move to Esther's question because Google was referenced, I think Lisa mentioned it. I'm assuming this was not Google because as far as I know

we have nothing even remotely close to something like that.

MS. FUZLULLAH: Didn't Google just buy a company called Jaiku that does voiceover Internet providing?

MS. WONG: Right, but we are not doing what was described earlier, which is to contact the user because they surfed on a website, which, again, I'm not clear that that could happen, but certainly unless a user gave permission, my company is not doing that.

MS. CAMPBELL: Would you agree, though, Nicole, that there are companies that are going to offer free over the Internet phone services that will search key words in an aggregate form and then provide advertising based on that?

MS. WONG: I've heard of them, yes.

MS. CAMPBELL: Thanks.

MS. HARRINGTON: Esther?

MS. DYSON: I just want to follow up on that question of how that might have happened. I would make the assumption that there was some kind of third party cookie there that was connected to somebody who did, in fact, know your information.

So, was it a completely random site or was it one related to somebody you often visit or something like

that?

MS. McGILBRA: I was the researching one on companies here today.

(Laughter)

MS. DYSON: Okay, so, let's have some transparency. Who was it?

MS. McGILBRA: I'm not going to mention names.

MS. DYSON: Well, I'm not in charge here, but I'd like to know.

MS. HARRINGTON: I think it's safe to say that we would like to know more than we know, generally. One of our hopes here -- one of our goals has been to learn more very specifically about exactly what information is being collected and how it's being used in the behavioral advertising context. And I think I can say that we still have more to learn, and we're going to have to keep figuring out ways to find out.

But I want to move on to the homework question, and then if we have any extra time, we'll think of some creative use for it, but I don't think we will.

So, Declan, we're going to begin on your end and we're going to go back and forth, back and forth, back and forth with answers to the questions, what is the most serious harm, if any, that you see arising from behavioral advertising, and what action, if you see a

harm, should be taken and by whom to address that harm?

MR. McCULLAGH: Well, let me answer it this way. What I've seen on this panel are hypothetical concerns, very broad, we need something, something-must-be-done-here concerns versus sort of the reality of what's happening now with we keep this for 18 months because of Sarbanes-Oxley. And both sides have a point. It's sort of the nos feratu (phonetic) problem.

Imagine a hypothetical search engine, nosferatu.com, that tracks everything, sells everything to marketers, has no privacy policy, or worse yet, has a privacy policy and then routinely, willfully violates it. I mean, this is a real serious privacy problem. The same thing if it's nosferatubook.com and it's a social network.

But, I mean, there are common law claims, class action claims, state law claims, the Federal Trade Commission would be involved. And, so, we don't necessarily need new laws, unless I'm missing something, to put nosferatu.com out of business.

And then one last thought, in 2004, I remember writing an article about of the Commission representatives testifying before Congress saying we already don't necessarily need new spyware legislation because we already have the power to basically put

evildoers out of business. I think the Commission probably has the power to put nosferatu.com out of business under its existing statutory authority.

MS. HARRINGTON: Okay. Larry?

DR. PONEMON: Okay, the other side, so we bounce back and forth. Good, thank you. I wasn't prepared. So, now I'll be prepared.

MS. HARRINGTON: The most serious harm, if any.

DR. PONEMON: I think we worry about behavioral targeting and all the information that organizations collect and these organizations doing sinister things, and I don't think that's a real threat. I think the bigger threat -- or two, one is the issue that all of this information is not secure and somehow that information gets into the hands of truly an evil party. It could be a government or whatever, and that's probably a little bit of a science fiction movie.

(Laughter)

DR. PONEMON: It never will happen. But that that concern, any time you collect data, you have a responsibility to keep it secure. And relating to that, I know Richard probably has something to say about this as well. Sometimes even with the best of intentions we invent new products and services that have flaws in them. So, for example, we did some research on Desktop Search,

which is a great product, but, of course, there were vulnerabilities, man in the middle issues and also cross scripting vulnerabilities. Even though the reason for the technology is behavioral targeting, there are people who will use it as an excuse to do bad things to the consumer. That needs to be factored into the equation as well.

I think, also, the other harm we haven't thought about here is by restricting invention on the Internet. I think there are things that are going to happen because there's a marketplace, and these opportunities, we don't want to curtail them. We want to actually make sure that we're not creating rules that prevent future innovation and great prosperity. That's a harm. In that situation, who would be harmed? It could be the venture capitalists, it could be the shareholders of companies, it could be the companies themselves.

So, I know we don't think of these people as legitimate parties because we're here at the FTC and the focus should be the consumer, but all of these folks, I think, could be harmed in different ways if we start to create restrictions and new laws that make it a lot more difficult to do good things.

MS. HARRINGTON: On the data security issue, should anyone act?

DR. PONEMON: I think on the data security issue, I think it goes back to the first -- when you have a vulnerability, you have a responsibility to fix it because there's no guarantee that you can invent a product without some flaw. The bad guys, the people that are probably somewhere in Central Europe or wherever, they're continuing to get smarter and better and they'll find those vulnerabilities. Quite frankly, they're going to look to Google or they're going to look at Microsoft. They're going to look at the biggest companies because that's their largest penetration. That's just the way they operate.

So, you know that you can't stop it, but you should be responsive to it. I think Google did a good job in responding quickly, but I think that there needs to be a pattern of response to these kinds of vulnerabilities.

Also, relating to that, I still think a lot of these organizations could do a better job building in privacy and security into these products. I'm not sure that your developers are thinking privacy and security when they're developing. They're thinking about very, very short-term goals, and I understand that's the way it works and they're really good at that. But I think companies that are inventing these technologies need to

spend more time up front trying to design for privacy, trying to design for security.

MS. HARRINGTON: Okay. Now, the grades on the homework assignment are going to go down the more words you use during the assignment.

DR. PONEMON: I now have an F.

(Laughter)

MS. HARRINGTON: You guys get Ds, the first two.

DR. PONEMON: Thank you very much.

MS. HARRINGTON: Nice ideas, need to be succinct. So, Kathryn, the bar is raised now or you're going to raise the bar for everyone. You'll do an A job, I know.

MS. MONTGOMERY: A D is still a passing grade.

(Laughter)

MS. MONTGOMERY: I mean, I think that there are a number of harms that I see now and in the future. We've touched on a few of them, but I think there are vulnerable segments of the audience, of consumers, rather, and certain areas of marketing where there can be abuses. Right now, we really have no way of stopping those. I mean, as I said, we have the good companies here talking about their good practices, and I appreciate their coming here.

But if you look at areas of health, if you look at drugs, if you look at the sub-prime market, a lot of categories where there can be abuses against vulnerable consumers where behavioral targeting can pull together a lot of information about these individuals and use it in ways that are really unfair and could perhaps even be deceptive. That's, I think, an obvious area where there would be harms.

We've also documented, in another report we did on interactive food marketing, what some of those harms can be around the issues of childhood obesity, for example, and the behavioral targeting that goes on there and in-game advertising for snack foods and pizza, et cetera, that are targeted at people who are vulnerable there.

I do think there is a role for the FTC. I think this is a very good first step. I would like to see the agency investigate these things more independently, in addition to hearing what the industry is here to report about what they do. I think we absolutely need some standardization in terms of how things are done. I mean, I've heard a hodgepodge of different approaches that all of these companies are talking about, and from the consumer point of view, that's extremely confusing.

So, I think we need some standardization and some clarity and more transparency.

MS. HARRINGTON: Okay, thank you. Leslie, looking for a C, still looking for a C.

MS. HARRIS: I'm looking for a C.

(Laughter)

MS. HARRIS: I think that the loss of control on a computer and personal information, we're moving towards the potential of rich personal profiles that are identifiable in and of themselves or easily re-identified with offline information that can be used for almost any purpose. And I think that that's the big harm there.

For me, personally, advertising is not the outer ledge of the bad things that you can use this information for, and I think we have to sort of think beyond. At the end of the day this is about consumers being empowered about choice, which is going to require more knowledge, it's going to require more transparency, and a lot easier ways to make their decisions to opt out of these systems.

MS. HARRINGTON: Good, there's a solid C, maybe into the B range.

MS. HARRIS: If that's not a B.

(Laughter)

MS. HARRINGTON: Well, we'll debate that. Pam,

the bar has been raised.

MS. DIXON: You didn't get to the who, did you?

MS. HARRIS: The who what?

MS. HARRINGTON: Who? Oh, the who on your harms. Is there anyone who should act? The harm is very rich.

MS. HARRIS: Well, I think, again --

MS. HARRINGTON: Extra credit here for Leslie.

MS. HARRIS: I think there are some things that the FTC ought to be thinking about, and obviously with others, including Pam, we've proposed the possibility of a do not tracking system to make it easier for consumers to opt out. Got to come up with a way if you want consumers to be empowered that they actually know who it is who's serving what to you. So, that's a matter of transparency, but also a matter -- I was very intrigued, I can't remember, maybe it was Pam that was talking about advertising with tracking that you went right into to be able to get out of. I think there's a number of things which is a combination of best practices.

I don't think the FTC on its own motion can do a do not track system. But we've got to come up with some ways. A consumer cannot go to 20 or 30 or 50 sites, not all of these companies belong to any one association or one method, and we've got to figure out a better way.

MS. HARRINGTON: We're going to end on time, so some people might get incompletes if the class can't pick it up.

MS. DIXON: All right, I'm a geek, so maybe I can pick it up. So, the harm --

MS. HARRINGTON: The most serious harm.

MS. DIXON: Okay, we'll stick with that. Indirectly or directly associate information which is then used to segment consumers and present them opportunities that may or may not be accurate and may present differing opportunities to people based on the different segmentation and, therefore, create different categories of consumer which can impact life decisions.

A real example, because I like facts, a consumer who browses for a car ends up with a loan offer or offer of credit that's different from the same consumer next door to them that has a different browsing profile.

Another example, a person who goes to a website and fills out a quote, unquote, "real age survey" with their name, and they have that self-identified medical condition sold to a marketing list which is picked up by an insurance company and then later they don't understand why they're denied insurance.

Whom? The World Privacy Forum is publishing a

report tomorrow. It's an analysis of the history and current operations of the NAI. It's very focused strictly on the NAI. And it includes the failures of the NAI. So, we've had self-regulation for seven years, and I think we've seen where it's failed. I think that what I'd like to see is I'd like to see this debate move to the FTC, and I'd really like to see some simple solutions for consumers.

I don't know how consumers can survive in an environment where they don't know where to opt out, they don’t even know what an opt-out cookie is, they don't know what the NAI is. I think we can do better, and I'd really like to see it moved to the FTC.

MS. HARRINGTON: Thank you. Richard?

MR. SMITH: Well, for me it gets down to a fairness issue. I think a lot of data collection that goes on is being done under the table and companies are doing it on the sly. I've always just felt it's not nice to snoop. I don't know if that's a harm or not, but that’s where I come at, it's sort of an ethical thing.

As far as what to be done about it, I've always felt that it’s sort of an accident that a lot of this has happened because of the design of cookies. So, I would really like to go back and revisit in browsers. I see a technical solution, but I think this is something the FTC

can drive on, more of an opt-in model for cookies, particularly in the third party area. Thanks.

MS. HARRINGTON: Well, that's a B plus. Thank you. Reijo?

MR. AARNIO: Thanks. My classical answer would be that this would violate our self-determination, our dignity, our right of equality and it might create discrimination between citizens and consumers. How would this happen is that if this profile created by this kind of a cookies and so on, if this profile starts to live its own life, we cannot control it anymore, and this has direct impact on the quality of our life, on our social life, our economical life and our well-being in general.

At the moment according to the Euro barometer survey, 50 percent of European citizens are afraid of electronic services and trade on Internet. So, this is not a good starting point for business, and if this behavior -- advertising creates this kind of feeling not to trust on business, of course, this might cause serious harm also to the business.

Since these legal obligations are there for data controllers, they have to follow these orders, but as civic societies we need to have the service organizations for data subjects, that means DPAs and this

is the reason why we exist. Thank you.

MS. HARRINGTON: Thank you. Chanterria?

MS. McGILBRA: All right, this will be very quick. Harm. The harm is not the collection of data, the harm is the data getting in the wrong hands. We know that Microsoft, we know that Google, we know that Facebook, we know that all of the companies up here do an excellent job of protecting their data, or they try the best within the confines of the industry, but it is preventing that data getting in the wrong hands that all consumers are afraid of.

The gentleman mentioned there's 50 percent rate of adaptation of the Internet usage in Europe. That is the primary reason why. It's not surprising that most of the companies in Europe -- excuse me, most of the online business in Europe is driven by the U.S. There is a direct connection. Think about that.

Next, who is to be accountable? I think that organizations like the NAI, CDD, all of these organizations, we need to start looking at global collaboration. How do we ensure that businesses globally are adhering to these rules? We had someone say maybe some guy out of central Europe is hacking into computers. Well, how do we address that if we're the companies they're hacking into here in the U.S.?

And that's through global collaboration. So, I think we're all responsible for finding solutions to that in a reasonable way.

MS. HARRINGTON: Thank you. Chris?

MR. KELLY: So, the number one cognizable harm sort of that could be addressed from a regulatory level is lack of security, and particularly around sensitive data, and that obviously would harm an individual who had their information that they had provided improperly accessed by a health insurer or by a government or a whole bunch of different options along that front.

But I also want to recognize that the lack of control that consumers feel around a lot of this information is a harm as well and could harm the marketplace. So, I think there should be a lot of presentation, that companies should be out there and a number of self-regulatory bodies should be out there working at deriving new ways to give people more control over their personal information.

MS. HARRINGTON: Thank you. Amina?

MS. FUZLULLAH: Ultimately, I'd say it's the lack of consumer control. I feel like I'm reiterating what a lot of other people have said, but at the end of the day, if consumers feel that they don't have control over what they're doing online, it will impact their

choices and affect their prices. That's a huge harm.

I think we recognize that problem in the brick-and-mortar world. I see no reason why we can't recognize it in the online world.

I think that the solutions to that would be increasing transparency and giving consumers straight talk. I mean, just being honest with consumers, what's going to happen with their data, how is it going to be used? I notice something that's really confusing, the Patriot Act managed to put in a policy, a notice on the back of credit card applications to explain how they're going to use that information possibly for their own purposes. And while there was about two sentences of gibberish that no one could understand even with a lawyer, there was literally words that said what this means to you. That's something I don't normally see in the online world.

MS. HARRINGTON: Okay. We're going to have to really shorten these last few. Nicole? Harm. Who should act?

MS. WONG: Yes. Short enough for an A?

(Laughter)

MS. WONG: Very quickly. I think I agree the greatest harms are clearly the inappropriate collection or combination of information about a user or the breach

of the security of that information. And that's I think where the FTC probably needs to take a close look as to whether they have a role.

Having said that, from a business perspective, the greatest harm that we can do is that we don't get it right, we serve the wrong ad, we don't target it well, we do it in a way that offends the user, then the whole enterprise fails. I say that as a company not quite in the space because, as I was showing, we really target based on keywords and content of web pages.

But it strikes me that the companies have the greatest to lose here as they build these infrastructures, and they don't actually get it right.

MS. HARRINGTON: Thank you. Scott?

MR. NELSON: Okay, going for broke here. The most serious harm would be to violate expectations of consumers. Folks, we've been advertising to people for decades. This is a channel. It's nothing new. People have norms. I go to a suit store. I introduce myself, they take my size down. If I go back a week later, I expect them to remember that. We just need to apply what we do offline online.

And by whom? Where's the money? I think everybody on this panel, with the exception of a few, generate revenue from advertisers. I don’t see a credit

card company, an automotive company or a travel company on the panel. They're funding this entire initiative. They need to take responsibility.

MS. HARRINGTON: Okay, Lisa?

MS. CAMPBELL: I'd just like us to remember that it's beyond browser, it's web, phone, TV and other media combined. The harm is the risks of unauthorized or illegal use rises with the greater and greater amounts of information collected.

Canadians are concerned about the deputization of the private sector. Others have mentioned that. So law enforcement and government access, they don't need to go into your home anymore, everything is with the ISP.

They're also concerned about the effect on very young users. Some people have called it the companies and their playground.

In terms of who should act? Companies need to abide by fair information practices, seek consent, be clear and transparent about the uses and disclosure, and give people choices. People have to be responsible to whom they disclose their personal information, when they choose not to disclose it. And, finally, regulators have to be proactive, technologically aware and raise issues and act as soon as they see breaches of law and policy. Thank you.

MS. HARRINGTON: Diane?

MS. McDADE: I think one of the things that we're seeing now is a lot of competition among the different companies to define their policies and to define their privacy innovations, and we've announced some the last week and several others have.

It strikes me that what we want to see, continued healthy competition, that we don't have concentration of data in just a few companies, and I speak knowing that Microsoft has a lot of data, I believe that there should be a healthy ecosystem, and that as we give customers more choices, they will clearly vote with their feet and they will sort it out.

I think we, as an industry, must be better at separating out what are acceptable practices, what are unacceptable practices as it relates to behavioral targeting, particularly in the sensitive areas, to give people the confidence, because I totally understand that many people are still, even in the United States, concerned about Internet transactions because they don't understand that.

So, I think the FTC has a role to play in the healthy competition. I think that the industry has a huge role and has got to step up and articulate some of those standards in a more comprehensive manner.

MS. HARRINGTON: If everyone would just stay right where you are, we've saved the best for last. Where did Jessica go? Is she down there?

MS. RICH: I'm down here. You can't really see me.

MS. HARRINGTON: With closing remarks.

MS. RICH: Okay, I'm Jessica Rich from the FTC and I just want to do a very brief wrap-up today. First, thank you very much for coming here today and for staying. It's amazing how many people are still here at the end of the day. We're very happy with the discussion.

MS. HARRINGTON: Jessica, there's still some doughnuts out there I see, for those who stayed all day.

MS. RICH: Is that what kept people here? And one thing I wanted to add in the list of the staff that Lydia thanked today, we wanted to add Tracy Shapiro who for some reason wasn't there, but she's one of the key players in planning this, and she's terrific, and I think she's listening in.

As we look forward to tomorrow's program, I thought it would be useful to identify some key themes that came out today. I've been listening closely all day, and there's certain themes that I kept hearing over

and over, and actually since this is a town hall, if I miss any, people can shout them out, those that I miss.

But everybody brings different privacy expectations to the table. It came up again and again. There were a wide variety of business models the different companies are using as they engage in behavioral advertising, and there's different levels of information collection. I think we all need to be mindful of that as we think about solutions in this area.

A lot of discussion about how consumers like personalization, but also a real question as to whether they understand what's happening when the personalization occurs and the trade-offs.

Delighted to hear there appears to be increasing amounts of competition on privacy issues. For some of us who have worked in privacy since the early days, there wasn't any competition on privacy then, and there's an enormous amount by all the people here. And, hopefully, it will be a real force in shaping companies' practices.

There was also a lot of talk about the need for greater transparency and, also, during this last panel, data security, data security, date security, which is good because data falling into the wrong hands -- no

matter how good your policies, if your data falls into the wrong hands, there's a problem.

Also a fair amount of agreement that certain sensitive information should be off limits, really sensitive information like health information.

Now, what all of these mean -- it's very easy to say all of these. What all of these mean at an operational level is another thing and, hopefully, we'll resolve all of that tomorrow.

Finally, I just wanted to say as we prepare for tomorrow, we think that in some ways this event has already been a success. We have a lot more to go tomorrow.

First, it's generated so much interesting discussion and, also, in the last few days we've seen an amazing flurry of proposals which is part of why we do this. We've seen the do not call proposal by the Consumer Coalition, we've seen one company say they're going to implement a do not call on a company basis, a variety of companies have talked about reforms they've made, maybe some of them in preparation for this event. CDD and US PIRG have filed a new complaint, and we just heard that Pam Dixon of World Privacy Forum -- actually you're representing a coalition, right -- is going to be issuing something tomorrow.

So, we look with great anticipation, we very much look forward to reviewing those and seeing all the ideas that are generated. And more tomorrow. Thanks very much for coming.

(Applause)

(At 4:54 p.m., the town hall was adjourned.)

C E R T I F I C A T I O N O F R E P O R T E R

MATTER NUMBER: PO75401

CASE TITLE: EHAVIORAL ADVERTISING TOWN HALL

DATE: NOVEMBER 1, 2007

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: NOVEMBER 15, 2007

_____

ROBIN E. BOGGESS

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

_____

ELIZABETH M. FARRELL