FEDERAL TRADE COMMISSION

FEDERAL TRADE COMMISSION	)	Matter No.
ROUNDTABLE SERIES 1 ON:	)	P095416
EXPLORING PRIVACY	)	
----------	)	

MONDAY, DECEMBER 7, 2009

Conference Center
Federal Trade Commission
601 New Jersey Avenue, N.W.
Washington, D.C. 20580

The above-entitled workshop was held, pursuant to notice, at 9:00 a.m.

FEDERAL TRADE COMMISSION

I N D E X

P R O C E E D I N G S

- - - - -

MS. HARRINGTON MCBRIDE: Good morning. Good morning, everyone. If everybody could take their seats, we're going to go ahead and get started. All right. Good morning, everyone. I know that it's going to be a little bit difficult because we are in cramped quarters today.

Thank you all so very much for your patience going through our security line. I know that you all appreciate the importance of security. I will actually make a formal announcement about it in a minute, but please understand that we are delighted that you could be here with us today and that you have withstood the test of the long line.

My name is Katie Harrington-McBride. I'm an attorney in the Western Regional Office and a member of the Privacy's Roundtables team, and I'm very pleased to welcome you here this morning for the first of our three roundtable discussions in the Exploring Privacy Series.

I have some logistics and housekeeping announcements, so the good news is that your fellows that you may have left behind in the line who are still being processed will not be missing anything substantive just now, terribly important, but non substantive.

We have food and beverages coming. We understand that the security line will pose some obstacles to you if you want to pop out for a coffee, so we are arranging to have that stuff delivered, and hopefully before the first break there will be opportunities for you to get snacks and beverages just outside in the hallway.

We also have a list of the other eateries if you're brave enough to want to get yourself outside and get a breath of air. Feel free to do that, and you can pick up that list at the table where you checked in.

The rest rooms are back out through the lobby. You do not need to go through security, but go back through the hallway that you may have been standing in, take a left, and the men's and women's rooms are right there.

When we begin, we're going to have panel discussions. As you can see we have our panelist who will be arrayed here. We would like to involve you in the discussion as much as possible though, but because of the crowd, we're going to need to do this in a rather organized fashion, so we have question cards that are available.

If you have not received one and are interested in getting one, you can raise your hand, and one of our

paralegals will bring you a question card. You can then hold it back up when you've written your question on it. We will collect it. We will bring it to the moderator of the panel, and with a strong tailwind, we'll finish in time so that there are is some Q&A time.

People who are watching on the webcast should feel free to Email to the address Privacyroundtable@FTC.GOV. We'll also be checking that account and bringing those questions to moderators.

For our security announcement: Anyone that goes outside of the FTC without a badge will be required to return through security. You will have to go through the magnetometer and the x-ray machine. If you spot any suspicious activity, please report it to the security staff or to one of the members of the Privacy Roundtable's team.

In the event of a fire or evacuation of the building, please leave in an orderly fashion. We will proceed across the street, across New Jersey Avenue, to the Georgetown Law School, to the right-hand side of that building, and at that time, if we have been evacuated, if you could check in with one of the FTC staff so that we can know that you've arrived safely, we would very much appreciate that.

If there are FTC staff in the room, I hope that

you will be kind enough to give up your seat so that our guests may take your seat, and you may return to your desk and watch on FTC Live, just good manners. These are company manners, folks. This is obviously an extremely well attended event, and we are delighted that you could all be here, so again if FTC staff wouldn't mind volunteering their seats or standing in the room, if you prefer , if you could please do that.

We're also investigating the possibility of overflow seating, and we will let you know at the first break how that's working out, but thank you to those of you who are willing to stand at this point. We're going to do our best to make sure that everybody can be comfortably seated for the duration.

With that, I would like to introduce the Associate Director of the Division of Privacy and Identity Protection, Maneesha Mithal.

(Applause.)

MS. MITHAL: Thanks, Katie, and thanks all of you for coming. It's a pleasure to see so many of you in the audience. It's great to see some familiar faces, and it's also great to see some new faces, and I think regardless of whether you're a repeat player at the FTC or this is your first FTC event, I think we're fortunate enough that we've assembled some of the best and

brightest minds on privacy issues here today.

So we're sure to have a discussion today that's filled with creative thinking, energy and enthusiasm, and speaking of those attributes, I think our first speaker embodies them. He's a creative thinker. He has a lot of energy and enthusiasm, and he's the chairman of the FTC, Chairman John Leibowitz.

Chairman Leibowitz is no stranger to privacy issues. Since he started at the FTC in 2004, he's spoken on a most of privacy issues, including behavioral advertising, spam and spyware, data security, telephone records, pretexting, and I actually remember the first conversation I had with Chairman Leibowitz. We were talking about the privacy implications of public who is databases, and we had a really spirited discussion.

So with that, let me introduce Chairman Jon Leibowitz.

(Applause.)

CHAIRMAN LEIBOWITZ: Thank you so much, Maneesha, for that kind and entirely undeserved introduction, and as I look around the room, I see so many privacy luminaries here and people who have really worked on these issues: Lee Peeler, Marty Abrams, Susan Grant, the eminent and distinguished Marc Rotenberg, Jeff Chester who is around here, Dave Morgan, and so

really I think this is going to be sort of a terrific workshop. We're going to learn an enormous amount, and you're going to help us do that as we try to think through these complex issues.

Now, I recently spoke about, I was on a panel, about Louis Brandeis, one of the intellectual fathers of the Federal Trade Commission of course, who was also a world renowned, turn of the last century reformer, Supreme Court Justice, and in 1890, Brandeis and his partner, Samuel Warren, authored a seminal law review article on privacy, and they wrote, I quote, and I'm quoting: "Numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the housetops or from the housetops," and what they were concerned about then was photography, photography in newspapers and sort of peeping toms.

Now, their work was enormously influential and prophetic in some ways in that it helped to shape American jurisprudence on privacy over the course of the 20th Century, and of course Brandeis' thinking continued when he was on the Supreme Court, particularly I think in Olmstead where he wrote that the right to be let alone was I think the most -- and Jeff Rosen will correct me if I'm wrong, but the right to be let alone

was the most sacrad of rights and the right most valued by civilized men.

The 1960s, as Americans started to lose faith in the government, and in the 1970s with the abuses of government surveillance powers, together with the advent of the computer age, created more ferment around citizen's privacy rights, vis-a-vis government, and the Privacy Act and the Fair Information Practice Principals, the FIPPs -- I like saying that, the FIPPs, you want to say it with me, the FIPPs -- grew out of that environment.

I'd argue that we're at another watershed moment in privacy and that the time is right for the Commission to build on the February behavioral marketing and behavioral targeting principles and to take a broader look at privacy or look at privacy writ large, and let me explain why.

One of my advisors is about to buy a home computer with a quad-core chip running at 2.66 gigahertz. It cost under $2,000. In the early 1990s, a slower Cray supercomputer, a slower Cray supercomputer cost about $10 million.

These advances have created extraordinary benefits for consumers, but also have tremendous implications for privacy. The computer costs of data

collection seems to be approaching zero. Data storage costs are unbelievably low too, the efficiency made possible by Cloud Computing compliments unbelievable advances in chip technology, so companies can store and crunch massive amounts of data relatively cheaply.

Now, these developments have allowed companies to collect and use data about consumers in ways that were never feasible or even conceivable before. Behavioral targeting is one of the many ways that companies can use data to try to tease out which consumer or IP addresses or uniquely identified cookies are more likely to respond to a particular ad.

Those who attended last week's workshop on the future of journalism know that a number of speakers spoke about the importance of revenue from targeting and funding journalism. There are both benefits to companies and to consumers from targeting such as more relevant advertising, but also I think, as we all know, costs in terms of privacy.

Now, those words still reverberate today and maybe more so then when he dissented in Olmstead. These technologies have fundamentally changed the privacy landscape in a way in which Justice Brandeis would have been completely unfamiliar. Consumers have to grapple with this brave new world of information without

analogies in their experience and without a real understanding of the ways in which their information is handled or transferred.

Take Internet advertising, for example. How many consumers, or at least ones outside this room -- I know it's early in the morning, but that was a joke -- have ever heard the names of the many ad networks that end up with their information in the process of targeting ads? How many people understand the network's role and other intermediary's roles in the Internet ecosystem? How many people understand what a cookie is much less how to distinguish a first-party cookie from a third-party cookie?

If brick and mortar retailers tracked consumer's meanderings around the mall the same way a consumer is tracked online, well, to ask the question would be to answer it. It's not just consumers who are grappling with privacy. Companies are grappling with privacy as well.

In the Commission's Sears case, consumers in a sense opted in. They were paid $10 for participating to a stunning degree of tracking of their web usage. The gist of our case was that while the extent of tracking was described in the Eula, that disclosure wasn't sufficient clear or prominent given the extent of the

information tracked, which included online banking statements, drug prescription records, video rental records, library borrowing histories, and the sender, recipient, subject and size for web based Emails, so consumers didn't consent with an adequate understanding of the deal they were making.

Now, nobody argues the folks at Sears are bad people who wanted to do bad things with the information they gleaned from consumers, and I think actually to the contrary, they probably didn't know exactly what they expected to learn from this data, and that just demonstrates, however, that all of us, all of us are still feeling our way around what respecting privacy really means.

Now, people have asked me what to expect to get from this workshop and where we're headed. I can honestly say we don't yet know. Our minds are open. We do feel that the approaches we've tried so far, both the notice and choice approach and later the harm based approach or regime, haven't worked quite as well as we would like, but it could be that this issue is a lot like Churchill's description of democracy, and he said I think: Democracy is the worse form of government, except for all the others that have been tried.

Still, we are going to try to look through the

issue of privacy, and especially online privacy, to try to think it through in a way that is better for consumers, fair to businesses as well.

We all agree that consumers don't read privacy policies or Eulas for that matter, and I think most people now acknowledge that you can focus on traditional PII, such as name and address when particular devices and even consumers are so readily identifiable without it, and of course Commission staff's thoughtful behavioral advertising principles viewed information in this broader, more holistic way.

Well, is there a better way to protect privacy? Is there an easier way? Is there a framework that conforms to consumer's reasonable expectations that businesses can understand and apply? If not a unified theory of privacy, are there steps to narrow the areas of confusion and empower consumers? Should we utilize more opt in, and I've been a supporter of opt in for quite some time.

Should we treat special categories of information such as personal health records or personal financial information differently, and how do we treat vulnerable categories of consumers such as children? We hope that we'll find out over the course of the next six months, and the experts who graciously agreed to

participate in today's discussion will start us off on the course of answering some of these questions.

And I see my distinguished I guess not former colleague but predecessor Mozelle Thompson here, so we're delighted you can be here, former FTC Commissioner Mozelle Thompson.

Let me thank at least a few of the many, many people in the Division of Privacy and Identity Protection who have worked so hard to make today's roundtable possible. Now, I won't list everyone, but let me acknowledge some of the key staff members. Loretta Garrison, if you guys could stand up unless you're already standing up in the back of the room, and then raise your hand. If you can stand up or raise your hand when I call out or mention your name, Loretta Garrison, Peder Magee, Peder? Oh, you're right in front of me, good. Katie Harrington- McBride, who started us off this morning; Katie Ratte, Michelle Rosenthal, Naomi Lekovitz, Jessica Scretch, and Randy Fixman, (phonetics) as well as Assistant Director Chris Olsen, who is around here somewhere back in the corner over there; Associate Director Maneesha Mithal, who introduced me. Maneesha, where are you? Oh, you're in the front next to Jessica Rich. That's great.

Of course, Deputy Director and former DPIP

director Jessica Rich; David Vladeck, who is in the back over there who is the architect of so many things in the Bureau of Consumer Protection, and we're delighted you came over from Georgetown to be part of the Commission, and also Jeffrey Rosen, who is standing over there in the corner and who is helping us think through these issues with a slightly different but incredibly informative perspective, so we're delighted you're part of the group that is digging through privacy, particularly privacy online.

I want to thank you really for assembling such a stellar cast and an accomplished group of thinkers on these issues, and with that, let's get the ball rolling.

You'll be very, very interested -- are we going to reveal the ecosystem charts today, this morning? Oh, that's going to be very exciting, so we have a number of exciting announcements going forward and a number of terrific speakers, and thank you so much.

(Applause.)

MS. MITHAL: Thanks, Chairman Leibowitz. I would now like to call to the podium Mr. Richard Smith who will describe some of the data flow charts that are in your packet, as well as the personal data ecosystem that's on the wall to my right, and while Mr. Smith is coming up, could I also invite all of the people on

panel one to take their seats so we can be ready to go as soon as Mr. Smith finishes his presentation? Thanks.

MR. SMITH: First of all, I want to thank the FTC for the opportunity to speak here today. My role is to sort of set the stage for the workshop and to talk about some of the technologies behind data collection and data use.

As we all realize, the flow of data makes our world work. It's a fundamental part of the economy and just everything that we do every day. A simple economic transaction such as making a cell phone call or buying something online all involve the collection of data and the use of data by multiple vendors. Simply to make a cell phone call might involve five different companies typically that collect data as part of making or completing that phone call.

What I hope to do in the introduction here is to look behind the scenes a little bit at some of the technology that makes all this happen and some of the business relationships that make this happen. The issue of data collection has been around forever. Probably the first time somebody made a stone tablet, we had data collection, but today the issue, as the Chairman said in his introduction, and it was very interesting to hear about this issue starting up with Brandeis, it's

technology driven, that we're seeing a lot more interesting uses of data and a lot more collection of data, an explosion of collection of data due to technology.

And I think many folks in the room can realize this, by thinking back only about 15 years to the first time that they owned a cell phone or used a web browser or had a credit card swiped with the magnetic swipe as opposed to say the embosser machine, so those systems are all indications of the underlying technology that's driving this data collection ecosystem.

One illustration of technology that I wanted to point out here is I have a hard drive. This is actually kind of ancient technology, it was made in 2003, but if you went to your local Best Buys or Staples, you could buy today a one gigabyte hard drive for around $150, and this is anybody could buy this, and these are used in personal computers, particularly in desktop computers, but more importantly in computer servers that hold information about what we're talking about here today, the data that's collected as part of transactions.

What is one terabyte of data that you could buy today? Well, that's equivalent to 300 million sheets of text, printed out text paper. That's one piece of paper for every citizen of the United States that can be held

in one hard drive. Now, we make hundreds of millions of these drives per year, and as the Chairman has pointed out, it is basically now practically free to store data. It actually costs more now to delete the data off these drives than it is to keep it, and the other point is we have to fill all these drives up, and we are as part of this ecosystem, the data collection ecosystem.

The other part of the technology advance that we're all very aware of is communications technology. Really there's two very important places that's happening. One is of course the Internet which allows us to connect all the computers and all these hard drives together to collect data, and we've watched in the last 15 years, from the Internet being something that was in universities, to something that we all use, and we no longer -- we used to connect up to the Internet through modems, and now we do it through cable connections and DSL connections or wireless connections.

That's the other important communications network that we have is the wireless zone network, which allows us now to collect data at really any location.

We're now going to take a look at our chart here. We call it the personal data ecosystem, which is an attempt to look sort of behind the curtain at a very high level of how data is collected in our world, and

the purpose of the chart is to show from the consumer perspective what they see as data collection and then things that are happening also behind the curtain.

One thing that I wanted to say about it is, it's obviously very simple compared to what's happening out in the real world. There's literally tens of thousands of vendors who are part of this data ecosystem and hundreds of millions of consumers, so it has to be more complicated than this diagram, and it's a high level chart, and it doesn't get down to some of the nuances and complexities that actually go on in the real world.

In the ecosystem, we have at the center here the consumer, which is the data supplier, and they provide the information as they go about their daily lives to a variety of what we call data collectors here, and they can be all sorts of organizations. They can be businesses that we interact with everyday. They can be in the area of medical. They can be our doctors or our pharmacies. We get into government collects data and a whole variety of folks who, as part of our daily lives, we provide information to. It can be direct, say through an application for a credit card, or it can be indirect, through say making a cell phone call.

This information then is used to provide services to us. We then move out one level to an area

that a lot of consumers really are not familiar with, to the data broker level where we have folks who collect data from a variety of businesses and government sources, put it together, aggregate it for the purpose of selling it.

This is an area that a lot of consumers are only vaguely aware of, and then we go out to the outer circle to the chart here, and we see all the different -- we see some of the different uses, the users of this data, who buy the aggregate data. One example is marketers or banks or so on who use all the different information collected through the data broker services.

Then coming back to the consumer, there's a variety of services that happen from the data users into this aggregation data, and it can be the extension of credit. It can be advertising. It can be a whole host of things that the data users then bring back to the consumer, and in some cases the consumer is a aware of these services, and in other cases they're not particularly aware of.

The one thing that's important here is that we have both a primary user of data and secondary uses of the data. For example, if I buy a house and pay property taxes, a lot of people don't realize that information about my house is then used to characterize

me for marketing purposes, so secondary use.

What we're going to look at also then today is some specific examples of the use of data in everyday transactions here. This is one that's personally applicable to me is over the last three or four years I've had to, like a lot of folks, start taking pills to regulate various health issues, and so one of the things I have to do is get my prescriptions filled at the local pharmacy.

And here we have part of this data ecosystem, how information is used to perform that service, some of which are -- I'm very aware of and other ones that I'm less aware of, but the basic economic transaction begins with the doctor providing me with a prescription. I then take it to my pharmacy where information is entered into the computer about myself as well as about my prescriptions.

One thing that's important is if you get pills on a regular basis, you get one prescription that renews for up to say a year, and it's up to the pharmacy and their computer systems to keep track of those refills, and so one of the benefits I get then as a consumer is I don't have to go back to the doctor for every prescription.

So when the pharmacy fills a prescription, they

enter the data into their computer systems, and one thing they do, a new service that the pharmacy is providing now is they will call me on the phone when it's time for me to refill a prescription. It's one use of data. Now, that's a marketing program as far as the pharmacy goes, but from my perspective that's a convenience.

Now, there's other places that data flow too out of the pharmacy. One if I'm paying for my pills through the health insurance, the health insurance company is going to learn about it, but then also there's a whole other hidden behind the curtain activity where various prescriptions go to a pharmaceutical analytics company that analyzes all the different prescriptions that people are buying for a variety of purposes. One can be disease tracking. Another one can be for information for media.

Another area that's been relatively controversial is in the area of marketing to doctors, that these aggregate statistics that are generated by analytics, some of these statistics are done specific to the doctor, and the information is then sold to pharmaceutical companies and also used by pharmacies to market back to doctors, and this has been an area that's been controversial, some legislation has been done

against, but the idea is that the pharmaceutical companies base their marketing to a specific doctor based on all the different prescriptions they've been developing.

Another area that's been interesting that's driven clearly by technology, particularly with high speed Internet connections and something that we're hearing a lot about is social networking websites. These are sites like Facebook and MySpace or LinkedIn, which provide a way for people, friends and colleagues and even strangers and whatever, to communicate. It basically provides a community where people can discuss in a semi private area a variety of topics.

And the basic idea behind the social networking website is you register with the website, so it's a voluntary activity, and you get an account, and from there you say to that website who your friends are, and so you get connected up to them, and it creates an area where everybody can communicate in.

Some of the information that you provide as part of that social networking, however, is made public, and it can be viewed by anyone. If you, for example, Google people, sometimes some of the first things you will see will be profiles at places like Facebook and LinkedIn, but then also there are other parts of the information

that is only available to people that you trust, friends and people who you've agreed to be connected up to.

But a whole other aspect that's going on behind the curtain in the social networking sites is the use of information that you provide as part of your profile, as well as part of your discussions with friends, is the advertising aspect of things, so you're being targeted with advertising as you're using the site based on all the information that's available either in the profile or in the forums.

Another area that becomes very interesting is many of these web sites support features, what are known as third-party applications, where the websites allow other parties, other software developers to come in and provide content and games and applications that run within the context of the social networking website, and these applications in many cases are supported by advertising, and what folks who are using these websites in many cases don't realize is these applications also have access to some amount of personal data that's being collected by the website, and again that's going off and being used for advertising purposes and potentially other uses that are not clear.

The last area that I want to look at here this morning here on the collection of data, and I think it's

a very important one, something that has become much more important over the last say three or four years is mobile phones or smart phones in particular. A smart phone is basically a computer that's portable that just happens to have a cell phone attached to it, but the key thing about that computer is that it can communicate through the Internet through wireless connection.

So we're able to collect data or observe data with that device at any place, at any time, and so a key feature of these new smart phones is the ability to locate themselves, that is, find out where they are on a map at any point in time, and they use a variety of technologies to do that, including GPS, Wi-Fi and cell towers, so you have a very powerful combination there for doing data collection.

You have a smart device that an run applications, arbitrary applications, you have a communication network which allows it to phone home, and you have something that provides location, so we have companies out there now developing a whole interesting host of applications using these technologies, and it's sort of the next level of data collection, if you will.

On the chart here, we show a couple different applications using smart phones. One is a mobile coupons application, the idea that as you're walking

around, you can run this application, and it can provide coupons for businesses in the area that you're currently at, and so the idea is you download the application to the cell phone, and you, at the same time, provide personal information to the vendor who is providing coupons, and the application runs.

Then as you execute it, it will provide you with a variety of coupons, and you can do things like say, here's the kinds of coupons I'm interested in, like -- I still have 30 seconds in spite of that. The idea is that you say what kind of coupons you like, whether it's restaurants, bars and so on, and then based on your location and the types of coupons that are available to the coupon provider, they're sent to your phone.

Another more interesting application, one that seems to be targeted at the younger crowd, I'm not sure I would want this one, but is the mobile friend locator. It provides sort of the next level of the ability to watch us as we go around our lives. The idea is you sign up with this service, again download an application, and it shows on a map, when you run the application, where all your friends are located, but you also have to opt in to this service. So the idea is that it's a Friday afternoon and you want to get together for dinner that night, you can go see where

everybody -- who's close by and then meet up.

Again, what else is going on behind the scene, it's a free service so there's advertising that goes on behind the scenes, so the ads are shown as part of the map with the idea trying, that's where you're going to meet your friends at.

In addition, one of the services we looked at allows you to also upload your position to your social networking home page, so not only people with phones can figure out where you're at, but also all your friends who are following you on a particular social networking website, and again advertising can then be provided on that website based on your location.

It's a level of surveillance I think a lot of people will be surprised that we would have -- if you go back 20 years ago would be accepting, but it's out there, and it's something that people, if they want to participate in, can.

With that, I would like to move on to the first panel here, and thank you very much for the opportunity for speaking.

(Applause.)

PANEL 1: Benefits and Risks of Collecting, Using, and Retaining Consumer Data

MODERATORS:

JEFFREY ROSEN, George Washington University Law School

CHRIS OLSEN, Division of Privacy and Identity Protection, FTC

PANELISTS:

ALESSANDRO ACQUISTI, Associate Professor, Carnegie Mellon University, Heinz College

SUSAN GRANT, Director of Consumer Protection, Consumer Federation of America

JIM HARPER, Director of Information Policy Studies, The Cato Institute

LESLIE HARRIS, President, CEO, Center for Democracy & Technology

MICHAEL HINTZE, Associate General Counsel, Microsoft Corporation

DAVID HOFFMAN, Director of Security Policy, Global Privacy Officer, Intel Corporation

RICHARD PURCELL, CEO, Corporate Privacy Group

MR. OLSEN: Can everyone hear me? I'm Chris Olsen. I'm an Assistant Director in the Division of Privacy and Identity Protection. I want to thank you all for coming. We have a huge crowd here today, so if it's possible for folks to squeeze in, if there are open

seats in the middle, I would ask folks to try and do that.

We have some panelists I see in the back there. There are some reserved seats upfront for panelists, if you want to come up. One more administrative detail, we have a Wi-Fi connection, and there are information sheets up front about how to get access to the Wi-Fi.

Again I would like to thank everyone for coming. First I would like to thank and introduce my co-moderator, Jeffrey Rosen. Professor Rosen is one of the nation's leading legal scholars and privacy experts. He teaches at George Washington University Law School, is legal affairs editor at The New Republic and serves as a senior fellow at the Brookings Institution. We're very pleased that he's agreed to help us navigate the issues we intend to explore this morning.

I'm equally pleased to introduce our other panelists. Alessandro Acquisti is associate professor at Carnegie Mellon University. Susan Grant is Director of consumer protection at the Consumer Federation Of America. Jim Harper, Director of Information Policy Studies at the Cato Institute. Leslie Harris is the president and CEO of the Center For Democracy and Technology. Michael Hintze, associate general counsel at Microsoft Corporation; David Hoffman, Director of

Security Policy Global Privacy Officer at Intel; Richard Purcell, CEO of the Corporate Policy Privacy Group. Anita Allen could not make it here this morning unfortunately, and we apologize for that.

I would like to say just a couple of words to introduce the subject of the first panel and explain how the panel is going to go. As we've heard already, technology has brought many dramatic changes to consumer lifestyles. Many of these changes have brought tremendous benefits, one of the most dramatic of which is the Internet itself with its ever expanding array of easy access, free content, information and communication and services.

Yet, at the same time, consumers are becoming increasingly concerned about how technology may be used by companies to collect information about their online behavior, to segment them into special categories based on their online activities, and use information about them in ways they may not know about or understand.

For a long time, companies have been gathering information about consumer habits, interests and activities in the offline world through warranty cards, surveys, contests, subscriptions and census information. That collection of offline information is now being enhanced through the collection of online information,

information such as click stream data showing where you travel around the web, online surveys at websites offering guidance for specific problems, purchase information, reading habits and search queries.

This opening panel, in the FTC's dialogue on privacy, is to explore this dramatically changing landscape, look at ways in which information about consumers and their everyday lives is gathered, analyzed and shared among companies for marketing and other purposes.

We will talk about the ways in which information may be compiled and used and ask our panelists for their thoughts on how the collection and uses of information offer benefits or create risks for consumers, whether certain information collection and sharing activities are subject to existing rules or laws, including whether there are limits on how long companies can retain information or how they may use information, whether consumers understand or are aware of the extent of data collection and compilation, and whether they can exercise control over that collection and compilation.

Our format this morning is a bit different than usual. Rather than having each panelist offer remarks or make presentations, we plan to explore the issues through a series of real world scenarios. These fact

patterns will allow the panelists an opportunity to discuss some of these questions and engage in a dialogue.

The audience is also invited to submit questions. We have staff members with index cards in the room. If you have a question, please raise your hand to get a card. Staff will collect the questions for us. Also webcast audience members may submit questions to Privacyroundtable@FTC.GOV.

Professor Rosen is going to lead us off with the first scenario. He may also have a few remarks.

MR. ROSEN: Thanks so much. Well, I am delighted that the FTC has begun this roundtable series on exploring privacy, and I'm honored to be part of it. I was so pleased that Chairman Leibowitz, in his introduction, cited Louis Brandeis, because Brandeis, of course, was not only the patron saint of American privacy law, but also the patron saint of the FTC, and I think he would have been very pleased by the FTC's turning its attention to this important subject.

Brandeis was deeply aware of the threats that new technologies posed to privacy. In the 1890s, as the Chairman said, there was the Kodak Camera and the tabloid press that made him concerned that what used to be whispers in the closets was now being shouted in the

rooftops.

By 1927, in his famous Olmstead dissent, it was a different technology, namely wire tapping that made it possible to listen on telephone conversations without physical trespass, but Brandeis was astonishingly prescient. In a remarkable passage he predicted the envisions of the Internet. He said that wats may some day be developed, which wouldn't be possible without physical trespass into the home, to extract papers from secret desk drawers and introduce them in court.

It was a remarkable bit of prescience. He had wanted originally to include a reference to a new technology, namely television, and he had newspaper clippings about it, but he was persuaded to omit the reference by his law clerk, Henry Friendly, who thought that it would sound too Sci-Fi and just that no one would believe it. It may have been this caution that led a later law clerk of Judge Friendly's to remark that, Friendly was indeed a genius but he wasn't friendly.

Brandeis, in the Olmstead dissent, said that the Constitution should be translated to take account of these new technologies and that the Fourth Amendment should protect as much privacy in the age of wire tapping and the electronic age as it had in the colonial

era, but in his role as a founder of the FTC, Brandeis was also deeply sensitive to the role that government regulators could play.

He was convinced that by bringing different constituencies to the table, labor and business, government and citizens, it was interesting that Brandeis hated the word consumers, that a thoughtful balance between competing interests could actually be struck, and that's why I think that he would have very much approved of our efforts today.

As Chris said, we're going to proceed by way of scenarios. The danger of privacy, as all of you know well, you're all pros here, is that if you stay too far in the clouds, you can miss many of the textures that make this debate so relevant, so I'm going to begin with a scenario that many of you will recognize. We will ask our panelists to talk about it, and then Chris and I will alternate with other scenarios.

Here's the first one. In 2006, AOL released a text file of 20 million web search queries for 650,000 users. It later apologized saying it was an unauthorized move by a team that hoped it would benefit academic researchers. Nevertheless, by linking search queries to a common identifier, the New York Times and others were able to locate individual searchers,

including a Georgia widow, who frequently researched her friends' medial ailments.

Another user, number 927, gained web notoriety after searching for Holocaust rape, Japanese child slave molestation and rape porn, virtual children. The disclosure led to the resignation of AOL's chief technology officer.

The next year, in 2007, as part of a copyright suit, a Federal Judge ordered Google to turn over to Viacom its records of which users watched which videos on YouTube. For every YouTube video, the Judge ordered Google to turn over the log-in name and internet protocol address of every user who watched it. In the face of privacy concerns, Google and Viacom negotiated a plan to anonymize the data. Imagine, however, that the data were hacked, de-anonymized and published on the Internet.

What I want to ask our panelists is: What concerns are raised by the possibility that our search terms may be exposed to the world? When I began thinking about privacy in the 90s, we were worried about Monica Lewinsky and the disclosure of her book store receipts. She was worried that she might be judged out of context on the basis of snippets of information that would come to define her in the eyes of the world.

These disclosures that we're thinking about today, AOL search terms, Google search terms and YouTube videos seem exponentially broader in their potential to judge us out of context.

Leslie Harris, why don't you start us off by describing what are people afraid of when they fear these disclosures.

MS. HARRIS: Well, what I think people are afraid of is a continuum of harms, starting with embarrassment, disclosure, perhaps to their own families about things that they've been searching. I think people forget we don't tend to have a computer that is just ours, so there's a broad set of people who may be involved.

Obviously people are concerned that they will be labeled, identified, that that piece of data will be combined with other data. I think when you talk about search data, you're talking about search data over time. I'll get back in a minute on whether or not I think it has to be hacked in order to do this because I think that that's not the case, but if you're talking about search data over time, you could well be talking about any other kinds of surfing data over time.

It's the question of: Can you aggregate and put back together from a bunch of individual, perhaps on

their face, innocuous pieces of data, a sufficiently rich profile that you identify a person, and once you identify a person and have that range of data, what we don't know, because we know very little about secondary uses, is: Is this going to be used for employment? Is this going to be used for insurance? Is this going to be used for credit? Is this going to be shared with others?

I'll give you an example my team was researching. One of my young researchers was going through all of her cookies and really doing -- she is a technologist, trying to figure out how all of this was connected together, ran into a network, not one of those who publicly is talked about like Yahoo and Google now are creating these spaces where you can see what you are being searched against.

It was none of those that we know, and most prominently, it said they were searching on medical marijuana and marijuana. It was sort of a cert on its face for the individual that we're talking about, and about 50 percent of the other things that were on that alleged profile made absolutely no sense, but that's single data point that was plainly connected to her through cookies, and it's pretty appalling.

I could have gone on to her computer and seen

that but we also want to know what's happening with that data.

MR. ROSEN: Very helpful. So, Susan Grant, Leslie says that you can actually be harmed by information that's judged out of context. Are there broader concerns, the right to read anonymously, cognitively, mental privacy, even freedom of thought that are at stake here?

MS. GRANT: Yes, there are. I think it's really important to go back to the basics, that privacy is a fundamental human right. The ability to maintain autonomy, to be anonymous, to maintaining your dignity is an important societal value, which we're very pleased to see that the Federal Trade Commission has recognized and that it's reorienting its approach to privacy on the basis of.

So when you think about the fact that most people believe that they're anonymous when they're doing things like searches and when you think about the fact that consumers shouldn't have to give up their fundamental right to privacy in order to use these tools, it means that if people were to realize that their rights are being violated in this way, it could have a really chilling effect on their use of these tools for all kinds of very valuable things.

It's not a fair trade-off, and consumers shouldn't be asked to make that.

MR. ROSEN: A nice way of putting it, the chilling effect can harm both these interests in anonymous reading, and also businesses that are trying to encourage the use of these technologies.

So let's start to think about potential solution. Anonymization is obviously one. Can anonymization address these fears or is the distinction between personal identification and non personal identification blurring, is the likelihood that bits of our digital footprints can be reassembled likely to thwart any efforts at anonymization.

Professor Acquisti, why don't you start us off with that?

MR. ACQUISTI: Well, I do agree that we are have ways because it's sensitive but what constitutes sensitive data has changed, we can take PI, single press information which may not be very sensitive, and we can aggregate it in an interesting way and with identifying information or very sensitive data, passwords.

As Jeff said, I do see anonymization more as an economic problem than a technical problem, and if I could explain what I mean so that it doesn't sound like another case of economics trying to be imperialist

science for concentrating on other disciplines, including computer science. The point is the research in the last five, ten years in computer science, privacy anonymity has made enormous progress.

We do have very good theory over when a certain system can be probably shown to be anonymous, and we have technologies to protect the data.

However, the conditions under which data can be proved to be anonymous, like economic models, are not often all the reality, in the sense that the attacker can often bypass this kind of constraint or these kinds of conditions. They can use additional data that the creator of the model had not considered.

And in the world of sophisticated data manning, cheap storage technology and incredible amount of software for the revolution in blogs. To fill out and is very easy to bypass this kind of protection.

Now, my message is not therefore that privacy is lost, get over it and I don't mean that things are impossible in this world, but it's instead that privacy enhancing technologists can, may not be assured about anonymity in any condition but can make the work or re identifying data harder, including more costly, which means it reduces incentive for another entity to try to identify data which has been protected.

More important than that, the best privacy-enhancing technologist, the best do not simply can block data. They try to allow certain data to be shared, which is for the consumer and for the corporation why they stop and protect other data. We can safeguard technology, and I do believe that we can use technology to meet the interest of both parties.

MR. ROSEN: Richard Purcell, how much faith do you have in anonymity as a solution here? Researchers are now exploring ways of anonymizing Emails and other data so that it has expiration dates, so it can only be read for a certain period of time and then becomes inaccessible. Is anonymity a solution to our concerns about searches being read out of context?

MR. PURCELL: Well, first of all, anonymity is not yet well defined, and so we struggle to a great degree with making a lot of assumptions, so like privacy, like happiness, a lot of these words are words that are more subjective than objective so, first of all, we have to begin to think about what anonymity means, and frankly we have to start thinking, and the more difficult question for me becomes: How do we begin to apply privacy rules to data that's perhaps not personally identifiable data?

Our underlying concept for privacy is that

there's personally identifiable information. If indeed records that are difficult to identify an individual within can become identified, should we start applying regulatory and other standards to those that are a greater standard of care? That might be very helpful.

There are researchers who believe that the identifying anonymous records is relatively easy today because the identification processes are so poor, and they can be improved. As Alessandro said, this becomes an economic model. How do you make it very, very difficult to re identify data, and what's the cost trade-off of attaining that level of difficulty in preventing and any exposure?

Whether a time-outs can matter, whether it expire, most of those can actually be overcome relatively easily. It's a bit like saying, Well, I've encrypted access to my hard drive. Fine, I'll use a screwdriver and take your hard drive out and mount it in a different machine and bypass that encryption routine. There's ways around most testing.

What I worry mostly about in the anonymity world is: How are we going to reasonably protect really sensitive data? Let's just take E health data, personal health record information. We depend as citizens on very, very robust research in order to help all of us

develop better health practices, better medicines, better treatments, et cetera.

Most of that is based on the examination of patient health records and histories that are anonymized in some way or another. If we can't achieve anonymity in that space, we threaten the ability for us to advance our general healthcare understanding as well. This is a very serious problem that has to be overcome.

MR. ROSEN: We've talked about some risks. Obviously there are tremendous benefits to search services offered by AOL and Google to YouTube. How can companies make use of this data, monetize it so that they can sell ads and also avoid these dangers?

I wonder, Michael Hintze, if you can talk us through some possible solutions. Should there be data retention policies so that data may not be retained more than a period of time, therefore it can't be accessible even if it's demanded? Collection or use restrictions, increased transparency? What in your view are productive solutions?

MR. HINTZE: I think the answer is all of the above. The benefits, as you mentioned, of search technology are enormous, and consumers find that a very important service. Search companies collective and retain search data for a variety of purposes to enable

that service to work. They log data in order to protect the security of the systems. They analyze the data in order to improve the efficacy of the search service itself and provide more relevant results, and those all ultimately benefit the users of those search services.

As we've talked about, there are enormous privacy implications to this data. The terms that people search on can be quite sensitive and among sort of their inner most thoughts, and when you string that together over time, there's obviously very important privacy implications to that.

The way to deal with that, the way to enable those benefits while minimizing and addressing the risks is to take a multifaceted approach to protecting privacy from the beginning, from the design stage. When you are putting together a search service, you need to think about privacy upfront.

We talked about anonymization. Anonymization I think is quite important, but it's not a silver bullet, and as Richard mentioned, there are many definitions of anonymization out there, and some are better than others.

I think if you look at the AOL search example, the way the data was re identified was the ability to link search queries over time, and when you amassed

enough data about a unique individual in some cases, that was enough to identify the person. I think it's important also to keep that in perspective. There were 650,000 users in that record. That data has been out there on the Internet for over three years, and a handful of people have been re identified as a result, but that's still a problem, we can do better and we should do better.

The anonymization method that we use on our search engine involves not only deleting the entire IP address, but also deleting all cross-session cookie identifiers, so you break that link of search sessions over time, dramatically reducing the likelihood of that data being identified, but you need to have data security around that system. You need to have transparency about how the data is used, and, yes, you need retention limitations on that data as well.

All the major search engines, and by that I mean the three big ones, have adopted data retention methods, data anonymization methods as well. They differ from search engine to search engine, but all search engines have tried to address that problem.

MR. ROSEN: David Hoffman, is there a point at which retention policies might become onerous from a business perspective? As Michael mentions, Yahoo and

Google now retain search terms only for a limited period of time. Yahoo deletes them more quickly than Google. What if the government were to require purging after a very short period of time, shorter than Yahoo now allows? Would that be economically infeasible and inappropriate from a regulatory perspective?

MR. HOFFMAN: I think it depends how you address the question. I mean, you could always come up with a period in time that's going to frustrate the business purpose and get to be incredibly short which I think calls out the need for having these kinds of discussions and more detailed discussions on individual issues and trying not to set specific legislative or regulatory requirements of certain periods of data that would apply to a wide range of business purposes.

At the same point in time, there's a number of companies out there that should be absolutely commended for the practices that are being put in place. I think the question we really need to ask is what kind of enforcement and what kind of regulatory structure is to be put in place for the companies that aren't doing that?

And in line with that, I think one of the things we haven't talked much about at this point in time, and it's connected to retention, is data minimization, so at

the end of last year, the Department of Homeland Security did something that I thought was incredibly important, which was included data minimization as a principle in its fair information practices. As we look at minimization, that needs to include a collection limitation, the use limitation and a retention limitation, not just a focus on retention.

I think what we found is we, in my opinion, wasted a tremendous amount of time in the past few years with arguments over what qualifies as personal information, what doesn't qualify as personal information. The reason why I think we've done that is because the consequences of something being or falling into the category of personal information have been tremendously burdensome in different regulatory structures.

If we could instead focus on what is the information that's potentially going to impact an individual, either beneficially or to their detriment, and understand and get a structure in place where we can make sure that companies are appropriately minimizing the amount of data that they collect and then handling what they do collect, I think that's really the direction we need to head in.

MR. ROSEN: Last question for this first

scenario. Jim Harper, you are a Braneisian on the panel, one of several. Brandeis feared the curse of bigness, both in government and in business, and he worried that centralized government regulation might exacerbate some of the problems that corporate size introduced.

So are there some regulations that would be too onerous, some minimization requirements or data retention policies that if imposed by the government in response to these AOL and YouTube examples might make the problem worse?

MR. HARPER: Well, thank you for that libertarian soft ball, first of all.

MR. ROSEN: That's my job.

MR. HARPER: Well, I prefer not to argue at a level back and forth why too much regulation would be too harmful. It's undoubtedly true that moving in to early in an area where we don't know well enough what consumers' interests are and what the future of technology or businesses are, that would be damaging.

I think everybody recognizes that, but what I'm interested in is maybe moving the conversation to another level. Let's ask the people who really have interests at stake. What do consumers want? How do we figure that out? We're, all of us in this room are very

keenly aware of these issues, and unfortunately the public is not. So I think the problem is to let the systems work, let the social systems work, let the market work, let advocacy work to draw out what the real problems are, and then strike the balances.

Is this a big enough problem? Should there be anonymization? Let companies challenge each other's anonymization practices, facilitated by the press, facilitated by advocacy and sometime regulators, so certainly obviously regulating too strictly too early would be a mistake, but we still have to define the problem set, not just as intellectuals in Washington D.C., but across the country and forward through the history of advancing technology.

MR. ROSEN: Great. Thanks so much for an informative discussion. For the second scenario, Chris.

MR. OLSEN: Thank you, Jeff. The second scenario involves two situations, both in the social networking environment. In 2007 Facebook introduced Beacon, a transparent form of online tracking, sending news alerts to user's friends about goods and services they buy and view online. One Facebook user was furious that his purchase of an engagement ring was broadcast to his fiance ruining the surprise.

Recently, after protests from thousands of

users, Facebook disabled the feature. Some have defined privacy in a sense as the ability to control how and when information about ourselves is disclosed to others. It could be argued that Beacon threatened that sense of control and inspired protests.

Another incident a bit earlier involved a woman, a 25 year old single mother hoping to begin a career as an educator, being denied a degree by Millersville University in Pennsylvania. She filed a lawsuit alleging the school denied her a degree because administrators discovered a photo on her MySpace page that showed her wearing a pirate's hat and drinking from a plastic cup with the caption drunken pirate. A court rejected her claim, finding the school offered other reasons for denying her degree, but the incident demonstrates the possibility at least that public information may affect the provision of benefits without our knowledge.

Social networking has become extremely popular and valuable to consumers. Facebook alone has gone from 100 million users in August of 2008 to over 350 million as of this month. Obviously provides it and other services tremendous ways to connect and build communities, but are there concerns about the scope of disclosure, about uses of information that may not be

anticipated or well understood by consumers using those tools? David Hoffman, do you have any comments on the use or unanticipated use issues that this presents?

MR. HOFFMAN: Well, I'm struck about a story that I heard from a colleague of mine who is one of the I think the most world renowned experts in data protection and the media who said they were meeting with some business people, and it took an entire day going through on the white board two understand how the data was flowing from different situation to different situation. I think we've gotten to a point where that's a good thing.

It's a good thing that people are innovating and finding new ways to provide businesses and services, and we don't want to get in the way, and we don't want to frustrate that. At the same point in time I don't think we can reasonably expect that the individual to whom the data pertains is going to have an ability to understand that better than world renowned experts who are trying to figure it out.

For that reason, I think we have got a foundation that we can build on. There's been tremendous work over the last couple of years that the Center for Information Policy Leadership has been largely leading to get to an understanding of what a

system of accountability would look like where the entity that the individual is engaging with will then take responsibility for how the data is going to be managed and make sure that the reasonable expectations of that individual are going to be realized across the -- understand that's there's going to be many uses for that data and many transfers of that data between different entities, to make sure that the individual services are provided, like shipping products, and across national boundaries.

MR. OLSEN: Thank you. You commented on the difficulty that consumers have in understanding the scope of data flows, and that raises a question about whether there are things that we can do to increase transparency and to make some of these data flows or at least key aspects of the data flows more understandable to consumers.

Leslie, do you have any comments on how that might work?

MS. HARRIS: Well, and I think there have been some green shoots in the privacy enhancing technologies that have to do with transparency. Google and then I believe yesterday Yahoo both provide I think very robust features that people can look at and see the kind of data that's being collected and the uses and edit that

kind of thing.

So certainly privacy enhancing technologies help, but we've put so much attention into the notion of notice and consent and not enough attention into a broader set of more I would call them substantive fair information practices, and we were talking about them, limitations on collection, limitations on use, limitations on retention, transparency, that I think that if we would shift the focus, the policy focus, and that I think would include the FTC focus, yeah, it's very important for good companies to be thinking about limitations, et cetera.

But I also think that our sort of policy framework needs to expand because I do not believe, and I'm a great believer in privacy enhancing technologies, that we are ever going to get to the position that simply making all of this more transparent to consumers is going to fix things.

I think these tools are important. We just initiated a campaign to get more of them out there in the marketplace, but that's not a whole answer to this by any means.

MR. OLSEN: And some of the efforts you talked about and we discussed earlier, the efforts made by Google and Yahoo --

MS. HARRIS: Very important.

MR. OLSEN: -- are important, but I guess it raises the question about other activities in the marketplace. What about the other companies that exist that may not be engaged in creative efforts similar to the Googles and the Yahoos? Richard, do you have any views on that? What do we do with the other companies?

MS. HARRIS: You regulate them.

MR. PURCELL: You regulate the hell out of them.

MS. HARRIS: That's what I was muttering.

MR. PURCELL: I've been at this for quite a long time, with major corporations, and the Federal Trade Commission wants informed consent. If we had informed consent, we would be a lot happier, and there are serious limits now -- because of the complexity of the data flows that David mentions, because of the issues that Leslie raised, there are serious concerns about how the heck we can use notice and consent and transparency in order to gain informed consent.

At the same time, it's personal opinion that companies have been very lazy about doing much work to develop an educated audience. There has been very little expenditure by major corporations or small ones, very little collaboration between the commercial and the public sector, to mount a real public education campaign

about online behaviors, advertising, risks, exposures, et cetera, et cetera, et cetera.

Most companies say, My God, there's two things, one expensive as heck, I just can't afford it; two, liability, liability, liability, I can't do that. I would much prefer to pay my lawyers their fees to just put up a real complicated and dense privacy statement, and that way I'm covered, but I'm covered is insufficient.

In my opinion, we've got to encourage companies to start taking on a more courageous role in not only educating their work force, which has only really just begun in the first place now, but educating their citizens, their individuals, the people with whom they deal, about the realistic use of the applications that they're putting forward online and spend the money on it, really work to do that.

We'll hear later today on some of the panels with Jules and others how that is beginning to take some -- there's some traction in the marketplace for this, but as David mentioned, if it takes informed people an entire day to plot out how it works, then how the heck are we going to be able to, in the kind of very short limited time span individuals will provide to us -- how are we going to communicate what the

implications of that are and the suggested actions that they take?

So we get to a privacy by defaults kinds of comments, as well as privacy by design. It's a very, very complicated area, but money has to be spent. Time has to be dedicated to this.

MR. OLSEN: Thank you, Jim. I want to give you a chance to comment as well, and for those of you on the panel, if you want to interject, just raise your name tag upward. Alessandro, I'm going to get to you in a moment.

Jim, I want to ask you if the concerns that -- the two scenarios that I played out are just that, they're two scenarios. Is there a larger concern represented here? Are these anecdotal stories? How do we measure the significance of this issue?

MR. HARPER: Well, I think that the thing to do with these scenarios is to flip how we look at them and recognize the role of trial and error and discovering what problems exist and how to address them. These are two errors of varying degree that taught various communities various things.

We all now race to be the first at any meeting about privacy and say, you know, data can be re identified, you know that Yahoo case, and we race at

meetings to talk about how the Beacon thing went. Also broader communities and the public learn from these errors, and those lessons propagating out across the business community and out across the consuming community help navigate the way forward.

And I think it's mistaken for us to, as much as we would like to and as much as we're good at it, to intellectualize about what consumers should want and then decide how to fix the problems that are obviously presented by these elaborate flow charts. There is a process for figuring out these things, and if we step back and watch it and understand that trial and error plays an important role in guiding us, that will be a great help.

I do think that we need to look to consumers to decide what they want rather than cutting short those processes.

MR. OLSEN: Thank you. Alessandro, you had a comment you wanted to make?

MR. ACQUISTI: Yes, and I would like to raise a slightly dissenting opinion on the topic of notification and transparency, which are good things, important things, but they're not enough, and I say this knowing that identification can work. The studies we are doing at CMU, we claim is -- sometimes it shows notification

can help consumers get closer to their stated privacy preferences.

However, I see notification, control, transparency as necessary conditions, but insufficient. And I say that not as an activist, but as a researcher. There is by now a wealth of behavioral data and databases showing what are the gaps between what consumers want in terms of privacy and their ability to achieve these stated intentions.

And there is probably first of all asymmetric information. When and often data is used and how, and maybe we can fill -- we can address it with education transparency and so forth, but there are other problems that a simple transparency identification doesn't help address.

There's a problem in that we are binding our cognitive ability to ask for information, and we have cognitive behaviors that do affect decision making sometimes and end up making people choose things they later regret, and that happens often in the case of privacy because privacy costs are often long-term.

We don't fear immediate loss when we reveal data. Nothing bad could happen, but if it happens, it's usually later on in time, sometimes much later in time, and it's been proven again and again by research that we

are very bad at making decisions when the benefits are immediate but the costs are at a much longer time.

Then there's an issue that it seems the privacy costs are coming to various -- there is not a very high frequency of probability, spam, for instance, or there are very high, very dangerous but very low probability such as being arrested for a case of mistaken identity or other examples, and both cases are difficult for us to deal with because cases where the risk is really high, but low probability, we tend to dismiss them and overestimate probability considering even lower than it is.

In cases where instead the probabilities of the event occurs is high but the cost is more such as say spam, some examples, we don't understand how these costs actually accumulate over time. Even each of them is small, but over a period of time they accumulate.

To give an example, not privacy related, many smokers do realize that smoking cause cancer. They do realize that each cigarette increases by a minimal amount the probability of developing cancer, but the challenge understanding the next cigarette you are about to smoke will indeed be part of a long chain of other cigarettes that you will be smoking the rest of your life.

In the privacy case, we have a similar condition. We do realize that we need more and more information can accumulate over time, but we don't take. We don't move into the next acting on that concern.

MR. OLSEN: Thank you. I would love to let all the folks jump in here. We're on a tight timeframe, and I think we're going to move on to the next scenario, but if you guys find an opportunity to raise the points in connection with the next scenario, please do so.

Thank you.

MR. ROSEN: So our third scenario comes from a world of list brokers. Imagine this. You're suffering from depression. In the course of your online research about depression, you fill out a personal survey that includes personal information which you hope will get you the help you need.

Soon after, you receive aggressive pitches online and through Email promising cures for your mental health problems. You wonder: Where did this information come from? It turns out that there's a list that markets can buy to identify people just like you. Here is an excerpt from an actual description list: "MedMat has brought together this group of individuals with wide ranging mental health issues. Mental health problems can create a significant burden on the

afflicted individual, making them extremely receptive to any campaign that may be able to offer some assistance or relief," and depression is not the only category on this list.

Other marketing categories include anger, antisocial behavior, anxiety, bipolar, depression, eating disorders, lack of sex drive, poor memory, high stress, or imagine that you have a weight problem and may have bought targets targeted to identify obese consumers in the past. Soon you receive targeted ads that promise to address your situation sold by a niche marketer who promises "these dieters are great prospects for all diet products and other health and nutritional products. These weight watching consumers will try anything in the hopes of being healthy."

So, these are only two examples of niche marketing categories available today on the Internet. There are thousands of similar categories available. It's easy to raise questions about niche marketing, but are there benefits to niche marketing lists? Don't people suffering from illnesses benefit from getting information relevant to them?

Susan Grant, why isn't this a great thing?

MS. GRANT: Well, this is not a new concern. This concern has long existed with telemarketing and

mail marketing. I think the Internet heightens the concern because of the increased ability to gather and segment information about consumers, and it's information that consumers are not knowingly providing for that purpose.

They're usually providing it for another purpose entirely, and as you point out, it can be used to take advantage of extremely vulnerable consumers. In our view, there are some categories of information, such as health, that are just so sensitive that it shouldn't be collected and used for marketing purposes.

I would hope that if a consumer was looking for health related information, they would get advice from their doctor, and they would anonymously, if that was possible, search the web to get that kind of information.

I don't think that whatever the benefits of this marketing might be outweigh the privacy concerns that it raises, and also the concerns for things like fraud and abuse of a vulnerable population.

MR. ROSEN: That's great, Jim, can you give a wholehearted account of what the benefits might be?

MR. HARPER: I can give maybe a suitable account. What this illustrates I think best is that advertising is tacky. Advertising about advertising is

super tacky, but the question is: Is it bad? Is it harmful? And we really should be careful about assuming the results.

For a long time, I have been a sceptic or maybe tried to warn our community about opposing advertising, about medical conditions. Take diabetes, for example. It's a condition suffered by many people who are lower on the economic spectrum, who may not be good about getting to their doctor on time, taking their medications on time.

Advertising may play an important role in advising them about new treatments that might be easier to take, that might be cheaper, et cetera, et cetera. So I would be very hesitant to stand in the way of allowing advertisers to reach communities like this.

As Susan says there are certainly concerns with a variety of abuses, and those stand out as obvious, but when people fail to get a new medication because we decided they shouldn't get advertising, that's a silent harm that could be greater than the risks we know about.

MR. ROSEN: Leslie, harms and benefits and why don't you advance the thought about whether this approach that both Susan and Jim have suggested, a sectoral approach identifying particularly vulnerable consumers or particularly sensitive categories of

information might be a way of balancing the costs and benefits?

MS. HARRIS: Well, I do think that we have to look at particularly sensitive information. I think it's pretty hard to do it by looking at sensitive consumers because we're not making rules that are going to get imposed on people out there.

I'm not sure that I agree with Susan that it should be banned all together, but I think this is the kind of circumstance that you would have to have the kind of serious, robust consent that is rarely provided.

I think consumers leave and often intentionally put a lot of information online about their health conditions, and there is a segment of consumers, and if you go to patients just like me and some of these sites who aggressively believe that it's important to share and get their information out there, and I have been struck by some very interesting conversations between privacy advocates and some of these disease specific advocates about fairly different views on this.

But I don't think because there are people who want to share all of this information publicly that we should somehow -- I just think you have a binary choice here that it doesn't make sense to me. I think that some kinds of advertising can happen, but it's got to be

very serious opt-in kind of consent, and I have to tell you that I am very, very skeptical about how you make that happen.

And I'm particularly worried because even when you do so in certain circumstances, the lack of transparency about making a decision that there's a particular place you would be willing to get offers from or you're comfortable, you're hearing about health on -- you're on a health site and people are advertising, that may not be the same kind of potential harm as that data being collected and advertised over time.

I have experienced having an ad served to me after doing substantial research online about a condition in my family that is not diabetes and not likely to show up, and I found it incredibly invasive, and I certainly didn't feel by clicking through on an ad as compared to reading the medical literature that I was reading that apparently led to this ad that that was going to add enormous value.

MR. ROSEN: We can imagine certain niche marketing might indeed provoke consumer backlashes that would be harmful to companies.

Let me ask, Michael Hintze, are there standards that should apply to businesses to prevent intrusive niche marketing, and if so, what should they be?

MR. HINTZE: I think the answer is yes, and the discussions around ads and ad targeting have addressed some of those as some of the panel have already suggested, around different sensitive categories or vulnerable populations.

I think one thing that occurs to me is that there are just simply responsible practices and irresponsible practices in the advertising space, and we all shake our heads at descriptions of practices that seem to be taking advantage of vulnerable populations, and in the discussions around ad targeting, we've talked about restrictions on advertising to children because they are a particularly vulnerable category of potential consumers, and there are others as well.

It's hard to draw a bright line that says this category of advertising should be off limits for the reasons that folks have talked about already, and in some ways, it's hard to say that vulnerable categories of people shouldn't see targeted ads because in some ways, you can actually be more responsible by targeting.

I mean, take kids as an example. By targeting them, you can make sure they're not seeing the ads for alcohol or not seeing the ads for products that would be inappropriate for them. So I think it really comes down to responsible practices versus irresponsible practices,

recognizing that's hard to write down in rules and legislation and regulations.

MR. ROSEN: Great. So what's now on the table is this question of soft paternalism. I mean, are there certain kinds of choices that should not be allowed? It gets into the transparency debate we were having. Brandeis, who of course said that sunlight is the best disinfectant, believed that when consumers got information about the huge underwriting commissions that were being charged by investment banks, they would rise up in protest and avoid the financial chaos.

But in this context, do you believe, David Hoffman, that consumers cannot be trusted to make certain kinds of choices and they should not be able to alienate sensitive information even if they want to?

MR. HOFFMAN: I think we should be careful in phrasing it that they can't be trusted. I think we should phrase it as: Is it reasonable to expect that they're going to be able to make those choices? There's another number of different situations where we don't just allow a system of trial and error to be out there.

I have young kids, so I think about this often from a child's perspective, and for instance buying children's toys. There are certain aspects where we allow parents to make decisions about children's toys;

for instance, getting some understanding of the age appropriateness of the toy.

At the same point in time, we don't, as of yet, say, let's let the parent make a decision about how many parts per billion of lead should be in the toy, and they can make that bad decision maybe based on cost and the functionality of the toy.

It's this concept, as Mike said, there are irresponsible behaviors, and to me it doesn't seem to be much of a leap to say irresponsible behaviors should be illegal behaviors. The question is then: How do you do that, and how do you do that so that you don't capture a whole bunch of behaviors that really aren't irresponsible or where they might not be irresponsible over time because of changes in the technology or changes in the environment.

I think that then argues for not just thinking about one regulatory process but a process where you have different layers of regulation. For instance, we've had this for a long time, but higher level principles and then with people getting together to talk about, in individual situations, how do you realize those principles, transparency being very important, but just being one component of those principles and with certain techniques and with certain ways of delivering

advertising, what would transparency mean in that context and how much could it do? How much would you have to rely on other principles?

MR. ROSEN: Great. Richard Purcell, it falls to you to propose a model regulation for this stormy question of niche marketing, is there effective consent or should it be explicit? You can cut the gradient map for us.

MR. PURCELL: Great. I think that David's points are very well taken, well said, well taken. It's very important. People need to -- first of all, those people collecting information have to have a very clear guidance on what sensitive data is and what data classes are.

The waiving of hands about sensitive data and the lack of standardization across multiple jurisdictions is making it very, very difficult to understand exactly what sensitive data is. Trade union membership? So it matters, and it's a very culturally specific kind of area, but there are some baselines.

And I think we have to be more vocal, more specific, and a little bit more aggressive or assertive about what sensitive data really, really is and how it should be treated, and certainly when you get to sensitive data, the reuse of that data is the issue

we're talking about.

MS. HARRIS: Absolutely.

MR. PURCELL: And for the most part reusing sensitive data should be prescribed out. It's just off the table. At that point we can it start the real argument.

MR. ROSEN: That's great. For our fourth scenario, Chris.

MS. GRANT: Is it possible to make one point?

MR. ROSEN: An unscripted quick question, absolutely.

MS. GRANT: We're talking about data brokers here, and we just want to make the point that because there's no fair credit reporting type restrictions on what can be collected and who can have access to it and for what purpose, it places all information collected about consumers, but especially sensitive information in a very perilous position.

MR. ROSEN: That's great. Chris?

MR. OLSEN: I wanted to interject, before the fourth scenario, with one question we've gotten from the webcast. The question is: Can a retention period work given the need to maintain copies in archives of information and to maintain audit trails for business decisions and to recover possibly deleted data? I

wonder if David or Michael can address, as two of the industry reps, about that question?

MR. HINTZE: Yeah. Data retention limitations and policies that are adopted around data retention can work. They do work. Companies like mine and others have adopted data retention limits, but it sort of depends on the scenario. There are scenarios where you do need the audit trails, where there's financial transactions. You need to be able to audit and prove and resolve disputes.

There's uses of data for improving products and services that I mentioned earlier, but with any scenario, it's rare that you need to keep the data forever, and so you look at the business need. You look at the ways you can minimize data or minimize the data and protect privacy while you need to retain it, and then you don't retain it a day longer than you need to.

MR. OLSEN: So a risk assessment process, depending on the data.

MR. HOFFMAN: Can I just add one thing to that? I do think it's an important thing for us to think about because I think we also need to look very carefully at any requirement that forces companies to retain data longer than that company normally would do to accomplish the business objective, and we're seeing a number of

those, particularly in the national security perspective.

So to allow companies to be able to retain the data for a shorter period of time and upfront to minimize their collection to begin with --

MS. HARRIS: That's my point.

MR. HOFFMAN: -- so that they don't even have the information because it's not just an issue of secondary use. Obviously we all get a number of security breach notifications every year. It's an issue of just having that data creates an opportunity for there to be a breach over time.

MR. OLSEN: Thank you. I'm going to get into the fourth scenario now, which we started to talk about a little bit. Actually, Susan, you made a point that addresses this. This is another information broker scenario but it involves the credit context.

You've charged something in a store, and soon after you call the credit card company to dispute the charge. Perhaps the item you bought was defective, but the merchant didn't agree and wouldn't give you a refund.

The merchant adds you to badcustomers.com, a list of consumers that have disputed credit card charges. If you find out about this, you can be removed

for a one time fee of $99 for the first removal. Subsequent removals subject you to further charges, but you may not know you're even on the list, which may implicate your ability to get credit in the future, and it raises potential questions about the scope of existing legal coverage and whether consumers are aware that they are or are not covered in a credit context by some of these activities.

Susan, you started to address this. Do you want to talk about this a bit further?

MS. GRANT: Sure. There are lots of other secret lists as well. There's a list that's maintained and shared by long distance telephone companies of deadbeat customers. There are lists of people who have abused bank accounts, and in many cases they're not covered by FCRA, Fair Credit Reporting Act requirements, so not only is there no limit to their collection of that information and who can access it and how it can be used, but also there's no right of consumers to access that information, to correct it, to delete it.

I would say that this is a right that should apply to marketing lists as well as bad customer types of lists, and it's really important for us to decide whether it's fair to have these lists, and if it is, to give consumers the fair credit reporting type tools that

are available to protect them.

MR. OLSEN: We talked about sensitive or vulnerable categories of consumers, and does this type of list create concerns about potential socioeconomic distinctions being made, vis-a-vis certain consumers, whether they're entitled to specific benefits or services?

MS. GRANT: I would love to answer that. Any time that you can segment people by their characteristics, you can make decisions about them for a variety of purposes, justified or not, based on all sorts of criteria that we, in our public policy, deem to be undesirable making decisions about people; for instance, according to their race or their ethnicity or their gender.

But because this is all being done invisibly, where if you get offered a certain price for something that's different than another person or terms that are less advantageous than someone else, unlike the fair credit reporting scenario where a notice has to go to you, alerting you you've been denied or treated this way because of this particular thing, you don't know that. You don't get any notice. There's no way for you to know it.

And the populations that we're concerned about

are the least likely really to be able to understand this and do anything about it.

MR. OLSEN: Leslie, did you want to add something?

MS. HARRIS: I think the key here has got to be some sort of access and correction rights, and I don't think this is just aimed at particular populations, and if we talk about, what do we need to move beyond the individual practices and into law, I obviously disagree with Jim that we ought to be doing privacy by trial and error, and I think we need a baseline law, and a key part of that has to be access and correction, and that has to be apart of everyone including data brokers, and that's just I think a key element.

You will always have, because of socioeconomic and educational differences, people more able or less able to exercise those rights and use them, but you have to have them as a baseline, and then you expect good companies to make it easier and better, and we expect the FTC to know more than we do, which I think it doesn't right now.

I think what I'm struck by mostly is that we're all having conversations with companies who have fairly transparent processes. There's a whole world of actors out there, and that we don't have the tools, and the FTC

I don't think has the tools to truly to investigate them. I suppose you have subpoena power, and you ought to use it more often, but on questions of: What are the other uses that this data is being used for, I really think it's incumbent upon the FTC to exercise whatever power it has to find this out, and then we can make public policy judgments.

I'm struck by that all of the examples tend to be when something is accidentally revealed, so we talk about AOL or we talk about the Facebook, which are sort of peripherals compared to sort of intentional, long-term decisions to use privacy, to misuse privacy.

So we have a missing piece here, and that missing piece is really understanding the practices. It's not just consumers who don't understand those practices. I don't know that any of us do. We're sort of driving this by incident and by what's revealed accidentally.

We have to come up with another way, if we're going to develop whether that's law or a new set of FIPPs for the FTC, we have to get a different information base we don't have.

MR. OLSEN: Thank you. I think part of the rest of today's program will address some of the issues, Leslie, that you've discussed.

Jim, I want to give a chance to comment.

MR. HARPER: Well, sure. It's pretty easy to argue that we should do with trial, error and learning, but it's pretty unsubtle. You can do away with a lot of progress, a lot of consumer benefits.

MS. HARRIS: I didn't suggest we do away with it. I just suggested that perhaps we shouldn't decide that the best way to protect privacy is by trial and error, but let's keep talking.

MR. HARPER: Very well. I was just interested in making a brief comment on the idea that the Fair Credit Reporting Act style protections would be appropriate for the kinds of data in this scenario, and I would be concerned with applying those kinds of connections in total because the Fair Credit Reporting Act preempted state tort law as to credit bureaus and prevents people from suing on the basis of defamation or interference with perspective economic advantage.

The causes of actions that over the last 30 years could have done quite a bit to turn the credit reporting industry in a more favorable direction for consumers, and so I wouldn't want to provide companies the protection of being made immune from state tort law, which is an important protection that we've foregone in this area.

MS. GRANT: I agree, no state preemption.

MR. HARPER: Deal. It's done.

MR. OLSEN: Our time is running short. Let's move now to the last scenario.

MR. ROSEN: Our last scenario has to do with mobile wireless technologies. Are there additional concerns when consumers are profiled based on their past purchases or creditworthiness and then sent targeted ads based on their geographic location?

Mobile wireless advertisers can track your physical locations and beam ads to your wireless devices based on your recent past buying habits. When you walk past a McDonald's, for example, you might receive ads for salads rather than hamburgers that mirror your healthy eating preferences or you might receive distressing ads for Big Macs.

Imagine that you've just activated your credit card, and an anonymous process tells a list broker to start pitching you for fundraising requests as you walk by museums or symphony halls or rap stadiums in the hope that you're feeling generous.

I want to ask what the benefits of these targeted mobile wireless ads might be. Jim, I'll start with you. I called us Braneisian, but when Richard Smith mentioned the mobile friend locator, I thought

that Brandeis would have shuttered. His form of social networking was his wife would invite people up to their chilly Connecticut Avenue apartment, and government officials would sit next to him in 15 minute intervals to discuss the Athenian Democracy. I mean, that was sort of the extent of his social networking.

Do you want to give a defense of what this sort of targeted ads based on your firm's buying preferences or your buying preferences in real time might be? What are the benefits of these?

MR. HARPER: No, I don't want to do that. I want to raise an additional concern that has not been discussed yet today essentially or you referred to it obliquely in your opening, so let's pull back the curtain. I think Richard Smith did a good job with these charts that are in everybody's packets, pulling back the curtain most of the way, but let's pull back the curtain the rest of the way and discuss government access to all this data.

In the prescription area, governments are using data that is collected to go after pain patients and doctors who prescribe. Certainly search and Email and the quote, unquote, cloud is a presently a huge repository of data that governments are beginning to discover for their purposes, and I think it's very

important not to think that this is just a problem between corporations and consumers but between the citizens and governments.

There's a very, very important concern that should be raised in this context, just like everywhere else with the fact that this data is going to be made accessible to governments.

Chris Sagherian who is here released a report recently, I might get it correct or not, but that one wireless company shared 8 million data points with law enforcement over the course of a year I believe. Mobile companies collect I understand 600 billion data points per day about their users, and they're just beginning to learn how to work with it.

When this kind of data is available to governments -- if it's available to governments on the terms that it is now, that is a surveillance system that we're barely able to imagine, but it's very significant, so I think that's a concern to discuss is how this stuff is accessed by government currently, whether the rules around that are appropriate.

MR. ROSEN: Great. So, Michael Hintze, Jim didn't give us the benefits. He's just afraid of government surveillance of citizens based on consumer data as he is of government regulation of the private

sector. Can you offer a more wholehearted defense of what the benefits of this mobile advertising might be?

MR. HINTZE: Wholehearted I'm not sure. I think, yeah, it's kind of cool. You can kind of think that it's convenient that you're getting the ad at a time that you might actually use it, so I'm not going to say that location based advertising is a bad thing. I think on a whole it's a good thing.

But I think, like so many things we've talked about today, there's a profound privacy implication to that, and all of the protections that we talked about, transparency and user choice and particularly in this space I think data retention are really important.

It's one thing to know where your customers are right now so you can show them the relevant ad. It's another thing to keep a map of every place they've been for the last three years, and so data retention I think is a very important piece of the mobile privacy issues.

MR. ROSEN: Great. So some benefits, some harms so far the harms have focused on misuse by the government or potential misuse because of storage. Alessandro, is there some privacy harm just to being noted in real space and being targeted on the basis of your preferences?

MR. ACQUISTI: Well, potentially you can be very

surprises about discrimination, undesired advertising, so we are going to the point -- I wanted to make it this way, and what I'm saying is that this scenario is a good example of what I was referring to earlier, talking about technology good price. Good price and technology don't simply adopt information.

They allows a nice battle between sharing data and protecting our data. In the specific case of behavioral location based advertising as seen in literature recently, technological space, there's this blind signature algorithms which were developed back in the '80s by David Cho and led to further research into anonymous payments, anonymous defaulting and his credentials.

So we do have technologies that allow you to be authenticated, authenticate the transaction now that a consumer is in a certain location and desires a certain type of advertising. Without identifying the consumer, and we do have the technology.

The challenge is how to bring the technology out of the lab and into the marketplace, and that's where we may be quoting that you have different solutions where smart regulations tried to push the market into adopting this technology that may work.

MR. ROSEN: That's great. So those

technological solutions are helpful. Let's thing about others. David Hoffman, can I ask: What about a risk based approach, privacy impact statements? What are other regulatory approaches to this problem?

MR. HOFFMAN: Well, I think what you're asking is for individual companies that are either going to be releasing technology or designing the services on top of it: Are there ways that it can be done in a more privacy friendly way? And I think that's absolutely right, and I think you need to see that in terms of the greater context of accountability, which is this idea of: How are you structuring that into your individual or company's development processes?

I think up until now companies have regularly said, Look, that's something we're going to do, but look towards self regulation to go and do that. I think we need to start asking the question of whether there should be some principles around accountability that we should be requiring of companies.

MR. ROSEN: Richard Purcell, you've been our data expert in many of these areas. What kind of -- how can principles of accountability be implemented specifically?

MR. PURCELL: Well, they need to be implemented without a doubt. Keep in mind accountability can be

reciprocal. So let's say that you have a privacy by default condition where all of this kind of location tracking and profiling is off until the person with a certain level of information and disclosure opts into it.

The reciprocal part would be as a shareholder of a major organization. Perhaps I ought to be able to track the CEOs, the directors and officers of that organization to make sure that their locations are appropriate to the kind of fiduciary responsibility we expect out of them, and if they can agree to that, then perhaps we would have a different conversation.

Most often, most often the commercial operators I talk with who argue against privacy by default, in other words, having the controls turned off or at the lowest setting available at shipping often say, Oh, that just doesn't work, I can't make any money, nobody will turn it on.

Well, why not? Well, because they're creeped out by it. Well, then fine, they're creeped out by it. If you want to make money by not telling people, and only those who discover it and get the creepy feeling from it will then opt-out, so those conditions just don't work, so the reciprocal nature of it would be good.

If I'm going to be tracked by my mobile provider, perhaps I need to track the officers and directors of the mobile company as well, make sure that they're doing their job properly and they're not spending all their time in Bahamas or in places where I think that they're not responsible for their duties. Accountability is reciprocal.

MR. ROSEN: We have time for one last comment. Susan, as representative of Americans consumers, I have to ask you: Do consumers want contradictory things in this context? They both want to be able to meet up with their friends and get relevant ads, but then they're shocked when the data is misused or retained? Is the problem consumer expectations rather than the lack of government regulation?

MS. GRANT: No. I think that if we want to talk about how to get companies to respect consumer's privacy rights, we have to talk about implementing the fair information practices into law. Location information is just another piece of information that can be used to make assumptions about consumers that may be unfounded or unwanted, no different than any of the other kind of information that we've been talking about here, although it could be really sensitive, not just information about your mobile location but just in general where you

travel and who you travel with.

That information is being collected more and more by government, through airlines and other companies and used for ways that consumers would never expect, and in the comments that we filed with the Consumer Travel Alliance, we pointed out that consumers are unprotected from things like a travel company going bankrupt and all the information that's collected about their travel being available for sale to marketers and others.

It's unreasonable to expect that consumers are going to be able to understand and anticipate every potential use for information that they either unwillingly supply or are asked to supply for another purpose, and we really need legal protections.

MR. ROSEN: That's great. Well, ladies and gentlemen, as you know, privacy discussions can be abstract and unfocused and unbalanced or they can be illuminating and precise, and I can that this panel very much fit into the second category.

It was a thoughtful accommodation of competing perspectives, which in many ways is the definition of privacy, and a very promising beginning for a productive day, so please join me in thanking our panelists.

(Applause.)

MR. OLSEN: Thanks to Jeff Rosen for helping to

moderate this panel.

(Applause.)

MR. OLSEN: We're going to have a very short break, try and keep it at ten minutes.

(Whereupon, a brief recess was taken.)

PANEL 2: Consumer Expectations and Disclosures

MODERATORS:

LORETTA GARRISON, Division of Privacy and Identity Protection, FTC

CHRIS OLSEN, Division of Privacy and Identity Protection, FTC

PANELISTS:

LORRIE FAITH CRANOR, Associate Professor of Computer Science, Carnegie Mellon University

ALAN DAVIDSON, Director. U.S. Public Policy and Government Affairs, Google

JOEL KELSEY, Policy Analyst, Consumers Union

JULES POLONETSKY, Co-Chair, Director, Future of Privacy Forum

ADAM THIERER, President, The Progress & Freedom Foundation

JOSEPH TUROW, Professor of Communication, University of Pennsylvania, Annenberg School for Communication

ALAN WESTIN, Professor Emeritus of Public Law and Government, Columbia University

MS. GARRISON: Hello, and welcome to panel 2. This morning we heard a lot of conversation from various people such as Jim Harper and David Hoffman and others talking about, Well, what do consumers really want and

what about disclosure and transparency? Well, we're going to get the answers from this distinguished group of panelists. This panel is going to address what we know about consumer expectations with respect to the collection and use of their information.

We've heard that surveys present little value on this issue because they don't actually measure real consumer behavior. On the other hand, there's general agreement that consumers really don't understand what happens behind the scenes, as they use a loyalty card when purchasing goods, they browse or they search online, they visit web sites or complete a survey.

So relying on actual consumer behavior to understand consumer's attitudes toward and expectations about the collection and use of their information has limitations. Our expert panel today is prepared to talk about these issues in light of their own research as well as to address the role that disclosures play in informing consumers about data flows or as a vehicle for consent to commercial collection and use of information.

First I would like to briefly introduce our panelists: Lorrie Faith Cranor from Carnegie Mellon University on my left. Next to her is Alan Davidson from Google; then Jules Polonetsky from the Future of Privacy Forum; Adam Thierer from The Progress and

Freedom Foundation; Joe Turow from the University of Pennsylvania; and last but not least definitely is Alan Westin from Columbia University, and I would also like to present to my right Chris Olsen, who is co-moderating this panel discussion.

MR. DAVIDSON: Can I just intercede to say you can't forget about the consumers?

MS. GARRISON: Oh, I'm sorry, Joel Kelsey, Consumers Union, my apologies. For those of you in the audience, again if you have a question for any of the panelists, write it on the question card. It will be collected by one of the staff who are circulating, and for those of you listening, you can Email your questions to Privacyroundtable@FTC.GOV.

Now, we're going to be talking about a number of consumer surveys and studies during this panel. Those are all available on the agenda at PDF links so that if you want to explore these issues in more detail, you're certainly welcome to find those materials there.

I would like to throw out a general question. What do consumers know about data flows and the collection and uses of their personal information, both online and offline? Joe, why don't we start with you because what I would like to do is have each of you talk at a high level about various studies and research that

you've done and what your findings are on this point?

MR. TUROW: Thank you. Yes, at a very high level, as you said, the report's available. We've also done national surveys over the last ten years, and some starting from 2003 I believe have data about what Americans know, so it's not just their opinions, and I think it's fair to say that generally speaking they know very, very little about what goes on online behind the screen under the hood.

The kinds of things they don't know would surprise many people around here, particularly, for example, Americans think that it's illegal to use discriminatory pricing. This is from surveys in 2005. That is, they believe that a company like Expedia and Orbitz is required to give people the lowest amount of fare, simply when people go online. They think it's illegal for supermarkets to change prices for different people during the same day. Generally speaking, people believe that the government enforces laws about privacy far more than it does.

So there is a sense that there are laws out there. People have this great sense that laws protect them far more than they actually do when it comes to privacy.

MS. GARRISON: Joel, have you found anything

similar to that or different?

MR. KELSEY: Our findings are largely similar actually. I think that consumers have a general perception that information is collected about them online. I think they're uncomfortable with the idea of third parties, but for the most part they think that if the information is is being used, sold to target them, they believe that they need to be given notice ahead of time, and that their prior consent is required.

Similarly with the government kind of protecting or government laws protecting the use of their private information, I think they feel relatively comfortable that there's sufficient protections out there when that's just not the case, and I think that the biggest concern that folks have comes from an identity theft and kind of financial risk position, and I don't really think they have a true understanding based on the data that we have of how the information is being used about them behind the scenes.

MS. GARRISON: Lorrie, do you have anything to add to this?

MS. CRANOR: Yes. We found pretty much the same thing, but I think people have very little understanding of both the policies and laws about privacy, but also even how the information flows. There are a lot of

people who don't know what a cookie is still. There's almost nobody outside this room who probably knows what a third-party cookie is, a flash cookie, all these types of terminology.

When we've done one-on-one interviews with people, we find that they're even confused about which part of a web page content is advertising, let alone advertising that's tracking them, which they have very little idea about.

MS. GARRISON: Alan, you've done a number of studies over the years. I'm sorry, Alan Westin, can you talk briefly about your high level findings and how consistent they are or different from what we've heard so far?

MR. WESTIN: My sense is that the surveys that I'm familiar with over several decades are remarkably in concert rather than in conflict. For example, on the behavioral marketing, all the surveys that are represented on the table here found that a majority, ranging in numbers from low 50 percents all the way up to 70 and 80 percents, say they're uncomfortable with behavioral marketing and would want to have, at a minimum, the kind of notice, choice, security and ways of intervening that would give them some comfort if they were going to have their information tracked in that

way.

So even though it's true that we're starting from a base of low knowledge by consumers as to how things really work, if you ask them how they feel about such and such happening, they're pretty strong in believing that they're being abused, that this is not something that they are brought into.

The other thing that my surveys show is that even though you can tell people that it's behavioral marketing that makes possible the freebies of Email and other kinds of Internet benefits, we've gotten to the point, the way the Internet is developed, that people just take that for granted. They're not prepared to make that into a real equation.

So in our survey we ask people in setting up the question that it's because of the ability to provide various free services and things to be free on the net that advertising makes possible. That bargain is now long gone, and people are not willing to trade privacy for the freebies on the Internet.

MS. GARRISON: Alan Davidson, can you comment on this in terms of what you found that consumers expect or understand about data flows?

MR. DAVIDSON: Thank you, and I think certainly it's clear that a lot more work needs to be done, and I

guess what I would say is that there is a lot of work being done now. What we're seeing is I think a lot of innovation in the space in terms of trying to find ways to give consumers more information.

I think generally industry is saying we've experienced that consumers don't necessarily understand all these issues, and there are lots of things that can be done to give them more information. We can dig into some of the examples, but I think, for example, Yahoo's recent announcement about a product launch this weekend that's very similar to something that we've launched to give people -- our users a chance to see more about what we know about them when we're showing them advertising I think is an example of the kinds of new tools that are going to be out there for people to see what is being collected and how these data flows work.

And that's just one of many, many examples. There's many people in the industry who are trying to come up with interesting new ways to inform consumers.

MS. GARRISON: Thank you, and, Jules, I think you're one of those who has been doing some of this work. Can you talk briefly about your findings here with respect to what consumers know and understand and expect will happen to the data?

MR. POLONETSKY: Well, the most recent work

we've done, A, was a set of focus groups and now a larger 2,600 user survey. The focus group feedback, when we tried to drill down specifically on behavioral advertising, the moderate expert users, who were just completely unfamiliar with the concept, the expert users, there were one or two that were familiar and they said, we know what that is, that's when you're watching a movie and all of a sudden you're really hungry and you want some popcorn, and there was something flashed, I thought we were talking about subliminal advertising.

So clearly lots of talking to people about privacy and privacy policies and all the other communications haven't really moved the bar, but what we did start seeing when we turned to the advertising industry, since it's the selling and this advertising that seems to be of such debate, we said, Well, can we use those skills, can we use those communication skills to actually talk to people and taking it out of the hands of lawyers and technologists who are experts in what they do, let's talk to people.

So the folks at BPP spent a chunk of time with us generating language and symbols that we hope can be effective at communicating to people, not a legalese and not anything about privacy but how your data is being used for you. That's a whirlwind for transparency. If

companies can advertise, if they're doing good things, if what they're doing is trying to sell you some stuff, which with or without the word consumer being the right way to talk about people, if they're trying to communicate something about what they have, let's use those skills.

So we're hoping that some of the output of this can be used by the industry who can adopt it and perhaps make it part of an IAB, a DMA, other self-regulatory programs that are not about privacy, here's how we are keeping things secret and not doing anything with your data, but here's how we are trying to communicate with you, and we'll be trying to circulate broadly which phrases work best and what really resonates with users.

MS. GARRISON: Thank you. And, Adam, do you have something to add on this point from a slightly different perspective perhaps?

MR. THIERER: Sure. Well, for many years at Progress and Freedom Foundation we've been taking a hard look at polls and surveys having to do with child safety and free speech, and recently we've expanded that to look into privacy surveys and polls, and our message is really quite simple, which is that while these surveys and polls may offer some really interesting insights into how some people in the public think about privacy,

advertising, and so on, ultimately they are no substitute for real world experiments, which involve making real world choices, often involving real money in real time with real trade-offs.

And those market based experiments happen every single day in the marketplace in ways that we probably wouldn't have imagined they could have if we would have listened to what polls said a couple of years ago. People are living their lives like an open book on social networking sites every single minute of the day and voluntarily giving away information that probably, if asked in the poll two or three years ago, would you do these things, they would have said absolutely not.

Of course we have to also remember what Jim Harper said in the first panel, I think which is important, which is that privacy is a subjective condition and that there's a lot of trial and error out there that people themselves personally experiment with how much they want to give away about themselves every single day in exchange for something else.

There is no free lunch and these services online cost something and sometimes it means we have to give a little to get them and sometimes that something is information, so what I would argue is that there's a little bit of rational ignorance at times at work in

these markets.

We might say one thing if asked by a polster or a survey about what do we think about X or Y. We might do a very different thing once we have our own time and money on the line.

MS. GARRISON: Lorrie, what about this disconnect between the online or the behavior that consumers exhibit on a daily basis and yet what we hear in the polls? Is this truly a disconnect in that what consumers are doing really represents their views toward privacy or is there something more going on here?

MS. CRANOR: So while it's true that there's only so far you can go with surveys, that people will say things and it doesn't necessarily reflect their real behavior, but you still can learn an awful lot from surveys, and I think that we do understand about their attitudes.

Now, if we look at behavior, we've observed all sorts of things about what happens in the real world, but it hasn't actually been set up as a controlled experiment, and so we have situations where people don't understand the consequences of their actions. We haven't done a good job of communicating this, and so people are behaving in the real world based on asymmetric information, as Alessandro had mentioned in

the previous panel.

And so that in and of itself is also not giving us exactly the data that we want here. We have in some of our work at Carnegie Mellon tried to facilitate some experiments where we could actually measure people's behavior in a controlled experiment, and this is very hard to do in a way that you have very valid data, but we have been able to show, for example, that if you annotate search results with information about website privacy policies, people actually pay a little bit more to shop at the websites that have better privacy policies.

So I think it's these kind of experiments, and I would love to have some of the search engine companies actually work with us so that we could do this on a very large sample of users instead of the small ones that we can do as a university.

MS. GARRISON: Alan, do you have any response to that?

MR. DAVIDSON: We would love to work with you on something like that. I was just going to comment in terms of these experiments that are happening in the marketplace, just to give an experience of our own recently. We launched a product at Sprint called -- what we call interest based advertising and an ads

preference manager, and some of you probably heard about it. We have a handout in the back that's kind of a screen shot of it.

Basically the idea was to try to be responsive to the concern that people don't really understand what's happening when we do interest based targeting of advertising, so there are three components to this. One is what we call in-ads notice, so when you see an advertisement that we've helped place, there's a little link so you can get more information about the ad.

The second is that link takes you to a privacy center where there's an ads preference manager that shows the user all of the target -- signals that we're using to target that advertisement, and then there's the ability for the user to change those signals, so the signals might include things like we think you're a sports enthusiast or we think you like interior design based on your web behavior.

And we not only let people opt out of this, but we also let people change it, so you might say, No, no, I'm not a sports enthusiast, but I really am interested in automobiles or cooking, and we've now had this out for about -- I guess since the spring, and what we've seen is it's been interesting for us. This site gets visited by tens of thousands of people every week now.

Actually there are tens of thousands of unique visitors each week.

The behavior has been interesting to us because I think we sort of had the assumption that people who were interested in privacy and were going to visit this site would all be opting out, and what we found is actually that a lot of people come to sites. We've had four times as many people who come to -- visitors to the site actually change their preferences rather than opting out.

So, in other words, people are coming. They're not necessarily using our persistent opt-out. What they're doing is they're playing with it to see what happens if they change these preferences, and actually ten times as many people actually do nothing when they come to visit the site as opt-out.

Now, there's lots of things you can read into this, and it's still a relatively new experiment, but I think to simply say that people aren't informed and if you inform them, all they want to do is get rid of all this stuff is probably too simplistic a view.

I think what we've heard is that your mileage may vary in terms of what consumers want and how they feel about their privacy, and what's been interesting to us is that if you empower people with choices, they may

actually start to exercise them. I think many consumers -- our perspective is that many consumers do understand that there is a bit of a bargain here, and that part of the reason that all of these amazing free services exist on the Internet is partly because of the advertising that supports them.

So there's a lot of work that we do to unpack this, but I think there are going to be more experiments like this in the marketplace, and we will see how -- it will be interesting to unpack how people use them.

MS. GARRISON: Joe Turow, do you have any additional information to add on this?

MR. TUROW: Well, I just wanted to suggest that while I understand what Google has done with those categories, it's important to realize that essentially from one consumer's standpoint, those are marketing categories. You go to that Google site and they say -- first of all, it appears incredibly benign. It almost makes what some people who worry about privacy look foolish because it says you like bicycles or you like water skiing. Why would that be a problem for anybody? And yes, you can get targeted for it and not targeted for it.

What is not shown in this kind of thing, and possibly because Google doesn't do this sort of thing,

maybe because they don't implement it yet, are the various kinds of psychographic, demographic activities that go on continue behind the screen to yield up it the particular categories, or the kinds of things that many companies do to supposedly anonymously grab people's financial information and link them to create profiles.

It appears as if it's simply a, do you like bicycles, do you like cars, sort of scenario, and I think it's not a correct assumption or set of projections of what's happening in our online and offline world.

MS. GARRISON: Jules, do you have a response?

MR. POLONETSKY: Yes. My response is this: What I think we're seeing hopefully, I'll let the economists debate the should users accept it because it causes things to be free, even if they don't like it. I would like to focus on the fact that there is a potential feature here.

When users do interact with the kind of tailoring they like, whether it's choosing a book and understanding what happens at Amazon or at Netflix, clearly we've got some real behavioral evidence that it works, so the question is: Can any of these models, despite the fact they're operating as third parties, the fact of the challenges of the ecosystems being linked as

it is, can any of them actually make data use a feature, and in developing a feature, can they succeed at it being an honest depiction of what actually goes on without it becoming incredibly complicated.

So I think things are going to go in the direction Professor Turow suggests, but I would hope they don't become a dashboard of a 767 because that's as complicated as it does get in some of the back ends here, so my argument is can we at least agree because the perfection is what has prevented any of these things from happening until now. This idea of showing the profile back in my early double click days, oh, my god, it would be too hard to do it accurately.

You need that little bit of experimentation and leeway to figure out how do you create a feature that will succeed in the market so people enjoy it, play with it. Today both Yahoo and AT&T's yellow pages went live with versions of this little symbol which lead to these sorts of ad preferences, interest managers, and so you're starting to see people doing it in different ways and experimenting, and you'll see whether indeed users play with it, like it, turn it off, tweak it and hopefully the kind of feedback, Oh, I don't like those kind of categories so why in the world are you doing them because they'll drive some interaction, will

actually be this first step of a development in the market.

So we need to featurize data use instead of hoping that interested people who care enough about privacy care enough to read a notice or find data about them.

MS. GARRISON: Joel?

MR. KELSEY: Sure. I would just like to go back to looking at real world choices kind of idea, and I think that we do actually see a lot of consumers making real world choices when it comes up to answering that cost benefit question of free content versus giving up information about themselves, and one of the things we found was a lot of consumers try to protect their anonymity by giving false Emails, by providing wrong information about themselves, by deleting their cookies.

And you can talk about whether that's superduct privacy or for computer hygiene, but I think consumers are going to great lengths to try to protect some kind of anonymity, to try to protect some of their personal information, and then we see the market response and the financial incentives of responding flash cookies and things like that to circumvent that consumer preference.

And so I think a lot of these things -- I would also say we also have real world experiences of data

breach of security -- financial security problems, and a lot of this to me leads down to a place where we need some kind of regulatory framework that provides more transparency, that talks a little bit about what kind of data is being collected, what is clearly acceptable, what's not acceptable in terms of what is being collected and how it's being used ultimately at the end as well.

MS. GARRISON: Alan?

MR. DAVIDSON: Super quick response. First of all, to the point about the benign nature of these categories, I will just say in our case it's because those are the categories that we're using. We're not using some of these other things, and I think that speaks to -- for example, there are categories in Google's interspace advertising that we don't have.

We don't have sensitive information that we use for targeting, some of the health, financial information, certain other things that have been discussed, but it speaks to the fact that there certainly is a need for greater transparency.

I also don't want to make it sound like this is an isolated occurrence. We've heard there are other companies who are launching actually coincidentally this weekend, right before this conference, shocking, similar

efforts, which is fantastic. Google has a product called the Google Dashboard that lets you see a lot more, not just about advertising, but all the information that we keep about a Google account holder in one place.

I think there are others. Facebook has been a pioneer in making transparency tools for all the information that's being kept, and these are going to be incredibly important, so we expect that there's going to be a lot of experimentation in the market. You're already seeing it. I would say that you have some very sophisticated players out there who are consumer facing and have a great desire to meet this demand that Joel has already said for people to have more control.

And it's going to be incredibly important because we really believe that transparency and consumer choice it going to continue to be a foundation of fair information practices and how we protect people online.

MS. GARRISON: In order to match the tools that you're providing with what consumers expect, do we have any understanding about their expectations with respect to say the company they're dealing with directly, what they expect that company to use, or do they have -- do we have any information about their expectations with respect to further use of that information by other

companies that are essentially behind the scenes?

Do consumers even know about this? And what would we understand their behavior to be if they did fully understand the data flows, which will never happen but assuming we did? I'm trying to get at differentiating what consumers expect with respect to information on different levels, also different types of information. You know, if you're just going to buy a toy online, that's very different from dealing with health information. Jules or Joe, do you want to start with that?

MR. POLONETSKY: I'll try to be brief. Joe's studies and so many others have shown this tremendous concern, and it's been this theoretical concern because nobody has actually played with a dashboard such as Professor Turow suggests and said, look, it's working, it's not working, this seems to bother me. They don't know what's happening, so if you tell someone, guess what, someone tracked you all day and a lot of the things you saw, I hope you found them useful because we did this for you, well of course you're going to get a negative answer, and that's the reality today.

The question is: Can we bring some of that into public view so that users actually get their hands on it, tweak it, feel it, and we start getting a good sense

as here's what they like, here's what they don't like. One of the things that I like about Yahoo's interest manager is it shows you something that everybody in this room probably knows and everybody outside other than the technologists don't know, that many of these sites know where you are, have some general based on your IP address.

So by saying not only are these the things we think about you because we walked into this behavioral, if it's not behavioral, no one cares, there's other stuff we care about and some of it seems trivial to us. Well, of course, IP, we all know you can geotarget based on IP, but users still kind of wonder why there are -- why there are cuties in Potomac that want to meet me, how do they know that, where do they know exactly where I am, and so the fact that it just says, hey, this is your IP address and so we think you're generally here is just this great I think demystification.

So I think we don't really know what it will truly be like when people start thinking, playing and we featurize data use.

Let me give one limited example. Facebook, we always took about the Beacon example. We've completely forgotten I think the most interesting Facebook example, which isn't Beacon. It may be why Beacon happened, and

that's the outcry that came when Facebook initially rolled out its news feed. Oh, my God, instead of just going to your page and seeing your own page and then having to visit your friends' pages, all this stuff about what everyone did, so and so on just broke up with so and so, so and so just got married here, boom, it's on your page, and there was a big outcry, we were stalking all of our friends.

And I think if you would have asked anybody, would you like, oh no, that would be terrible and instead there were groups, people joined it, and there was an outcry, and now it's now why do we go to Facebook? Because we know learn that Jules is here and he's there and she's there.

And so I think you need a little bit of room, and this isn't an argument for or against legislation -- but we need a little bit of room for letting people delight users with new ways of engaging each other, and then let's learn about how to make sure that we're not surprising them once we understand what they like.

MS. GARRISON: Joe, did you have a comment?

MR. TUROW: Yeah, not to disagree at all what Jules just said. We found that, for example, it's not just the online world. I don't want to color it only as an online. I don't think there's a difference anymore

between online and offline, and most Americans, for example, don't realize that supermarkets have the right to sell their data, and they probably have no idea that supermarkets collect the enormous amounts of data that they collect.

I want to bring up another issue briefly that you suggested I think in your question, which is: How do people even know to trust the companies, whether they trust the companies? So you may have seen yesterday's piece in The Times about Next Jump, which is a company that companies, corporations, Fortune 500s contracts with for discounts, for employee discounts, and why not? It sounds like such a great idea, but apparently what this company has been doing is collecting enormous amounts of data about the people who get discounts, tying it to some extent with their credit ratings, credit card activities I should say, and then using it now to deliver advertising and whatever else they're going to do.

That's the kind of thing it would be very hard to know that anybody in the companies that worked there had any clue that this stuff was going on and whether in fact there was a privacy policy presented to the people, so it's a very difficult scenario to imagine. How do we know when companies are being straightforward when maybe

the companies themselves haven't taken the opportunity to look.

MS. GARRISON: Alan Davidson, I would like to go back with a couple things to you. One is you said that you don't use sensitive information. Can you describe or explain what you mean by that? And also, before you get there, can you give us any sense in terms of a percentage of the total number of visitors to Google, how many actually have gone on to the ad preferences site or to the Dashboard?

MR. DAVIDSON: So on that first point, I don't have an exact number, but I would say it's small. It's obviously very small if we're getting tens of thousand of people to visit each week, and we have many, many, many more users.

Now, you could argue many different -- there are many different points that one could make from all we have is sort of the data we can offer, but it also may be that this is something that users probably don't necessarily interact with on a regular basis, right. I think that if we do this right for a lot of our users, it's the kind of thing where they'll set their privacy preferences or controls in a way that they feel comfortable and then not have to think about it again until they've changed or they're interested in it.

So I don't think we necessarily expect a lot of recurring traffic to the site, but others will draw other conclusions.

On the question of sensitive information, I think this is a really important area and one where there's probably -- where guidance from the Commission has been helpful and probably will be helpful in the future, so, for example, for our own -- and again this is all within the narrowed context of our own interest based advertising, product and others have done similar things in different ways, we don't use signals about certain categories of sensitive information that we believe aren't appropriate to use for that kind of targeting.

So health information, information about, for example, sexual preferences, information relating to children, certain categories of financial information we don't use, and there are others who are more expert if you wanted to dig deeper about how you un package those.

Defining those is really important. I think we also heard in the earlier panel about some of the reasons people might want to do that. We've made a choice not to. In this context we think that's very important. We think that's appropriate for this kind of advertising regime from our perspective. Others may

feel differently, but I think this is an area where clear guidance from policymakers to set a baseline of understanding users would be helpful.

MS. GARRISON: If I can just push on that a little bit to understand better, when you say, for example, health information, if someone did a search for Alzheimer's.

MR. DAVIDSON: You will not see --

MS. GARRISON: Are they used and/or not used?

MR. DAVIDSON: Well, and you would see, and anybody can go look, and we hope you will go look at these ads preference manager. You can search for it on Bing and it will come up actually, but the fact is if you look at the category -- this is the easiest way to know this, if you simply look at the categories that you can make choices about and that you can see, you will not see something that says Alzheimer's patient. You will not see anything that's even close to that.

And that's the most important way we can show people directly. I think this is the power of this, of these kinds of approaches is that people should be able to see what it is exactly ads are or other -- what other kinds of information is being used about them. As Jules said, this was heresy a few years ago, and I will say that when we first talked about it internally, it was

heresy, the notion that we would show users what it is that we're using to target an advertisement to them? Could we do it? Wouldn't they be freaked out if we did it?

And I think what we've hoped for or what we've -- I guess the reaction that we've gotten is we think actually users are pretty mature about it, and some of them will be freaked out about it, and that's appropriate for them, but some of them actually have had a totally different reaction to it, but this is just one small step in the market. It's a relatively narrow part of our business, but I think it's a good example of what could be done.

MS. GARRISON: Thank you. Alan Westin, you've done some work in the health area in terms of consumer surveys, I think personal health records in particular.

What have you found about consumer's attitudes with respect to their health information as opposed to say just buying a toy online?

MR. WESTIN: Whenever you ask people what's the most sensitive information about you that could be collected and used, health information and financial information are always the winners. We've done a number of surveys on how the public feels about the emerging electronic health record movement, and also personal

held records, and in general when we've asked people: Do the privacy risks outweigh the benefits that you see electronic health records bringing to healthcare and to your care or do you think that the benefits outweigh the privacy risks, we get an absolutely 50/50 division in the surveys we've done.

So half the people feel it's the privacy risks outweighing the benefits and half believe the benefits outweigh the privacy risks, but I think that as electronic health records are now unfolding throughout the healthcare system, trust in the keepers of that electronic health records is absolutely central, and we see that it's only when promises are made and explained as to limits on who will get to see a health record without your explicit consent or data security will be provided to make sure that data breaches of health information, which are much in the news lately, will not take place.

Will the people that we survey feel they're comfortable with and trust the people running the system? And I think there are a lot of quotes from the top levels of the electronic health record officialdom then that without trust, the advantages of electronic health records will never be achieved because people will not willingly give their information or subscribe

to health research using their medical records with explicit notice and consent, so I think there's an absolutely central aspect of the whole personal health record and electronic health record developments.

MS. GARRISON: Thank you. Joel Kelsey, are there other areas that consumers are particularly concerned about or sensitive about the use of their information or disclosure to others?

MR. KELSEY: Well, I think financial and health is absolutely the top two, but I wanted to go back actually to what would -- if consumers understood the true difference between first-party and third-party kind of data collectors, would their behavior change? One of the things that we found is that they're absolutely aware that companies are tracking their behavior online.

They're uncomfortable with it, and they take steps like protecting anonymity and things like that, but going back to the beginning of the panel, we also found that they do that, and that cost benefit analysis in their head leads them to a particular choice, largely also because they're confident that there's some kind of government protection if the data collected about them or is being used about them goes too far.

So I think I would ask the question a different way in that: What would consumer behavior look like if

they, A, knew what third parties were able to do with their data, ad networks, data exchanges, collecting demographic, geographic information, financial transactional information, and pretty soon that starts to be combined and looks pretty close to PII.

So if they knew that on one hand and also knew that there wasn't a whole regulatory framework to protect them from bad uses of that, not necessarily to target ads but to maybe hold back financial offers on mortgages, on credit cards, on travel, things like that.

I think their relationship to first party sites then would very much then change, and I think one of the things we have to address and one of the reasons I'm glad the FTC is having this debate is there's really this kind of growing tension I think between the usefulness of display information and display advertising that is going to require -- the financial incentives in the market are going to require information be collected as it gets closer and closer and closer to PII in order to target information more.

And I think that we really absolutely need fair information practices to start talking about what that information should -- what kinds of information should and shouldn't be collected and ultimately how it should and shouldn't be used.

MS. GARRISON: Jules.

MR. POLONETSKY: Just a quibble because we all throw on this third-party thing online in this unique way, and if we actually explained it to consumers, they're minds would explode, so I'm not sure any consumer would choose UPS over Fed Ex based on the fact -- unless they cared about the labor issue, that the Fed Ex folks were contractors technically and the UPS folks were employees.

They care that someone was in control and someone was responsible, and I think what ends up happening online all that much is that we can see some of these third-party things because the technology makes it visible, and whether or not it's really someone else who has a right to do something with it or whether it's just a technology that is completely under the control and because of the nature of the contract, their first, their third.

So we throw around third. We throw around first in ways that I think people would have no clue, and it would make them melt down if they said, Hey guess what, the website you've gone on is actually operated by someone other than the person who actually owns it and it's stored somewhere and it's hosted somewhere, so we ought to focus a little bit more on who's accountable

and who's in control, who's responsible for what's going on and do they have a right to do something with it?

Now, there's users that are a bit guilty because we have lots of folks who are kind of vendors who also seem to have the right to do stuff with data, and so we've created the confusion, but still I think we need a little more clarity here so people -- so to when we try to communicate with people, we actually tell them things that are meaningful that they might actually make decisions based on.

MR. OLSEN: Adam, I wanted to raise a question for you and give you a chance to respond to what's just been said as well. I think you mentioned the real world scenarios that exist every day, and I guess the question that I have is: If you were to do a study where the full extent of the trade-offs were made known to consumers, could you do that? And this goes to Jules's point a little bit: Could you provide adequate information that consumers would understand that would reflect the sort of trade-off that's going on everyday?

MR. THIERER: Well, it would help in an experimental economic sense if we had consumers bargaining with something that approximated their own money and their own real time, and obviously gave them access to other types of relevant information that is

often missing in some of these polls and surveys, like what other types of tools do you use that might be privacy enhancing that would change the equation?

Why is there no mention in surveys and polls of things like Ad Block Plus which has 67 million downloads in the last five years on Firefox and is the number one most downloaded utility in Firefox history. Number 2 by the way is No Script, another privacy enhancing or security based measure.

So people are obviously doing something. Now, maybe Firefox users are an especially unique class. The point is that in the real world they take privacy enhancing or security enhancing steps, so those are the kinds of things that I think need to be worked into surveys and polls, but again that's not going to substitute for what happens when people actually make a choice in the real world.

I'll just go back to the social networking examples and some of these others. I mean, information flying around on networks that just would have been unthinkable to many of us a generation ago, not just a generation, just a few years ago, and to some of us still raises sensitivities. I'm really concerned about what my kids put online, and I take steps to try to minimize it and teach them why they should think through

that decision. So I just think those things need to be taken into account.

MR. OLSEN: I wanted to raise a question that came in from the audience, and I'll paraphrase it a bit. There seems to be considerable support for the view that consumers may not be fully informed as to aspects of data flow and what happens to the data, not withstanding some evidence of deployment of Ad Blocker Plus and other tools.

Given the lack of information that consumers have about the benefits of certain activities, should we really care about attitudinal evidence about what consumers may or may not feel? In other words, do attitudinal surveys really matter if there is an information deficit? Alan, you wanted to make a comment?

MR. WESTIN: If you lay the consumer privacy surveys along side larger surveys of consumer knowledge, it's quite consistent. Consumers are ill informed about financial affairs, investments, about home protection, about medical affairs and so forth, so the base has to be that we have a largely uninformed majority consumer population in the country.

The second point would be that most consumers then get their signals from the organizations that they

trust to tell them what to think about and what to do in that situation. So it would be consumer organizations or business organizations or ideological organizations or the AARP, et cetera, and if that's your model, then you say how can you make privacy relate to that?

The other point I would make is that studies that we've done show that the American public divides into roughly three groups when it comes to privacy: About 25 percent are intense, will reject benefits and insist upon strong privacy protection. About 10 to 15 person are privacy unconcerned. They couldn't care less because the benefit is fine for them, and they're not worried about their privacy, and I would like to say that for ten cents off they'll give you their family history or anything else you want.

In between are the privacy pragmatists who say, what is the benefit to me, what are the privacy risks that are presented, how do you propose to inform me and give me some choices on that, and fundamentally do I trust you or do I think that only law and regulation will make me comfortable in this situation?

So when we talk, as we've been doing this morning, about the consumer, I think it's useful to see that there's a pattern that the American public divides into, which has been shown over 20 years of surveys to

be a repeat in terms of the way in which the public divides on these issues.

MR. OLSEN: Joe, do you or Lorrie want to add anything to that given the framework?

MR. TUROW: Yeah. I think that on a number of levels you can interpret the data that we've collected. It's true that attitudes can be critiqued as simply a point in time, but we've also collected a lot of data about what people know, okay, in relation to those attitudes, and what they believe in terms of what the government does, and if you lay those things one on top of another, people who know very little believe the government does a lot and are very nervous.

We even asked the question: If you found out that a company is collecting your information illegally, what would you do? And aside from the monetary amount, we asked them what would you do to executives? While something a little over 30 percent said they would get the company to train people, teach the people in the company about privacy issues, I should say outsiders privacy issues, a strong percentage wanted to put the people in jail, the executives in jail, and I think it was 18 percent wanted to shut the companies down.

Now, I don't think that if people were on a jury they would really do this, but I think what it does do

is it shows a kind of frustration and anger that people have about these sorts of issues, even while they believe that many companies are doing the right thing, whether or not they know. I mean, they think the U.S. government is doing the right thing, meaning protecting their privacy.

One more point I would like to make, which is we have done four times -- asked the same question, true, false in this sort of way. If a website has a privacy policy, it means that that site will not share your information with other sites or companies without their permission. In fact, every time we've asked it, 75 percent of the people get it wrong, that is, most Americans don't realize that the word privacy policy doesn't mean that a company will protect your privacy in terms of not sharing your information, and it seems to me that label is defective and deceptive, that it really doesn't mean what most Americans think it means.

MR. OLSEN: I want to move on now to disclosures a bit, and I'll note, Jules, you described what you and WPP have worked on. Alan, you have talked about the Google ad preferences manager. We've heard discussion about Yahoo's new efforts, I think AT&T new efforts as well, to bring additional transparency to information management practices, and I guess one question that that

raises is how usable, how feasible is it to have these multiple different systems available, depending on what service you visit to manage your privacy, and is this something that consumers will really be able to navigate going from one site or one service to another.

MR. POLONETSKY: Well, I think the answer is industry groups need to adopt and standardize, and if they're going to have real meaning to the self regulatory programs that have been hammered out, the final step needs to be adopting a good standardized way so that every time a user sees something, it means your data is at work, and then perhaps different businesses may do different things behind that.

They're different models, there's different features, but that that paradigm is the thing that indicates, see, this is a smart interaction, and let's be a little broader than behavioral advertising because it's not the entire world, right? Data is being appended. Lots of folks talk about behavioral advertising and don't include retargeting and re marketing and there are billboards that are interacting with me and there are screens, and we're in a world of smart interactions.

And will users understand it's not just click, I've paid and I've been charged, but I'm getting

something different than the person before, this is being used in some robust use. I would like the fact that my local Giant again in Potomac where those folks are looking to meet me is now giving me coupons as I use the scanner and I work through the supermarket and I am wondering -- I looked at the coupon that popped up, and I wasn't in the aisle that had the orange juice, and I was wondering: Is it because they know my shopping? It would be useful if that was or if they knew where I was, but I was like, I have no clue, and if I simply saw sort of a symbol whether or not which dashboard was behind it, I would get it, this is -- I want to use this or not based on whether I want to know who knows about my shopping and whether I find this of value or not.

So I think industry adoption and industry putting rules behind it that this is what it means. It means TRUSTe promises this, BBB is asserting this is essential.

One effort by a couple of companies, by FPF, by WPP will be nothing. If we're going to move the vast majority of people and get it on the radar screen of their consciousness, it needs a broad effort.

MR. OLSEN: Lorrie, did you want to comment to this?

MS. CRANOR: Yeah, so we've done a lot of work

at Carnegie Mellon looking at how to communicate with people about privacy and on privacy notices, and going more broadly than just the behavioral advertising, looking at the privacy notice in general, and we found that the traditional English language privacy notices is completely un penetrable to most people, and we've done studies where we ask them basically reading comprehension questions as well as see how long it takes them to try to figure out will this company sends you postal mail advertisements, like people read a privacy policy, they can't figure that out.

So we've tried a number different formats including the layered notices format. We've tried some things that my students have come up with, and what we found is that if you move to something that is closer to what we call the nutrition label, where you have this very simple format, that everything is always in the same place, then suddenly people are able to actually use it and derive information, and you can give them these policies from two companies, and they can compare them and tell you what's different.

And we tried a variety of these formats, and actually the gains from did you put it in paragraphs, do you put it in tables, you get little gains here and there, but the key thing is that they're standardized,

that the two companies both used the same format, and that's where you get a really big win.

MR. OLSEN: Are there particular elements that you think consumers are most interested in and would it be, I share information with other unaffiliated companies, for example, or are there other things that are more important when you talk about a nutrition label that should be included?

MS. CRANOR: Yeah. So we've looked at the survey work that's been done over the years by many people, including some of them at this table, and it seems like some of the hot buttons for people really have to do with information sharing and the secondary uses of their information, and then there are particular sensitive data types that are also hot button as well.

So in the nutrition label that we came up with, which you guys can all check out at Privacyfinder.ORG, you can do a search and any website that has a P3P privacy notice, we automatically generate a nutrition label for them, but anyway, we have tried to highlight some of the areas that do seem to be more hot buttons with consumers.

MR. OLSEN: Alan, did you want to jump in here?

MR. DAVIDSON: Yeah. First I want to tackle something Jules said which is just that to the question

of whether this is feasible, I think in some ways we don't necessarily know, but what we know is that industry is going to really have to get together to do more together, to address some of these issues.

So, for example, I mentioned the persistent opt-out that we created for our own interest based advertising offering, and I think one of the biggest legitimate critiques of it has been that it works for Google, but what does a consumer do for all the other information out there?

Now, the great thing about it is we released it in an open source forum, and an intrepid young hacker who will remain nameless but is in the room actually took it and made it something that users -- that would work for a large number of other advertising networks, and that's great. That's the kind of thing we need to see more of and to do more of.

But I think the fact is that there's a giant challenge here, and to your earlier question about whether these attitudes matter on the part of consumers, they absolutely matter, and I think they're a strong signal to all of us in the industry that we have to do more and do better here. It's a business imperative. It's difficult. I don't want to sugarcoat it because I think you can look at Lorrie's fantastic work on the

nutritional labels and realize how hard it is because it's not like vitamin A.

We don't have a recommended daily allowance of these things, and they're not objectively measurable in a lot of ways, so it's going to be very difficult. I looked at her great paper again this weekend, and if you look at the label that I think -- one of the labels it didn't include location information, right? This is a dynamic environment. There's new things happening all the time, so the nutritional label is hard, but we have to find better ways to communicate with people.

MS. GARRISON: In addition to a standardized format, is there something more that can be done with respect to delivery of the information? I mean, typically right now you have a link at the bottom of your opening page, which just says privacy policy or privacy notice, and we've heard from Joe about what that means to many consumers.

So how can we make the disclosure more effective? How can we have better transparency in terms of delivery? Does anyone want to take that on. Jules?

MR. POLONETSKY: One of the things we tested was what happens if you mouse over the disclosure and you get a simple sentence that says, here's what's happening, and people gob that, even though 15 minutes

before they had very little concept of behavioral advertising, a simple brief sentence, and then go ahead and find out a lot more.

So I think that is in some way consistent with where the self-regulatory regime focused, don't point this to your privacy policy, point it to something that is relevant to what's happening here, and so again to get back to my point about featurizing, I don't think I've read -- I probably have read the Amazon privacy policy, but I think most of us may not have in the real world out there, but yet we know that books are being tracked and we're getting books based on the books that we've done because it's in context.

It's relevant to what I'm doing, so I think that's the feature we need to crack, how do I not give you the policy that my lawyer will insist has every caveat and everything in every case. Can we, the legal folks and the consumer protection folks over the world give a little bit of leeway so someone can say something and give users the gist. The gist is never going to be exactly accurate, and it's not going to have the 18 caveats, but if we don't give them the gist, then we have no hope of -- one of the very interesting thing from the focus groups was we tested a particular phrase, why this ad.

And what users said to us was I get what that means, but why are you asking me questions and then making me click to go find out what it is. They said, if you've got something to tell me, tell it to me here, and then I'll decide whether I want more information, and so you have to kind of avoid a little bit of, here's what you should want to know right now with actually testing and hearing what they had to say.

It was remarkable to me because I thought that that would about the obvious term, but they said, tell me, what do I have to click and come back, and maybe I won't be able to come back, there will be a pop up, my browser won't work. Let me know whether I want to know of something, and then I'll move on.

MS. GARRISON: Consumers are a lot smarter than we give them credit for, I think Joel, do you want to pick up on this?

MR. KELSEY: Yeah. Well, I think one of the things that would be interesting to talk about would be if every time data is appended to an existing profile that exists within -- with running the risk of being ambiguous I will say third-party data collector, most ad networks, ad exchanges, so every time they append new information they've either collected or bought to an existing profile, it would be interesting to see what

that looks like, how close it comes to being able to come to actually point to which consumer the information is being collected from, and then making sure that those consumers have access to any information that's being collected about them.

In going back to I think the distinctions that need to be made and what information consumers care most about, I think Google and Yahoo should be commended for trying to be more transparent in adding some types of transparency to the marketplace, but I think consumers do actually have -- there's a difference in the consumers' brains I think with regard to Google or Yahoo as a search engine and Google and a Yahoo as an ad network, and the Dashboard I don't necessarily know makes that distinction and lets them kind of understand how that information might be used differently when they're off of Google's properties or off of Yahoo's properties.

And I think everybody has actually said this as well is needing consistent information or consistent -- the need for consistency with regard to transparency is absolutely crucial, and I'm not sure that the companies that are collecting the data have financial incentives to be consistent across the board, and so that I think calls again for getting away from this notice and choice

model which I think has clearly failed because we don't have clear disclosure and two some type of regulatory framework or national standard that will give consumers consistent information upon which they can make marketplace decisions in a rational way.

MR. OLSEN: Joe? First Joe and then Adam.

MR. TUROW: I just wanted to second what Jules was saying, and actually Joel now too about the point -- it's very important, it seems to me, to know what's going on at the point of the ad being served because so many things are happening now that may not be, for example, Yahoo doing it or even the site publisher.

There may be a network that bought a particular person in real time. Right now what's happening is more and more people are dynamically served in real time based upon ad exchanges, and so you're literally buying individuals or at least individual consumers' computers rather than clusters or space or time, so that makes the challenge much greater, but it also I think makes it very important to say you're a dynamic person. Your profile may not be what's in some back page somewhere. It may be available at that moment for that particular purpose.

MR. OLSEN: Adam?

MR. THIERER: Let me sort of cut to the chase

here, I know we're short on time here, and get to what I think is the ultimate issue at stake here. We're talking the need for more information, more disclosures, more transparency. Everybody agrees that's generally speaking a good thing for consumers, but how we get there is what's the real challenge, and we have to ask the question if we're going to allow ongoing experimentation with disclosures and dashboards and privacy tools and settings and so on or if we're going to foreclose that process with sort of a one size fits all model that says, well, this is the way we think it should work and work forever more.

I think we've all lived through this in this town when we've had debates about disclosures and things like product or information ratings for content in the field of child safety. I mean, we had a debate that many of us were involved in the 90s about, should we have a one size fits all with the V chip model for rating all television content.

I'm not here to say that didn't work out at all, but I think look at the model that evolved when we allowed experimentation in the Internet context, where you have myriad tools, a rich mosaic of tools and empowerment methods that exists there that don't exist for television. Those are two very different types of

models that we chose, and I think the latter one is something that has some lessons for us here, that we should allow and encourage more experimentation, more competition between these companies like what Google and Yahoo and others are doing for better dashboards, better information disclosures, better seals, so and so on forth. I say let a thousand flowers boom.

MR. OLSEN: One follow-up question on that point, Adam, which is: Does it make sense to have -- even in the context of experimentation, does it make sense to have certain things be consistent from one entity to another? And, Jules, you mentioned the Amazon example. Consumers may understand that information is being collected to provide guidance about books they may read.

Similarly, there may be certain expected uses of information that companies engage in. Do you need to provide consumers with a notice and choice or additional information related to the fulfillment of an order, for example, or to let consumers know that information may be used for fraud detection?

So one way of simplifying the information that's provided to consumers is perhaps to take some uses, expected or anticipated uses, off the table to reduce the amount of information that consumers are hit with,

and does that sort of approach make sense?

MR. THIERER: Well, I think a couple different questions there, but the question of whether or not we should have a standardized disclosure or should we have standardization of terms, and the problem is the terms and notions they involve. Again getting back to something Alan Davidson said, you look at some of the things that are out there that we're trying to measure or trying to deal with, take location based services and privacy surrounding that, things that have developed and come on the market very rapidly we didn't expect before.

I mean, I'm for holding companies to the promises that they make about the information they collect. I think that's really where we need to be about saying, if you promise to treat information a certain way, live up to your promises, but the question of taking a different approach of mandating, everybody apply to the same policies across the board, I think forecloses experimentation innovation in this field.

Information is the life blood of the Internet, and if we foreclose it through these sorts of regulatory regimes, I think that has profound ramifications for the Internet.

MR. POLONETSKY: It doesn't help industry not to

be working really hard not to figure out, right, if I got into a car and every car had a completely different set of controls, we would be in pretty big trouble, right? We have sort of worked, by combination of legislation and effort and consumer research about what actually works, such that at least my five year old, when she sits down and gets a new computer game, she can already kind of scroll her way around. She knows generally what different things do.

So I think we need to drive it, and we joked about people doing coincidentally things for today, but it's these sort of touch points that let the privacy folks in the room go back and say, look we have to do things by next week, by tomorrow because there's a bill, because there's a law, because there's a proposal, because the FTC is into it, so I urge you to keep the whip going and use the different tools to cajole because it's a messy ecosystem, and sometimes it needs a prod, and sometimes it's industry leaders, and sometimes it's you guys, so keep pushing.

MR. OLSEN: Joe, you wanted to make a comment?

MR. TUROW: I just wanted to say in response to something Adam said. We're not just talking about the Internet anymore. Television is becoming the Internet. All you have to do is look at what various television

cable networks and other entities are doing in terms of new ventures and Comcast lab experiments with collecting data, the same thing that we're talking about in terms of coursing people's data through the Internet is going, is beginning to happen in what we call television.

These words are now metaphors that are going to have less and less meaning over the next several decades. The other point is all the data we're talking about, this is peanuts compared to what's going to happen ten years from now, and it's not going to just be through advertising. Increasingly the news, the information and the entertainment you get will be varied based upon the profiles that you have.

And I think the issue here confronting us not now, not to make rash decisions, is how are we going to live in a society where those kinds of data get coursed under you without you knowing it and without you having any control about it? Do you want 60 Minutes to be different for your neighbor compared to what you see based upon what companies know about you and you don't? Okay. Do you want discounts to be different based upon what companies know about you and you don't?

These are small things that exist now but only in small technologically feasible ways. Add up some of the fire power in terms of the technology and it's going

to happen because the industrial logic points that way, and that's why I think we have to be worried about this stuff.

MS. GARRISON: Alan Davidson, I think you'll have the last word.

MR. DAVIDSON: Wow, what a responsibility. I'll go back to what the Chairman said at the beginning when he posed this question about: Is this the worst form of government except for all the others? And I would say actually maybe it is, and it's one of the reasons why we really have to get this right.

I mean, if ten years ago we had been sitting here and said there's going to be a website, there's a set of websites out there that will ask you to input all sorts of personal information, where you went to school and all of -- who your closest friends are, and we're going to share that information with hundreds or thousands of people including thousands of developers who develop applications, we would say that is crazy and we should prohibit that in terms of these prohibited practices, or that there are going to be location based websites that will ask you to share with all your friends where you are at any given moment, and they'll do the same thing. We would say, that's nutty, we should never let that happen.

It's a very dynamic environment, so I think we have to be careful. That said, there is a giant business imperative for us all to get this right. We need to work more closely together.

I would offer one challenge to the Commission, which is an area that we haven't talked about, which is how government gets access to information because one of the things I think consumers really don't understand is under what circumstances we all are forced to turn over information to the government. The Commission because it's both a law enforcement agency and a consumer protection agency has a very interesting role to play here I think to play in helping us all think about that.

Thank you for having us.

MS. GARRISON: I want to thank all of the panelists. This has really been a very provocative and interesting discussion. We could clearly go on for another hour or two, so there are many, many challenges ahead, but I thank everyone for their participation today.

(Applause.)

MR. OLSEN: Let me add one logistics note. We have a limited amount of food available out here. There is a list with local eateries outside at the registration desk. If you do leave the building to get

food, please keep in mind that it takes time to get back through the security, and we'll reconvene promptly 1:20.

(Whereupon, a lunch recess was taken at 12:18 p.m.)

AFTERNOON SESSION

(1:19 p.m.)

MS. MITHAL: Good afternoon, everyone. If you will make your way to your seats, we'll begin the afternoon session.

It's my pleasure this afternoon to introduce as our kickoff speaker Commissioner Pamela Jones Harbour. Commissioner Harbour is an internationally known expert on privacy issues, and when I say internationally known, I'm not exaggerating. Commissioner Harbour has been the senior member of the U.S. Delegation to the APEC committee that's considering privacy issues in ECommerce, and in that role she has been instrumental in drafting APEC cross-border privacy rules.

So it's our pleasure having her here this afternoon kicking off our afternoon session. I would like to call her up to the podium. Commissioner Harbour?

(Applause.)

COMMISSIONER JONES HARBOUR: Thank you, Maneesha. Welcome back from lunch and thank you for the opportunity to offer a few thoughts to begin the afternoon.

As many of you know, my time at the FTC is coming to a close. Throughout my term, privacy issues

have been among my highest priorities, and I'm encouraged that the Commission, through this roundtable series, is now engaging stakeholders in a holistic discussion of privacy.

In 2007, at the Ehavioral town hall, it initiated an important conversation by focusing attention on behavioral targeting, but even more importantly, the town hall raised the key questions that have since triggered a return to first principals as the FTC reevaluates the frameworks it uses to analyze privacy.

As part of its promise of change, the current administration has embraced technology and innovation along with a new era of openness, but real change cannot just be aspirational. It requires concrete action, and unfortunately, with respect to privacy, I believe action has not been a high enough priority to date.

Now, I certainly do not intend to criticize Representative Boucher's efforts to craft legislative guidance on behavioral advertising, but as I have previously stated, the United States needs comprehensive privacy legislation. If we continue the piecemeal approach to privacy in this country, we nearly push aside the underlying issues.

The privacy debate goes far behind online

advertising because behavioral targeting represents just one aspect of a multifaceted privacy conundrum. Data collection, aggregation and use as well as reuse, sale and resale are driving the creation of online and offline digital dossiers. Capturing data reflecting individual interests and habits is an enormous and growing business, evidence that consumer privacy is under siege.

Online advertising is an enormous source of information collected about consumers and serves as an important lens to focus our understanding of data collection and use. Most consumers cannot begin to comprehend the types and amounts of information collected by businesses or why their information may be commercially valuable.

Data is currency. The larger the data set, the greater potential for analysis and profit. Collection of consumer data is by no means new. Consensus information, credit reports and Nielsen data have existed for decades. The Internet, however, enables the creation of vastly larger quantities of consumer data.

This data are collected every time we send an Email, update status on a social networking site, read a newspaper article, run a search or make an online purchase.

Of course, these technologies have the potential to offer valuable benefits to consumers. The problem, however, is that many consumers are completely unaware of the privacy implications of these services which makes it difficult for consumers to exercise informed choices about the sites they visit and the data they disclose. In many instances, consumers pay for free content and services by disclosing their personal information.

Their data are then used to generate targeted advertising that subsidizes online activities, and I'm especially troubled by the asymmetry between consumer perceptions and business realities. If consumers do not comprehend how their personal information is collected and used, it is possible -- it is impossible for them to knowingly consent to either disclosure or use, and once data is shared, it simply cannot be recalled or deleted.

The cumulative consequences then for consumers are magnified whether they realize it or not. It is possible that small discrete disclosures of information do not raise concerns for an individual consumer, but large aggregations of data based on a lifetime of commercial activity might evoke quite a different response, and I fear that we might reach a tipping point whereby consumers decide they want to exercise greater

control over the use of their data, but their attempts to exercise this control become futile because so much of their digital life already has been exposed.

Industry attempts to provide notice and choice to consumers have been insufficient thus far, and I hope we all would agree that disclosures about information collection and use and control are not meaningful if they are buried deep within opaque privacy policies, and even if we can decipher the cryptic disclosures, they provide consumers with no meaningful choice or access, which renders those concepts largely illusory.

We have strayed far from the information, from the fair information practices that should serve as a baseline for any comprehensive privacy legislation, and all of this matters because consumer really do care about their personal privacy, and they are willing take steps to protect it.

The findings of the Turow-Hoofnagle legal report conclude that 66 percent of American adults reject tailored ads to begin with. That number increases to over 75 percent when consumers are actually educated about the relevant marketing techniques. Yet companies are not delivering the privacy protections that consumers prefer. Even when consumers have the ability to opt-out, the effects are limited. If consumer data

is unavailable from one source, often it can be obtained from another.

Flash cookies and other technologies largely circumvent cookie controls. For every company crafting a response that addresses notice, choice or transparency, there are several more companies trying to parse and evade the intent of Commission guidance.

We have entered a digital arms raise, if you will, and the outlook is troubling. Privacy issues are important enough that the Commission should use every possible tool at its disposal. During my term as a Commissioner, I've been immersed in both consumer protection and competition issues, and I have steadfastly argued that the Commission should apply its competition expertise in the privacy arena.

For example, when the Commission approved the Google Double Click merger in 2007, I wrote a dissenting statement that, among other things, highlighted the nexus between privacy and competition, and while my colleagues at the time disagreed with my premise, subsequent changes in the marketplace have reinforced the validity of my concerns as well as my premise that privacy protection is increasingly viewed as a non price dimension of competition.

My dissent proposed the concept of a market for

data itself separate from markets for the services fueled by the data, and the dissent discussed John Battelle's database of intentions concept, which he describes as the aggregate results of every search ever entered, every result list every tendered and every path taken as a result, and to Battelle asserts that no single company controls this collection of information, but posits that a few select companies have control.

And one of my key concerns in Google Double Click was that the merged entity might move closer to dominating the database of intentions, and that the network effects generated by combining two firms might have long-term negative consequences for consumers. In response to questions raised during the concurrent U.S. and EU review of the proposed Google Double Click merger, Google assured regulators that the deal was not motivated by a desire to enter the behavioral advertising market.

In March of this year, however, the company did in fact begin to engage in interest based or behavioral advertising, and last month, Google purchased global advertising company AdMob. This acquisition enhanced Google's ability to extend its advertising strategy into the fast growing mobile market, an important market and which I hope and I expect the Commission will remain

vigilant.

Turbulent economic times are forcing companies to seek out new sources of revenue. Those sources are driven in turn by increasingly large amounts of data as well as the ability to mine the various connections between pieces of data, and as firms continue to develop new database markets, including for example, Cloud Computing and Smart Grid Services, we must engage in more serious inquires regarding both the privacy and competition issues that effect consumers.

It is worth noting that to the extent one might define a punitive market for consumer data, recent mergers have further concentrated the competitive landscape. It may also be the case that Comcast's announced acquisition of NBC from GE should be analyzed from both competition and consumer protection angles.

In any event, competition on the basis of privacy protection is likely to increase as consumer awareness grows. The issues raised by data collection and use provide ripe opportunities for companies to develop pro consumer privacy tools and to market these features to distinguish themselves from their competitors.

In conclusion, I know the Commission will continue to be the thought leader on privacy, and I will

continue to do my part to push the Commission, as I have done for six years now, by challenging mainstream opinions and asking the tough questions, and wherever the conversations may lead, I am proud of the efforts of the very talented FTC staff, and I am extremely gratified that we have reached the point where we are hosting these roundtables today.

Thank you very much.

(Applause.)

MR. SMITH: I've been asked again to give a brief introduction to the afternoon sessions here to give a technical background of some of the more types of data collection that goes on.

In particular, we're going to have an upcoming panel here, discussion of online behavioral advertising, and so the first quick summary I'm going to provide is the technology behind behavorial advertising.

As we all know, this area has a good bit of controversy about it, and a couple years ago there was a whole workshop by the FTC on behavioral targeting and behavioral advertising. At the time I did a much larger presentation on the technology behind this type of advertising, and I'll give sort of an abbreviated version of that.

The key thing is: What is behavioral

advertising as compared to contextual advertising? The key thing I think as many of us know that is that in behavioral advertising, we create profiles based on people's use of the Internet. Over time we look at what new stories they're reading, what they're searching for, perhaps what they're purchasing, and we provide ads tailored or targeted based on the use of the Internet.

Contextual advertising, on the other hand, is more like the yellow pages where you show an ad next to whatever the content is, an ad related to the content and it's much less related to a particular person.

The way at a high level view -- again this is a high level view, there may be companies out there that do things this way or do it other ways, but I have a chart here on the screen that shows some of the pieces that go in to building a behavioral advertising system.

We have our consumer here down on their personal computer. They're surfing the web and going to a news website, which provides them news articles, and this could be any website, the New York Times, Washington Post, Wall Street Journal, anything like that, and they're reading an article. Along with that article, of course, we see the banner ads that come along with the article.

And in a behavioral advertising system then, the

ad network provides the ads, not the news websites themselves, but instead we have external ad networks, and what's important here, the data collection device that goes on in behavioral advertising system is based on cookies, so that over time, it can track a person through the web browser cookies, and that's something that the ad network gets as part of the browser that they're running with.

The key piece of information that they're looking at is information that comes in a URL that describes in some way the article or activity they're doing at the website, and then that information goes into a profiling service of some sort, and this is the engine that creates and discovers and builds the profile and provides back what kind of ad you could potentially be interested in. They're called inter segments in industry terminology. From those inter segments then, the ad network will supply an ad, send it back to the browser.

Some other inputs into the profile though can be the news website if it has registration associated with it. Information such as your Zip Code, your age or your profession can be fed also into the profile, and I've actually seen that happen in certain circumstances. That information sometimes goes to the browser, and it's

actually possible to observe that.

Other inputs into the process can be advertisers themselves can provide information about passed purchases and have that go into a database and also be part of the targeting process, so we have a very complicated and sort of wide ranging set of players here providing data for a profile.

In addition, the ad network that does profiling can also choose not to show their own ads, but then have, using what's known as a redirect, send a redirect URL to a person's browser, have that bounce off and then have yet another ad network provide ads too, so it's a very wide ranging set of players, and another group of -- another type of vendor that's in this process are the web analytics providers, whose job is solely to look at what you're doing at a website and then providing information directly to the main website, which then also can drive advertising into the systems.

It's possible to observe this all inside of a web browser, which is something very interesting. A lot of data collection that we see in this world is done behind the scenes, but because of the way the technology is, the way the Internet works, it's actually possible for tech savvy people to observe a lot of these activities. It's a little bit different than the

offline world.

In the offline world we only kind of the results of the tracking within online behavioral advertising or advertising in general on the Internet. We can actually watch all this take place.

So we're having a panel shortly here that will talk about this, go more in depth. I do want to talk about one other data collection system, which a lot of us are familiar with, and this is sort of the offline version of, if you will, potentially of behavioral advertising, which is the reasonable loyalty card. They became commonplace maybe about 15 years ago, and what they provide is a way for online -- or sorry, offline stores, regular stores, retail stores to do tracking over time.

And so with a retail loyalty card, it's something you apply for. So you sign up and you provide your name address and phone number and possibly an Email, and that information then is provided to the retailer, and they give back in return this loyalty card, which every time you go shopping, you present that at the cash register or many of us are very familiar with this, and that's basically provides that same technology as a web browser cookie where it provides a persistent identifier that can be used for tracking

people over time.

The retailer then will provide back to the consumer various coupons and special offers and advertising based on their purchases over time, and that information is derived from the purchase history as well as the loyalty card.

What the consumer probably doesn't see in the background is all the things that are going on with that data, and one thing is when you get coupons, those are actually forms of advertisement which the retailer gets paid for by whoever is providing the coupon, so it's a form of advertising, and there's targeting criteria when an ad is created to match it up with individual consumers, and that's based on the profile that's created by the retailer in a data mining engine.

Then information about purchases also are used by marketing departments to look at product trends, what products are hot in one part of the country versus another, what products are purchased in tandem, what products over time seem to be purchased together and so on, and all these drive various kinds of advertising decisions made by companies as well as product development decisions by companies. So in this process, there's many uses of that data that go on besides just providing coupons.

Another very interesting aspect of this process too are the data vendors because one of the things you can do is once you get somebody's name and address, you go to various vendors and get more data on people and get estimated household income, estimated household size, and that information can then be added also into the profile and used for targeting purposes.

So with that we'll get started on online behavioral advertising. Thank you.

PANEL 3: Online Behavioral Advertising

MODERATORS:

PEDER MAGEE, Division of Privacy and Identity Protection, FTC

MICHELLE ROSENTHAL, Division of Privacy and Identity Protection, FTC

PANELISTS:

JEFF CHESTER, Executive Director, Center for Digital Democracy

DAVE MORGAN, CEO, Simulmedia, Inc.

MELISSA NGO, Attorney at Privacy Lives

ZOE STRICKLAND, Vice President, Chief Privacy Officer, Walmart

BERIN SZOKA, Director, Center for Internet Freedom, The Progress & Freedom Foundation

OMAR TAWAKOL, CEO, BlueKai

CRAIG WILLS, Associate Professor, Computer Science, Worcester Polytechnic Institute

LINDA WOOLLEY, Executive Vice President, Government Affairs, Direct Marketing Association

MR. MAGEE: Good afternoon, everyone. My name is Peder Magee, and with me is my co-moderator, Michelle Rosenthal. On this panel we're going to be discussing online behavioral advertising.

Just a quick reminder, if anyone has questions, you can fill out a card and give them to one of the FTC people in the room, or if you're watching online, you can submit your question through an Email to Privacyroundtable@FTC.GOV.

Let me introduce our panelists. We have Jeff Chester, the Executive Director for the Center For Digital Democracy; Dave Morgan, CEO of Simulmedia; Melissa Ngo, who is an attorney at Privacy Lives; Zoe Strickland who is Vice President, CPO at Walmart; Berin Szoka, who is Director, Center for Internet Freedom, The Progress and Freedom Foundation; Omar Tawakol who is CEO of BlueKai; Professor Craig Wills who is a computer science professor at the Worcester Polytechnic Institute; and Linda Woolley, who is head of government affairs at the DMA. Thank you all for participating.

Just to set the scene for the behavioral advertising discussion, I'll give a little background. The FTC held a town hall event on behavioral advertising in the fall of 2007, and we followed that event with a set of proposed principles to guide industry, self-regulatory efforts. In February of this year, the Commission issued a report discussing the comments we received in response to the principles and setting forth revised principles.

Over the past two years, we've seen a number of efforts by industry to improve transparency and consumer control. At the same time, however, there's evidence that consumers are concerned about the privacy implications of online behavioral advertising, and a number of consumer groups have called for legislation.

What we're going to talk about now is behavioral advertising as we've defined it, and that's the tracking of consumers activities online in order to serve targeted ads. We're also including in that definition retargeting where someone visits a website, and the website sends on ad based on another website based on the prior visit. The definition does not include contextual ads which Richard mentioned or first-party ads or other purely first-party uses of data such as mapping the site traffic.

So let's start out talking about the consumer benefits that are associated with behavioral advertising, and I want to direct the first question -- and let me just say, this is an interactive discussion, so panelists, please weigh in. Even though we may start with one of you, everyone is welcome to weigh in. Just raise your little name triangle, and we'll call on you.

Berin, you've written about how online content, things like news sites, social networking sites, search

engines and blogs are free to consumers because they're supported by ad revenue. Do we know how much of the free content is made possible by behaviorally targeted ads as opposed to contextual or non targeted advertising?

MR. SZOKA: I know Omar is going talk a little bit more about the technologies involved and the fact that the lines are actually very difficult to draw, but if you take a big step back and you look at advertising generally, you would realize that it's not just that these things can be funded by advertising. It's that they have to be, and this is actually not inconsistent with the history of media in this country, that media and content such as you've mentioned are all things that people are generally unwilling to pay for because, as we all know, information wants to be free. It also wants to be expensive.

So back to colonial times, to radio, to newspapers and to television, it has been advertising that has supported content throughout all of those media, and today advertising is supporting both content and services, ranging from search engines to applications on your mobile phone or your computer, and if you look at what behavioral advertising is funding today, you have to think about it in two senses.

Behavioral advertising as the industry usually talks about it as a product is a fairly narrow and specific category, and it's something like a billion dollars today of the $23 billion of online advertising revenue.

If you look at behavioral advertising more broadly, as Omar will talk about, you realize that the techniques that are involved that could be affected by regulation affect a much larger percentage of online advertising, but today online advertising for display, that is for publishers who are relying on advertising is about $7 billion, and just to put that in perspective, that's about what the three national newspapers earned in advertising revenue in 2007.

And to put all this conversation in perspective, what we have to realize is that while many people think that we're in a privacy crisis, we're also in a crisis about how we fund media and content in this country, and the best indicator of that is the fact that as a share of GDP, advertising is down 25 percent from 2000.

So the challenge here from my perspective is: How do we make advertising produce more revenue for more publishers so that it's a more reliable source of funding? And the answer to that question I think is exactly what you asked. It's that unless you're able to

use those techniques of behavioral and other targeting to tailor ads better, they aren't worth very much, and they aren't worth very much to particularly smaller websites and sites that serve non commercial content, because if you limit it to doing contextual advertising, you are limited to having basically ads targeted based on the key words that are on your pages, which means that if those key words aren't worth very much, your advertising isn't worth very much, and the quality of what you can offer is very limited.

And if you're offering video or other kinds of content that don't lend themselves easily to algorithmic targeting of key words based on context, your advertising content may be worth next to nothing.

So I think the central challenge here is to figure out how we fund media content and culture in the future, and I think the answer to that is better tailored advertising that is more reliable for publishers because it's not an option. It's a necessity.

The simple reality is that paywalls and subscription based content and micro payments don't work. We've been there. We were there in the 1990s, and that world collapsed, and it collapsed because the proliferation of choices and because people aren't

willing to pay for something that they can get for free elsewhere.

MR. MAGEE: Jeff?

MR. CHESTER: The Commission has embarked, and it's kind of a distinct conversation. It's an important one when one talks about how to fund serious journalism investigative reporting. There's a conversation we had here last week that FTC has now launched an initiative on those behavioral advertising panel, and I think that when it comes to journalism, I think many of us are extremely sensitive about the need to fund it.

There's no reason why we have to engage in any kind of trade-off for our freedoms in order to save journalism. There's no reason why you can't have a system of online advertising, interactive advertising, especially conducted by the news media that in fact is citizen friendly.

So it's a false dichotomy here, and the fact of the matter is there are alternative models, and anybody in the industry will tell you that it's going to be a combination of online advertising and subscription and donation, et cetera, and let's not also equate the Internet with advertising because the two are interrelated but distinct.

I would rather us talk about the general issues of behavioral advertising, directed advertising than the journalism issue which does require a more distinct focus, unless you want me to start --

MR. MAGEE: No, that's all right. Berin?

MR. SZOKA: Just very briefly, this is really the essence of this debate is that some people think that privacy is a fundamental right and a monolith that is the same for all people and all users, and something that cannot be traded off against other values, and others, such as myself, think that the world is full of trade-offs, that every single decision we ever make in life is a trade-off, and we have to recognize that.

We have to recognize that in a world where digital economics means people are not willing to pay for bits because they can be generated elsewhere and their marginal cost of production is zero, this is what economics tell us. This is what we see in the real world. This is why free predominates.

In that world, this trade-off is of vital importance, so the challenge is to figure out a way to make online advertising work such that users are educated and empowered to make decisions about the specific things that they're sensitive about so that if they're concerned about one thing in particular, they

can hide that, and if they decide that they want to pay for something rather than engaging in behavioral targeting, they can do so, but not to set a one size default for everybody that reduces the amount of funding overall because that really, to reference what Professor Turow said this morning, if you want to talk about an industrial imperative, which he mentioned, let's talk about industrial planning.

Industrial planning is when the government comes in and decides how much revenue is going to be available to which business models, and that's a terrible idea and what's at stake is information, culture, content, services, journalism and media.

MR. MAGEE: Well, as far as educating consumers, you seem to be suggesting that consumers should be free to make a choice here, and I'm wondering what would be the impact if the choice was that the consumers had to give express consent -- Jeff, can I finish please? What that would mean to ad revenue, and in particular smaller publishers? Would opt-in consent across the board mean that publishers had to charge for their content?

MR. SZOKA: In a fantasy world, in an economist's fantasy world where there are no transaction costs, and we get to make all of our decisions with full information, and there's no limit to our time and our

attention, the answer would be that it wouldn't matter. It would make no difference. Opt-in and opt-out would produce exactly the same results, and this conversation wouldn't be worth having. We could just do it.

The problem is in the real world where we have trade-offs and limited time and limited information, these defaults matter hugely, and the reality is if you set an opt-in, you could end up having -- you could have ten percent or less people opt-in, and you could have exactly the same percentage of people opt-out, and it doesn't reflect people's real preferences.

What it reflects is the fact that people for many cases just don't care that much about what's at stake, and the hassle of having to go through the opt-in process is itself a huge cost. It is a barrier to entry that when we're talking about digital economics where the costs of production are zero, and there are so many choices out there, setting that sort of a threshold could be catastrophic, not necessarily for the biggest companies, the biggest players out there, but especially for the smallest ones.

So what's at stake is not just how much funding is available, but how democratically is it allocated? How well does it reflect the preferences of consumers? To what extent are consumers able to vote with their

intention -- is their intention actually going to be worth something in terms of what publishers are able to essentially sell it for to advertisers?

So that makes a huge difference, and it also makes a difference in terms of competitiveness. All the concerns that Commissioner Harbour raised earlier today talking about this landscape of online advertising and Google and all the companies involved, that landscape will become less competitive if we have restrictive regulations. It will become more competitive, and not only more publishers competing with each other, and among other terms, on privacy terms that they're able to compete, and if you set a default mandate, you're going to wipe up a lot of that competition.

MR. MAGEE: That's an interesting point, and I want to give some others a chance to weigh in here, but there seems to be a tension based on some of the studies we heard about this morning. It appears that a lot of consumers are very uncomfortable with the idea of being tracked online and having their behavior used to target advertisements.

I'm wondering how we square that, and Linda, perhaps you want to weigh in.

MS. WOOLLEY: Thanks, Peder. Yeah, I did want to weigh in on that point, and I think it's important to

talk about the state of the Internet now and what consumers are doing.

Right now, just right after Cyber Monday, some of the numbers are in, not all of them will be in until the end of December, but close to -- very close to 100 million people made online purchases on Cyber Monday. A hundred million people is one-third of the population of the United States. That is pretty significant.

All morning the conversation has gone around this idea that if consumers just knew, they wouldn't be doing -- if the consumer just knew blank, they wouldn't be doing blank. Consumers do know, and they know because there are things like the Google program. There's the Yahoo program. There are programs on every major browser that's out there that enable you to get rid of your cookies completely. You can opt-out of all of the major databases, data collection agencies that are out there currently. You can do private browsing on pretty nearly every major browser that's out there.

If you really are familiar with ad networks and you want to go to the NAI site, you can opt-out of all of those, so if you're of a mind to do private browsing and do everything anonymously, the tools are out there to do it, and as I say, I think we have to pay attention to that hundred million people who made online

purchases.

MR. MAGEE: I think that's a good point, but it also seems to put a lot of burden on the consumer to find out about these practices, which really are not that transparent. I think for the more sophisticated online user, perhaps they're aware of tracking and things like behavioral advertising, but I suspect for a large percentage of the population, they have no idea this is going on, and perhaps then would have no idea that there were tools to control it.

MS. WOOLLEY: One of the things that DMA has that we have had -- the Direct Marketing Association has had for a number of years now is something called DMAchoice.ORG, which actually is mail preference, but we are actively engaged in conversations about building DMAchoice out so that it includes online preferences, and I think that that really does have the capacity to be a global opt-out in a way that certain other tools that are out there are not.

The other thing is the issue of education, and we heard consistently this morning that there is a great need for consumer education, and we couldn't agree more, that there's a great need for that. You mentioned the principles that the FTC did in February. A group that DMA and others convened in response to those principles

also came up with a set of principles, and one of the principles was education, so I think that I think everybody agrees that more and better education is necessary.

MS. ROSENTHAL: Thanks, Linda. We're going to move in to some of the privacy risks associated with behavioral advertising, and we got a question from the audience, and I think it's an interesting question that might be able to frame the discussion a little bit. When will we admit that privacy is gone, that technology is too powerful and that consumers should be advised that once they opt into the Internet or use a mobile device, all of their info including health and financial info will be readily available?

MR. CHESTER: Well, I think that's a good way of starting it because, as I said, behavioral advertising as we all know is just one small part, and Pamela Harbour, Commissioner Harbour spoke about it. It's one small part of this incredible interrelated data collection apparatus for profiling, tracking and targeting. Very few consumers know about it.

The industry hasn't been candid with the Federal Trade Commission or the Congress. They haven't been telling the public the whole truth, and we're at a critical moment here because we have now seen the

emergence of targeting 2.0 as Professor Turow talked about and optimization, real time targeting, data exchanges. The so-called distinct silos are all collapsed, and you can buy offline and online data instantaneously and targeted, and none of the -- none of the hundred million people that participated online if they knew how their data was being collected, how their profiles were being created, how their ethnic information, how their sexual information, how their economic information, how their ethnic information --

MS. ROSENTHAL: Let me --

MR. CHESTER: -- was in fact part of the profile. They would begin to object strongly as they will --

MS. ROSENTHAL: Maybe you can talk about -- you mentioned that there are groups that are targeted based on age or ethnicity or race. Could you talk a little bit about that? Are there examples that you might be able to provide?

MR. CHESTER: Absolutely. Absolutely. Absolutely.

MR. MAGEE: Jeff, can I just stress that we're trying to have an interactive discussion. We're not giving speeches.

MR. CHESTER: I know we're not doing speeches,

but I also think it's important -- I told you this at the beginning. I think it's very important that the Commission convey to the public the people who are watching this perhaps online what the broader apparatus is here, not just reduce it to the payroll --

MS. ROSENTHAL: Absolutely, and the best way to do that is maybe provide examples of some of --

MR. CHESTER: I also think it's important to say what the industry is saying, and I want to read this very briefly from what the Winterberry report on interactive advertising apparatus from October 9, 2009, which I supplied to the Commission, just said: "Our contact information is now collected at virtually every step in a user's online experience. The registration pages, for example, and web surfing behavior is tracked down to the millisecond providing publishers and advertisers with the potential to create a reasonably complete profile of their audiences and this enables the matching of a user profile to enable robust segmentation."

MS. ROSENTHAL: Jeff, do you have an example of groups being targeted based on their age or race or ethnicity? We've talked about that as a concern. Maybe you could talk about that.

MR. CHESTER: Yes, I have. In the first place,

of course, the U.S. PIRG and CDT has filed, as I'm sure other consumers have filed, in this proceeding and over the last few years many, many examples of targeting of children and teens and persons of color, and indeed we're going to be calling on the Commission to open up a separate inquiry into how multi cultural communities are being specifically targeted here, Hispanics and African Americans, and --

MS. ROSENTHAL: Maybe we can get into another area.

MR. CHESTER: Listen, I can give you -- I brought many, many examples but, for example, if you want to talk about African Americans or if you want to talk about race, there are plenty of behavioral targeting networks that do that.

If you want to target Hispanics and you want to target Hispanics of X, Y, and Z behavior, you can do that all online. No person with -- no person has been asked, can we use the fact that you are on a Hispanic site or we've identified we think you're on a Hispanic site, no person has said they want that to be part of the target.

MS. ROSENTHAL: Are we talking about contextual or behavioral?

MR. CHESTER: We're talking about behavioral.

You can buy Hispanics. You can buy African Americans. You can buy kids. You can buy teens. You can buy anyone to target them all across online and social networks and no individual user knows anything about it, and if you want to see just one good example, a series of examples on how are youth are being targeted and how it's linked to the obesity crisis in this country, which is costing us billions of dollars a year, just go to digitalads.ORG, which is a site we operate about interactive advertising and youth obesity and see what the companies are doing, including many members of the IAB and the DMA.

MS. ROSENTHAL: Does anyone else have a response to that. Omar?

MR. TAWAKOL: Yes. A lot of the concerns he's talking about I would have to agree with which is there are certain sensitive topics that absolutely something has to be done about it, so, for instance, do you really want someone to know what potential disease you're researching are? Do you really want people to know what your religious preferences are, your sexual preferences, whether you like alcohol or gambling or porn?

There are a lot of topics that I think it's very clear consumers, A, don't know and they shouldn't be targeted for those, and there should be some sort of

standards about that.

MS. ROSENTHAL: We set those standards.

MR. TAWAKOL: Part of setting that standard, the way we approached it at BlueKai was to say BlueKai is not going to decide for you. We're just going to embrace the concept of complete transparency, so two years ago when we founded the company, before we went live with anything else, we went live with a tool that said if any data is ever going to be shared, it's going to be completely transparent in this tool, and it's going to be linked to by people who would work with us.

And so we're kind of letting the consumers decide what sensitive is after a minimum bar set by the industry, so a minimum bar would say, look, this is clearly sensitive to almost everybody, but beyond that bar, I don't think it's our position to determine -- what may be sensitive to me may not be sensitive to you, and the real solution I believe is to put a stoplight on it and to make it completely transparent.

Now, I understand that we came out -- BlueKai came out with a register before Google and Yahoo did, but who knows BlueKai out in the consumer world, right? So better than that, Google and Yahoo came up with one, so a possible objection would be, what if 55 or 500 different companies have these tools, how will consumers

know about them?

I agree that's a problem that needs to be solved with some more innovation, but I think transparency is the most important step that we can give to empower users to play with this because the comment that was made on the earlier panel was by the gentleman from Google, and we have seen this in our own data, is that when people come to use these tools, they don't opt-out in the percentages that you would expect. They end up interacting with the tool, and in our case they get charity for doing so, but the more important thing is if you allow innovation around transparency, I think it will help to clean up the behaviors.

MS. ROSENTHAL: Do you think that's going to happen on its own, or do you think that companies need an incentive in order to -- so, for example, whether it be a company being more transparent or actually defining sensitive data and staying away from sensitive data? Can they do this on their own or do we need to set some type of standard, whether it be through self regulation or directly?

MR. TAWAKOL: I do think sensitivity does require some standards. Now, I think the industry can create that, but somebody has to, and I would say that your, FTC's involvement and the government's involvement

in this issue has produced some good results. Now, I am a big fan of self regulation, but a little bit of a whip has helped in my opinion.

MS. ROSENTHAL: Okay.

MR. MAGEE: Let's give some other folks a chance to weigh in. Dave?

MR. MORGAN: The point I want to make is I think I'll sort of follow the question that had come from the audience, which is: Does opting in from the Internet mean that you opt-out of having your privacy protected? And I would hope all of us would agree clearly not, and that this notion that you're privacy is gone, get over it, that's not an appropriate kind of response.

However, a lot of what's happened or is happening out there is not in our control, and I think particularly if we look at the media driven marketing world, advertising as we know it, the Internet is changing and has changed fundamentally, and it will never be the same again.

Most of us certainly in younger parts of our life were part of what was a world where media was controlled by distribution. Analog media is all about scarce distribution, so you need scarce licenses, scarce printing presses, and it was quite frankly a vertically integrated monopoly, sometimes regulated,

sometimes not.

There were gatekeepers, and it was not very democratized and accessible. The Internet has changed that forever. Now, distribution is not scarce. Attention is scarce, and we have a world that has flattened out a lot. We have a lot of new practices we've never had before.

We have -- now that small market participants can play, we have lots of co-dependency with other companies, which brings in a lot of sharing of information and a lot of inter dependencies, a lot of inequitable bargaining powers between them.

We could sit and argue as to which was better, the big corner office in the media tower downtown or this somewhat crazy, anarchistic difference, but we're going to have to deal with it, and I think one of the most important things is that I don't think you hear from anyone in the industry that there's not a willingness to do a lot more, and I think having been here two years before, we've seen a lot of progress.

Clearly we're a long way from having a lot of answers to it, but I think ultimately to answer that one question, it doesn't mean people will have to leave privacy and we're going to have to find a lot of ways, combinations of industry, self regulation and government

support.

MR. MAGEE: Melissa?

MS. NGO: Yes. I want to go back to when we brought up the fact that this is putting a substantial burden on consumers to make these choices, and some consumers out there do have knowledge of what's out there. They have the knowledge of the data collection, and in the panel right before ours, I think Joel Kelsey said that the top two Firefox downloaded add ons had to do with privacy, had to do with blocking data collection, so some people out there are making these choices, but there are a lot of people out there who just don't know that this is happening.

You can have this conversation at any dinner party, and most people there will say, what do you mean that's being collected, I don't understand, what am I supposed to do? Putting the substantial burden on consumers is not the right way to go about it.

Let's again also talk about sensitive data because it's been brought up. When you look at the industry principles that just came out a few months ago they say that sensitive data is one, personal information of children under 13, and two, financial account numbers, Social Security Numbers, pharmaceutical prescriptions or medical records about the specific

individual, and also the principles do allow for the collection and use of the second category, financial account number, Social Security Numbers, medical information if a user consents to the collection and use.

Again this is a question about what happens in terms of does the user understand. We've seen what some of these privacy notices look like. They're confusing. They're long. There are a number of people who are very aware and very polished in terms of understanding these issues that really don't understand what some of these privacy policies even mean.

So that --

MR. MAGEE: Melissa, can I? I want to weigh in on that, the sensitive data issue. We heard a lot about that this morning, and it's a very challenging concern. It seems very subjective. What's sensitive to one person is not always sensitive to another.

In fact, I'm reminded of an example a friend of mine made the other way where he said -- he's bald, and he said that the fact that he uses Rogaine is not sensitive to him but the fact that his elderly grandmother does would be very sensitive to her, and I think it sort of highlights the fact that sensitive to one is not always sensitive to the other.

And because it's so challenging to define this and draw lines here, is another approach to look at it from the perspective of limiting uses of data so that you say, you can only use this type of data for the reason it was collected or perhaps limiting the amount of time it's retained or given consumers access to the data to see what someone has about them?

MS. NGO: Yes, we do want there to be focus on the fair information practices and the OECD principles of data collection limitations data quality, purpose specification, use limitation, as well as security safeguards, openness, individual participation and accountability.

And we can say that people will collect the information, they'll only use them for a specific purpose, but then we move into accountability. How do we know? How do we know that the data being collected and used is only being used for the specific way in which a consumer has opted into using it, and I believe that it should be opt-in, not opt-out.

MS. ROSENTHAL: Melissa, maybe we can talk about -- we were hoping to talk about some of the other risks involved, so in addition to sensitive data, what about the contention that some companies actually use tracking information to red line, and that's a term used

which basically means to discriminate, to offer different prices based on past browsing activities, so basically price discrimination, is there any evidence of this, and is this a concern we should be worried about?

MS. NGO: Well, Jeff will have the examples.

MS. ROSENTHAL: Jeff, maybe you can provide an example of this.

MR. CHESTER: I do think there's no question that if you look at the literature the industry is talking about in retargeting one person being low income, one person being middle income, one person being a much better target, there's a lot that we don't know, but what we do, know is that the online data collection process has been used to identify people and then to make them offers which I believe, particularly in the financial area, were likely unfair.

Online lead generation triggers play an important role in the sub prime prices, offering certain people a bad loan, a higher interest loan, than other people. It's something that the FTC still needs to look at, and the whole area of loans and credit cards and the kinds of offers people receive and online lead generation and triggers and what the decisions are being made about individuals once again is completely non transparent.

In the area of health, we're glad the FDA has finally gotten to regulate the social media and interactive marketing space we will be filing soon. Let me just read you very briefly a case study.

MR. MAGEE: Wait a minute.

MR. CHESTER: Let me finish because you asked me to give you examples, and I did bring examples of targeting ethnic Americans, targeting Hispanics, which I can read to you from their own words and this is Lunesta, a sleep aid, where people first found out about it was called an unbranded website, and they ended up with a 2 million person database so people could be targeted for this prescription drug. This kind of thing is harmful to consumers.

MS. ROSENTHAL: Let's talk about some of the other consumer harms. We've heard about the concept of boxing where consumers, rather than being offered different prices based on their past browsing activity, they might be offered different products or services based on their browsing activity.

For example, I used to be a big college football fan until the Gators suffered a miserable defeat on Saturday, so let's say I was a college football fan my whole life, but I no longer am a college football, fan but I'm still getting ads about college football because

I am pegged as a college -- and Omar talked a little bit about what BlueKai offers.

I can go out and I can decide I no longer want to be considered by BlueKai a college football fan, but maybe we could talk about the bigger concept of boxing, and sort of this idea that consumers are not actually seeing all that's out there because they're actually -- their choices are being limited based on their past browsing activity.

Do any of you want to talk about that?

MR. CHESTER: I want you to guys to talk about this, and you, Dave, and you Omar, at DMA, the landing pages, the conversion testing, all the things that are done to personalize. There's a downside as far as I'm concerned to personalization, a downside, and the downside is what Joe Turow really talked about today, that we're going to see increasingly that it is something created just for you, and you have no idea why nor have you given your consent.

There's no question that's the trajectory that we are headed towards with this system unless we implement -- unless the FTC implements a digital age fair information principles to restrict the collection and use of this data.

MS. NGO: When take we talk about

accountability, I'm sure the industry will point to the principles that they just released. However, when you look at the principles there is no real enforcement provision. What happens is that there is self reporting of violating the principles, and then if one is found to have violated the principles, it's public reporting.

I mean, those are the sanctions for violating these principles, so when we talk about this, I really, really want to focus on the fact that unless we have strong legislation, there is little accountability out there.

MS. ROSENTHAL: Linda maybe you could speak to that, and then, Craig, we're going to get to you in just a second.

MS. WOOLLEY: Sure. About the issue of accountability, for the last 30 years, the Direct Marketing Association has had a self-regulatory program. It covers all channels of marketing, not just online. It covers mail, telecommunications, mobile, whatever channel people want to use. The program is active, robust. We've gotten just this past year alone over 3,000 inquiries. Those are handled either by one person who is -- the one person who handles the telephone calls can sometimes just dispose of them with information and education and help.

We also have -- some of those inquiries turn into ethics cases, and those are handled in a really very judicial like way. A case is opened. There's an opportunity for both sides to present information. There are time limits built into the information gathering, and then there's a ruling.

Cases that are clear violations of law get referred routinely to the Federal Trade Commission. We enforce not only against DNA members but anyone in whatever marketing channel happens to come to us, and we also have an exemption that has been long standing by the Federal Trade Commission that enables us to do business to business complaints. It's an antitrust exemption that enables us to do business complaints as well.

MS. ROSENTHAL: Thank you, Linda. So we want to move into a different area, and that's something that we've talked about already on this panel, and that's consumer control. A lot of the panelists here have discussed that consumers have the ability to control the data collection and that if they want to -- they can go on and they can delete their cookies or they can change their browser settings, but, Craig, maybe you could talk about some of the ways in which consumer controls are actually circumvented by various entities.

MR. WILLS: First of all, I would like to say that people have suggested earlier, Berin and Linda, there's tools out and they'll solve all the problems. If we use the tool -- as a computer scientist, I've used these tools. These tools have implications. They protect some amount of privacy, some amount of information going to third parties.

That doesn't mean they prevent all of it, and they also have side effects that in some cases are very unpleasant. They're so unpleasant they drive all but the most extreme users away from it. If you use no script, very long, you do have to be very committed in terms of they -- in lots of ways in terms of turning off stuff.

In terms of stuff that we have studied and ways that are being circumvented, we talk about first-party. There's talk about third-party. One of the things that we've tracked over many years is the increasing use of that third-party providers are actually serving content, serving cookies via first-party themselves, so users who think they use third-party controls within the browser, they're not even controlling all third parties.

There is a content that is going through the first parties, that the first parties are letting third parties basically use some names within their domain.

It's been brought up a few times about flash cookies here. It's something that there are different kinds of cookie that are available.

This was brought to light over the summer by some folks out to Berkeley that cookies are being re spawned, traditional cookies being re spawned via these flash cookies. There was some news about this. One of the companies that was pointed out then went and changed how it worked, but it turns out in looking at this the last few weeks, all we've done is there's still ways to link old copies of cookies to new copies of cookies so in a sense that issue has not gone away.

MS. ROSENTHAL: Can you talk a little bit more about flash cookies? Why are flash cookies such a concern?

MR. WILLS: Well, flash cookies are a concern because they're not controlled in the same way that a traditional cookie within the browser is controlled, and any changes you make in your browser settings to control cookies have no cookies over flash cookies, and to my knowledge the NAI opt-out and any of that stuff has no control over flash cookies.

MS. ROSENTHAL: One more question, and then we'll get to your comment, Jeff. So we've also heard that even if consumers actually go in to their browser

and they delete their cookies or they don't allow cookies in the first place, that there is tracking that can go on through the IP address and the user agent data. User agent data includes the operating system on your computer and your browser version.

So we've heard about research that if you include the IP address and the user agent data, you can track someone even without a cookie. Is there any evidence of this, and can you maybe speak to that subject?

MR. WILLS: I think there is evidence out there that companies are constructing as much information as they can about browser type, browser version, configuration within the browser, that enough of that information is strung together, along with IP address that doesn't change as much, can essentially identify uniquely a particular user or a particular browser, which then can be linked to multiple accesses across different sites.

MS. ROSENTHAL: Okay. Jeff?

MR. CHESTER: I still think it's very important to understand, you cannot look at behavorial targeting in isolation. This is a system of influence. This is a system of persuasion. That's how it works. It's not just the cookie. It's the other online interactive

applications that are facilitating the collection of information, but I wanted to raise or discuss -- the industry is claiming that all of this is non PII, right?

In the new campaign, in the self regulatory initiative, which frankly doesn't really inform consumers about the process. Let me just read to you one paragraph from Microsoft's new guide for online advertising. "Behavioral targeting works by analyzing individual consumer behavior to establish patterns and then using these patterns to assess likely purchase intent," and in another document that Microsoft made available to advertisers talks about online can meet more needs than offline media including the psychological needs.

This is a very powerful system. You have to see the system in its whole context to understand the data collection strategies and what the implications are to protect consumers, especially when sensitive information related to health and our finances are such an important part of online advertising expenditures. $3 billion was spent last year from the financial services industry in this country targeting consumers online for mortgages and loans.

What happened? The FTC needs to go under the hood and understand how the online targeting of

financial service products is affecting consumer welfare.

MR. MAGEE: Thanks. I want to change gears a little bit, and I have a question for Dave, and, Zoe, I promise we're going to get to you next. You've written a bit about the increase and available online content and how that's affected supply and demand for online advertising space and also how ad exchanges and the term you've used is the daisy chain operates. So I wonder if you could talk a little bit about that and highlight some of the privacy implications from that.

MR. MORGAN: Sure. As I mentioned before, with the networked media marketing world, though it's very democratized and that now creates a lot of interdependencies, and so there's a couple things that sort of -- the realities of what's happening out there.

Most medias pricing currency has historically been on the impression, how many people do you reach, how many advertisements can you impress on them, will they see, and then some factor of pricing against that.

What we've seen online, because we don't have sort of physical barriers to distribution, and you can have sites like Facebook that can have 350 million users for I guess a five, six year old company -- I guess it's younger than that, scary, but are that the number of

impressions, the number of opportunities to be able to deliver ads to people is no longer scarce, the actual just an impression, being able to say I will reach 50 million people in the next month. That's not longer scarce. That's not longer price tied.

So it's been talked about before in a marketplace where if someone is producing content and wants to be able to monetize it to pay their reporters or their journalists or their bandwidth costs, they have got to find ways to be able to pay for that, and in most cases, almost all cases I would say on their own, that's not possible anymore. It requires dependencies, and so in most cases you need to be able to work with other companies that may be able to reach advertisers you can't reach, and hopefully those advertisers have a higher rate.

You may work with companies that have data on that browser or data on browsers like that or data that relates to the vertical segment that you're operating in. Otherwise you're not going to be able to get the kind of rates that were more consistent with media as it was done before.

This is sort of the good and the bad of it. I mean, the good is we have a lot more people producing a lot more content for a lot of others, but now we have a

lot more people that touch the ecosystem, and so one of the things that I have said, and I think it's really critical here, and this is why I think it's important to note the steps the industry has taken over these last two years, which has been the potential for harm is certainly significant.

I mean, the amount of data that is moved and as you mentioned before, is it possible to technically tie Internet protocol addresses and other data to be able to get closer to identifying a particular person or a particular device? Absolutely, and I think one of the most important steps the FTC has taken that hasn't been probably promoted as much is essentially moving away from the personally identifiable information standard to a broader and I would say more appropriate standard of being able to relate information to a particular individual or device.

MR. MAGEE: You talk about in terms of how that affects a publisher, specifically whether a publisher knows who is collecting information on their site, how many different people. Richard highlighted it in the diagram, the idea of somebody having the ability to serve an ad but passing on it, dropping a cookie and given it to another entity.

MR. MORGAN: Certainly I would commend Richard's

charts, but I think they are extraordinary particularly in light of the overall ecosystem, but as you might know for those who can talk about the fact that browsing doesn't work as well as script that's turned off, is it's an interdependent economy. There may be 20 different scripts or cookies that are running on any web page to make it work, different content providers, different analytic providers, different advertising providers.

What's also happened so that a website can be paid the most possible for any ad is that when they hand an ad unit to another network or a third-party company like a Yahoo or Google, it may be conditional. It may say you can look at this, then if you have an ad place it, it if not, hand it to another party and then hand it to another party and then hand it to another party.

The level of control starts moving away from the publisher or who the person first came to, and that brings this balance, which is if the publisher can't deal with third parties, then they can't pay for the content on the site and maximize the revenue, but then the balance is if you go down to third parties, you may have 7, 8, 10 different companies now that have a chance to put a cookie onto a browser to determine what's the most appropriate ad.

And this is where I say what we can't change is that there is now this interdependent ecosystem. I think the question is: What's the right balance of sort of bully pulpit from the FTC, strong enforcement to prevent things going in the wrong direction and some of the standards.

MR. MAGEE: Can we get -- I would like to play off that idea about control and direct a question to Zoe. We seem to be focused on the paradigm where it's a content publisher, but Walmart is a retail publisher, and I'm wondering what sort of control Walmart is able to exert on the entities it contracts with for behavioral advertising?

MS. STRICKLAND: Yeah. I do think that there is a distinction with how are you dealing with third-parties on your site, be they for OBA purposes or just basically serving your website and all the functionality it includes, and that's been the case since B to C websites first arose, so there's a very different set of folks who help you deliver your website and the platform that goes along with it.

There are a different set of folks who help with online advertising, and that can be first-party or third-party, so it's very distinct, and we'll make sure as we talk about those things, we think about them in a

sort of bucket sort of fashion and say: What's your underlying principle that makes sense there for those?

And I do think it's very much in the publisher's interest to make sure that they -- you talked before about the different players in this ecosystem and what they're bringing to the consumer relationship. The publishers are the ones that have the face to the consumers. We need to make sure that we don't delegate too much to the folks or technology experts to build all of these things. We need to message it to our consumers that way that they understand because businesses really don't want to upset their customers.

They really do want to do the opposite, and I want to bring back a point that I think that Michelle made about technologies. I almost think there was two pieces to this question, one is the technology and the fixes and how do we make sure that if folks opt-out or opt-in or whatever they've done, that there's compliance with that, and I think that's not just true with just OBA. It's true with everything.

You're doing email marketing. You're doing telemarketing, whatever the case may be, how you're doing Email marketing, not getting phished. There will always be ways that you have got to make sure technologically that you have delivered what you

promised. I think there's a lot of good industry efforts out there to make sure that industry can deliver what they said they're going to deliver to consumers and to police that.

But the second issue is: Besides the technology and the compliance feature is how are we communicating to -- how do they understand it? What's the right defaults? First-party, third-party, they our different. For Walmart when we launched our privacy policy. You get a mixture of opt-in and opt-out, and there are other folks here who have dashboards and we find the same thing. The people get on there and play with it, so they're really sort of different issues, where the policy should be and then how is the compliance behind it.

MS. ROSENTHAL: So I have some follow up questions to some of what you're talking about. So we hear sort of two different things. Something we hear that publishers have a problem sort of exerting control over the different entities that they are working with for behavioral advertising, so in terms of negotiating -- if you want to negotiate terms about the collection of the data or the use of the data by those third parties, that sometimes it's difficult for publishers to engage in that.

But then on the other hand we see, for example, where Walmart was able to exert a lot of control on green issues, so Wal-Mart has said these are the standards we want you third parties to comply with, and we won't work with you unless you do that.

So can you talk to us maybe about where on the spectrum publishers are when it comes to these sort of privacy issues? Are they able to exert control? Are they able to tell the people they work with, look, we're Walmart, we're not going to work with you unless you do this, or do you -- have you found a difficulty in actually expressing how that data should be collected and used by the third parties you work with?

MS. STRICKLAND: I think historically when publishers work with third parties and with folks who are experts in the technology and the ad space is you look at a result, which is how am I making sure I'm reaching my customers effectively, and so you look to those principles and say, how do we do that. We need to do a better job of understanding what the technology is behind that, so what cookies are being placed, are they flash cookies, are they regular cookies, how are we following industry standards.

And one thing I think is not in our customer's interest is when like, for instance, your standard

contract clause that just say comply with laws. That's not good enough. There's a lot of industry stuff out there. Just complying with laws doesn't even scratch the surface on what we are doing here, so I think publishers need to step up more in terms of the delegation that's gone on.

MS. ROSENTHAL: Omar?

MR. TAWAKOL: Yeah, I just want to talk about when we think about what third-party cookies are used in behavioral advertising, there's some confusion, and that is usually when we're talking about it, we're saying that you know something from the profile and you're delivering your ad to them somewhere else, but the majority of third-party cookies use for targeting actually isn't traditionally called behavioral advertising.

What I mean by that is something like conversion optimization, so an advertiser buys a contextual ad from a newspaper site, and the newspaper site thinks they're sold them a contextual ad, and they did, but that advertiser needs to put a cookie to see if that contextual ad performs and results in a sale later.

Sometimes they even buy CPA advertising which is to say, Hey, I'll put this ad up but I'm not going to pay you unless they bio my site. These methods dominate

the revenue stream in display advertising, so we participated in a survey that was actually implemented by the IAB and the full results have not been released yet, but to give you a sense of it, what we found is that 68 percent of all agency dollars use some sort of conversion optimization.

Another 43 percent use frequency capping. Frequency capping is a technique which you say, I am going to only fill out this ad five times, therefore I have to track how many times I showed it to you, which goes into your individual cookie, so these techniques dominate about 70 to 80 percent of all the money coming through display advertising, and they require a third-party cookie, and they require the level of tracking you would have called behavioral advertising, and they find the content and in many cases, the publisher who sold that piece of advertising wasn't thinking of it as behavioral.

MS. ROSENTHAL: Right, okay. Berin, let me -- yeah, go ahead.

MR. SZOKA: I just want to briefly, I swear, touch on the points that these three made, and to say that really if you remember one thing today, you should remember the point that Dave made, which is to put it in a shorter fashion is that the co modification of

attention, right, so if attention and advertising is what funds content, the problem that Dave described is that there are so many sources now for advertising that the rates that everyone is getting are plummeting, and that's why traditionally ad supported industries like journalism are being so challenged.

So the central dilemma that we face is if advertising for attention becomes com modified, if it becomes something that's worth essentially the same almost everywhere, how do we make that more valuable across the board, and then how do we increase publishing revenues for everybody? So there I want to give you four quick statistics.

The first is to just put this all in perspective, in 2008 I believe newspaper advertising revenue online was $3 billion, out of a total advertising revenue of $39 billion, so just think about how much time you think people spend online versus reading traditional papers, and you'll start to see there's an enormous disconnect there and a huge problem as newspapers are increasing and moving to screens.

The problem is basically that the digital -- that the dollars in the real world are being replaced with cents in the online world, and the best way to think about that is to look, as Dave said, at the

impression rates, and if you look at those, and Howard Beales is here in the audience and has done great work in charting this, if you just compare those, in traditional media, you talk about 4, 10, 20, sometimes even 50 dollars per impression. Online put those in cents.

You're generally talking about less than a dollar per impression, right? That's the central problem we need to talk about here.

The third static, very briefly, is advertising in general, online advertising, 7 percent of total U.S. advertising, right, above a shrinking pie, a pie that is significantly smaller than it was last year and than it was in 2000, and it's now at its smallest point since 1976, but of that 7 percent, 45 percent of that goes to search engines.

So for all of you in the room here to think that Google is too big, well 45 percent of revenue goes to search engines, so what I'm really concerned about -- I mean, Google offers great services and it is valuable to every one of us, and I want them to make more money. I also want the publishers that depend on display revenue to make more money.

What do they get? They get essentially a third of total online advertising spending, which is less than

3 percent of total U.S. advertising spending. These are the statistics you need to think about in understanding what the challenge is for publishers because consumers have many values. Privacy is one of them, but getting content and services is another, and that's what it depends on.

MS. ROSENTHAL: Thank you, Berin.

MR. MAGEE: Can I ask about -- Zoe, I'm interested in just what the return on investment is for behaviorally targeted ads as opposed to contextual ads, and maybe you can talk about your experience with that. We've heard a lot of statistics, but it still seems to me that it's unclear how much more valuable a targeted ad is versus an ad I get related to sports because I'm on a sports site.

MS. STRICKLAND: Thank you, Peder, and I think that's a very valid question, which is a return on investment which is how businesses tend to think about things, which is much deeper than just dollars and cents, so as you think about it, OBA is really just another tool that you can use to reach out to customers and to serve them.

And yes, I think that it's been pretty demonstrated, and I think most folks would attest that there is a lift based on OBA ads versus contextual ads,

but when you look at that as a publisher, and you weight that against the costs of participating in OBA, whether or not being part of a network, do you want retargeting on your own website and what is the value of that, and then also consumer desires.

Businesses really don't want to annoy their customers, so how do you really understand what they want? I think the survey data, the education efforts are enormously important, and then you look at it in the context of your business model, which is an ECommerce site versus, as an example, the journalism sites that we've talked about that depends on ad revenue to a greater degree for their content.

I don't think there's any magic to this. I think that OBA is just one more example of a different tool that you reach out and touch your customers with, and we can certainly give an example in our offline where we talked about, hey, we want to customize coupons to you and what we've seen there. I would be happy to talk to that.

I think websites existed before OBA and I think they exist afterwards. It depends what that would look like, but I think given the interest in this topic and the attendance here goes to show that OBA has some real attention to it and value to it.

MR. SZOKA: Peder, if I could add one sentence to that. This is the fourth statistic I meant to add. There's a lot of data out there, it's hard to say, but the difference could be up to ten times as great for some publishers so the delta we're talking about here is not small.

MR. MAGEE: Are you referring more to the long tail of the Internet small publishers?

MR. SZOKA: You're exactly right. You have to look at the major publishers versus the smaller ones, and the difference gets bigger the farther out you go, but if you look at increases in click through rates and the other metrics that are used to track the effectiveness of advertising, for the first year of publishers which is things like newspaper websites, the difference may be relatively small. It might be only twice as effective, twice as revenue producing.

For small sites it could be in many cases up to -- again there's a lot of data out there, but it could get ten times as revenue producing so it's had to see how it all plays out in the aggregate, but we're not talking about a 5 or 10 percent improvement. We're talking about several factors of revenue, and that's why the stakes are so big here and why the changes in defaults and regulations make such a big difference.

MR. MAGEE: Omar has got something, and maybe you could also, after your comment, we talk about what sort of research we need in this area to pinpoint this a little bit.

MR. CHESTER: Can we ask each other questions?

MR. SZOKA: Just to add one level of precision. I don't think you want to compare behavioral advertising just to contextual because I would say about 70 percent of the Internet impressions are very low in context, and that type of inventory goes to what we call run of network pricing. Run of network pricing tends to be in the tens of cents, and typically when you use reasonable behavioral data to sell a campaign to an advertiser, it's going to be anywhere from the $2 to $8 range.

So you're lifting inventory that would be anywhere from like 10 cents to 50 cents to $2 to $8 when you talk about applying data to a run of network buy, so that was the first comment I would like to add.

The second question was?

MR. MAGEE: Well, I'm wondering if there's research in this area that needs to be done to get a tighter handle on the value of behaviorally targeted ads versus non targeted.

MR. SZOKA: I think there's a lot of data that's already on there. The type of research that I think is

interesting, I know that there are some groups under the IAB standard that's doing this and hasn't finished yet is trying to take the dollar that comes from all the agencies and break it up and say, what percentage of the dollars and campaigns go to each technique within behavioral advertising, re-targeting treated differently then campaign optimization, frequency capping, third-party data targeting, demographic targeting. That survey and that analysis would be I think very useful once it's complete.

MR. MAGEE: Dave?

MR. MORGAN: I would add one thing and I would support the numbers that Omar has referenced having been in the industry for awhile. It is about -- ten X is probably a pretty good way to think about it. It is different. The couple areas, which I would -- I don't know how much research has been done, but not all content supports the same; in other words, if you publish automotive content or travel content or technology content, well that's much easier to support in the context alone represents a lot of value.

Having originally come out of the newspaper industry, I will tell you the kind of content that supports the worst, and it's news. News does not carry a commercial value to most advertisers such

that -- because it's also a little scary. It could be a plane crash. It could be a murder, it could be crimes, things that advertisers don't always want to be associated with.

In that case, and typically it's much more than ten times as much, and one of the problems, for example, some of the traditional journalism companies have had is that 80 percent of their page views and their impressions are on this generalized news. A very small amount is in automotive or high areas, and so I would say their over weighted in their dependency, and this has been I think as everyone knows like the IAB and the DMA having tried to push through a lot of these standards -- one of the biggest problems was to get all the individual publishers to be willing to sign up for a lot of self-regulatory standards and principles because they feel so dependent, but it's the reality we live in.

MS. ROSENTHAL: Thanks, Dave. I'm going to switch gears and ask one question that came from the audience, and then I think Peder will wrap up.

So we hear a lot -- even though the FTC behavioral advertising report that came out back in February -- in the report we talked about we're not going to make a distinction between PII and non PII. Yet we still see industry making that distinction when

it comes to privacy policies and notices that they are giving to their consumers. We still see notices that, oh, we're not going to give personal data or, oh, this can't be used to identify you, so even though, the FTC staff did not make a distinction, we still see that distinction being made by various entities.

So the question is: Is it naive to think that anything is actually truly anonymous? We see examples that are out there, for example, the AOL search information that was published for research purposes, and information that was supposed to be anonymous was able to be -- they were able to re identify someone based on the very specific searches that they had made.

So the question here is: Can we really consider information anonymous or is there such a high chance that it could be de anonymized or re identified that we should be making no distinction?

MR. CHESTER: I think -- I mean, everything the industry says and we have supplied so much information to the FTC about this, and it's in the record, and it given to the top staff. Everything the industry says daily it is about an individual. Yes, we don't collect PII, but they can target an individual, the self-regulatory regime adopted by the trade organizations, and the new PR campaign that was just

launched last week should be investigated and rejected by the Federal Trade Commission because they're not telling consumers the truth.

They're not collecting information, they tell you, they tell the consumers, but to their clients like Microsoft did in the document I read, it's an individual. They know you. The whole system is designed to know you, to find you, to engage you, to develop a relationship and collect more information, and that's why I am glad -- when I finally conclude, I am glad finally that the FTC hasn't started a serious investigation of the online advertising industry, collecting documentation, so it can come up to speed because as Leslie Harris said this morning, the Commission needs to know more about the online ad space and respect to privacy.

MS. WOOLLEY: I think it's important to go back to what it is we're talking about. We're talking about ads. We're talking about ads that are targeted. There was a lot of talk this morning and a little bit on this panel as well about problems that result from ads, and there was talk about redlining. Redlining is illegal. Redlining is proscribed by DMA guidelines and every other industry group of guidelines that I'm familiar with.

We can keep bringing out the parade of possible horribles, but none of those things have actually happened. We're talking about ads, and I think it's hard to be upset about ads that could possibly be relevant to you and improve your online experience.

On the issue of PII, non PII, I again don't know of companies that are collecting PII and telling consumers that they're not collecting PII, and I think it's very -- again very, very important to let the marketplace work in the way that BlueKai does.

Transparency is absolutely paramount and let consumers make their choices. We have tried very hard to do this, as I said with DMA Choice, which is a mail preference service. It enables consumers to go online and figure out what they want, how they want it, whether they want it, mailed several times a year, and it's when you get into the granularity of individual consumers making individual decisions about themselves is when you can best meet consumer's needs.

MR. MAGEE: I think the transparency is a key component here. On the question of PII versus non PII, I think that's tough, and I think it depends on the definition you're using. We see that as --

MS. ROSENTHAL: Everybody wave your hands.

MR. MAGEE: We're going to give a final weigh in

on Craig Wills, if you want to talk more about the PII, non PII distinction based on your research.

MR. WILLS: Well, let me say one of the more recent things we've observed is certainly that third parties are involved in all other sites are also involved in social networking sites, and we put out a paper not long ago that basically showed your social networking identifier gets passed to the same companies, so not only your behavior is being linked to your identity in that way.

MS. ROSENTHAL: We do hope to get into some of those issues in our second roundtable as well.

MS. NGO: Just something really short. I just don't want to let stand the statement that it's just advertising, it doesn't lead to anything bad. We have given examples, yes, redlining is illegal, but it's happening, so bad things are happening because of interactive -- because of the advertising targeting, and we need to look into it. If they weren't, we wouldn't be here.

MR. MAGEE: Thank you very much, and thanks to all the panelists for your time and your energy.

(Applause.)

PANEL 4: Information Brokers.

MODERATORS:

KATHRYN RATTE, Division of Privacy and Identify Protection, FTC

LORETTA GARRISON, Division of Privacy and Identify Protection, FTC

PANELISTS:

JIM ADLER, Chief Privacy Officer, General Manager of Systems, Intelius

JENNIFER BARRETT, Global Privacy and Public Policy Officer, Acxiom

PAM DIXON, Executive Director, World Privacy Forum

RICK ERWIN, President, Experian Marketing Services

CHRIS JAY HOOFNAGLE, Lecturer in Residence, University of California Berkeley, School of Law

MS. GARRISON: We ask every one to sit down, please.

MS. RATTE: Thank you to everyone who stuck around with us today. My name is Katie Ratte, and my co-moderator is Loretta Garrison. We're with the Division of Privacy and Identify Protection, here at the FTC, and today we've been discussing the collection and use of information in various contexts, as well as the extent to which consumers are aware of those business

practices.

One area where we don't think consumers really understand what's going on with their data is the aggregation of consumer data for marketing uses. Earlier when we were discussing the retail loyalty card chart. Richard Smith talked about the data of pen vendor, where you can get additional demographics data for marketing purposes. And that's just one example of how these marketing profiles are enriched in ways that consumers may not understand.

There are also data products being sold directly to consumers that are being put to secondary uses in some cases that consumers may not anticipate or like, so the term information broker is pretty broad, and it covers a lot of ground, so I want to define for the purposes of this panel what we would like to cover.

This panel will deal with unregulated uses of consumer information. By that we mean those that fall outside of the Fair Credit Reporting Act. We plan to talk about the sale of consumer information to businesses for marketing purposes. We'll also call this the B-to-B context, and we plan to explore the business to consumer or B-to-C context as well, and for what purposes some of these direct to consumers products are being used and what secondary uses might they be put to.

During the previous panel we also heard a lot about the online collection of data, and here we plan to look at some of the offline practices in the information broker business as well as how some of these new online sources are being used to enrich databases created from offline sources.

With that I would like to introduce the panelists. First to my immediate left we have Jim Adler from Intelius; Jennifer Barrett from Acxiom; Pam Dixon from the World Privacy Forum; Rick Erwin from Experian Marketing Information Services, and we hope very shortly by phone to have Chris Hoofnagle from the Berkeley Center For Law and Technology. Chris wasn't able to be with us in person today, but we hope to have his virtual participation very shortly.

Just a quick reminder to the panelists, please raise your table tent if you have a comment. Although I'll be directing a lot of the questions in the first instance to a specific panelist, I encourage a lot of interactive dialogue so please jump in if you have something to say.

Also if you have a question from the audience, please write it on a question card and hand it to one of the staff circulating. They have extra cards for you if you need them, and for those of you listening in on the

webcast, you can Email your questions to Privacyrountable@FTC.GOV.

So I thought we would start it off with a pretty easy question, and that's how to define sensitive information. I'm just kidding. That's not an easy question at all, so I would like to start off by asking the data brokers that we have here what types of information you collect, whether it includes sensitive information and how you go about defining sensitive information, so, Jennifer, let's start with you.

MS. BARRETT: Let me start with what types of data we collect because I think that kind of sets the stage. Our data collection practices fall under three main categories. We do use information from public records and other publicly available sources. We use information collected from surveys that the consumer fills out directly themselves either for us or for other parties that we acquire that data from, and we use information from companies that are consumer facing and have consumers as customers and given notices that data will be shared by third-party.

Our definition of sensitive information actually falls into two categories. We classify all the information that we have at Acxiom in any of our data products into three classes. The first is sensitive.

The second is restricted, and the third is non sensitive.

Our definition of sensitive information in this context is information that typically contributes to the consumer being at risk for identity theft. Restricted information is information that has a sensitivity to the consumer but probably doesn't put them in quite as much real financial or other type of risk like a cell phone number or like an unlisted telephone number or in combination, certain kinds of data that the consumer might be concerned about.

So we have special rules around how we treat sensitive information, obviously the higher standard of protection. We don't sell it to near as many people. In some instance we screen the client that is acquiring the data to a much higher degree from a security or otherwise standpoint as well as restricted information has a set of rules around it.

And then for the non sensitive information, we enter into a contract with all our clients, make sure they have a legitimate purpose for it, and depending whether it's used for marketing or for risk management, there's a set of conditions around what the client can and can't do with the data within their own enterprise.

MS. RATTE: Jennifer, can I just follow-up to

that and ask you to give us some examples of categories of sensitive information? You said it was things that put the consumers at risk of identify theft, but that could be a pretty broad category.

MS. BARRETT: It will be detailed information, account information, identifying information like a Social Security number or a driver's license number would fall into that category or full date of birth, that type of thing, mother's maiden name, that type of thing.

MS. RATTE: Where would something like health information or ailment information fall?

MS. BARRETT: If it's protected health information under HIPPA, that obviously falls under the sensitive classification. If it's voluntary information on a survey, typically about ailment information, we consider that restricted.

MS. RATTE: We'll come back to the survey issue in just a little while. Rick, would you like to add to that?

MR. ERWIN: Much of what Jennifer described is also true for Acxiom. Both of our companies are extremely rigorous in the way in which we collect and care for information. One point I would like to make, just to back up to the definition of the panelists here

as information brokers, I think I can probably speak for Jennifer when I say our clients don't think of us as information brokers because in our industry, in the marketing industry, brokers are usually entities that never take possession of the information that they are providing to their clients, and nothing can be further from the truth in the case of either Experian or Acxiom.

In Experian's case, we not only rigorously vet every single data source that we have but we rigorously manage every bit of data that comes through our doors.

So having said that, I will just say the data we collect falls into three categories: Public data, public record data, which is things like telephone white pages and Census Bureau data. It's self reported survey information, which is where a consumer has been presented with the request to participate in a market research survey for the express purpose of using their information for marketing.

And then the third category of information is permission marketing data, and that falls into the category of data that has been collected with the express permission, with proper notice and choice from the consumer, and that could include the kind of information you would find provided by a retailer.

MS. RATTE: We definitely want to come back to a

discussion of exactly how those permissions function, but maybe, Jim, could you tell us a little bit about your categories of information and what you consider sensitive in your data products?

MR. ADLER: Sure. For those that don't know, Intelius, we are an online information retailer. We provide search services about people, businesses and assets to consumers and enterprises. We are really a retailer. We obtain a lot of information, and we package it up for individual consumption to consumers typically.

Similar to Rick and Jennifer, how they described the information, it's similar. We obtain data from the industry, public records data, which are birth and death certificates, business records, property title kind of information, also publicly -- publicly available information, information that's on the web, business information and then commercial records, what's commercially available, lists, phone connect, disconnect information. Also business profile data comes through commercial sources as well.

MS. RATTE: Okay. It sounds like we still haven't got Chris to join us. Pam, did you want to talk a little bit about how these definitions of sensitive information function and what you think might need to

change in this space?

MS. DIXON: Sure. I think first off I think this is an enormously challenging area. The definition of sensitive information if something that we're wrestling with in the state of California, just at a state level trying to determine what that definition would look like for healthcare standards, for health information exchange, and let me tell you, it is not pretty. It's not fun, so I think that these are honest answers.

I would just offer a couple of thoughts. I think that Jennifer's idea of information that puts an individual at risk for identify theft is actually not a concept that is frequently seen through the definition of sensitive information. I think it's a good category to add, and I think it's a positive step forward.

I do think that there are standards in the EU for the definition of what constitutes sensitive information, and I think those are important to take a look at because those standards were arrived at by a thoughtful process, and they're robust. I think that the OECD has done a lot of work in this area, and again, it's been a multi stakeholder process, and those are robust.

So just without reinventing the wheel and going

through a whole book of information, I just want to focus on one area, which would be healthcare information. One of the great concerns we have, it was brought up earlier in the day when, for example, the MedNet health list was discussed in terms of those ailments being published.

I think that all us in this room would find and agree that it's fairly repugnant to sell people's mental health ailments on a marketing list and say, Hey, look these people are easy targets. That's just really I think ugly, and I think we can all agree with that, but the way that this information was released was not from a doctor's office. It was from the consumer themselves agreed to release it, therefore pulling it out from under HIPPA.

So you have the same information that would be held under HIPPA, the identical information then with the consumer's own consent is released, so when is this protected information? Is it protected just because it's held by a doctor, or is it protected because there's a reason that it should be protected? And I think that is really the core of what we need to look at.

Do we want this information protected or just the context the information is held in? So I would

argue that we should protect the information, and there should be standards. Defining those standards is not easy, not fun, but I do think it needs a rigorous, consensus process that has friction, intention and teeth.

MS. RATTE: Rick, you have something to add?

MR. ERWIN: Yeah, I couldn't agree more that a thorough discussion of these things is always a great idea. I failed to answer you on the notion of what Experian considers sensitive data among its marketing data assets.

We would consider children's data, data on older Americans, healthcare data including ailment data, account number data and financial information all to be sensitive data. However, we only collect and provide to the market the first three; that is to say, children's data, data on older Americans and self reported ailment data.

And we have about three decades of experience with those types of data that I just described being safely used for marketing purposes, and it's not an accident. It's not because there was no regulation and no industry self-regulation. It's because we've maintained a system where self-regulation works and where the industry continually does things like this,

this forum, and establishes the right balance between the interest of consumers and marketers.

For our company when we sell what I just defined as sensitive information, we not only put every client through a rather detailed credentialing process, we make sure that we see the actual advertising piece that they will be using, whether it's a mail piece or a script or whatever. We require that the contract not only require them to sign on to adherence to industry self-regulation, but also our own, Experian's own global information values.

We randomly seed all of these data files, all of these databases with real addresses, with fake names that we can monitor to make sure that they're not in fact doing something with the data that they did not warrant that they would be.

So the point is that's not an accident. That's because companies like Acxiom and Experian are extremely responsible in the way that they do this, and in my experience the DMA has represented an industry where that method of self-regulation works, and it's been working for 30 years, and I haven't heard a lot of examples of where we can point to deep consumer harm because they received the wrong advertising as a result, and I think we can't overstate that.

MS. RATTE: Jim, did you want to add something to that?

MR. ADLER: Yes, just let met downstream from the Acxiom experience, and I want to thank you for that since we are consumer facing, and from our perspective things falls in, to three buckets, buckets that are the buckets that are clearly sensitive or should be restricted, things like data about children, medical histories, telephone conversations.

On the other side of the spectrum are things that are clearly okay, data that people put out on the web. LinkedIn public profiles come to mind, clearly okay to obtain that information, and then we're discussing in forums like this everything in between, and as Pam said it's difficult, and transparency and clear debate and discussion are vital to have bright lines around what is okay and what is not okay.

MS. RATTE: Since we got on the topic of the MedNet list, I wanted to get down into a little more detail about how the permissions function when consumers give you that information. How do you ensure that the consent that a consumer is giving to disclose a mental health condition is the type of -- I think Leslie Harris called it serious robust consent that we would want to look for?

Put another way: How can we be sure that the consumer actually knows that by filling out this survey they're consenting to the use of that information for later marketing purposes? Rick?

MR. ERWIN: I'll tell you what our standard is. Our standard is there is a massive sign at the top of that -- if it's an Internet survey, at the top of that page that very clearly says, We are interested in collecting marketing type information, market research information, and we would like your opinion, and it goes on to very clearly spell out -- from anyone whose data that we would buy to resell for this purpose it goes on to restate that any data that they provide can be used for marketing purposes with other marketers and advertisers, and gives the Respondent or potential Respondent multiple opportunities to leave the process without that information being used if they don't choose for it to be used.

It's really quite simple and quite clear in the case of our sources.

MS. RATTE: I think Pam would like to respond to that.

MS. DIXON: Thank you. A couple things. One of the problems that I think has been highlighted today is the role of consent in privacy and the role of kind of a

subtopic about opt-in opt-out. I think we need to look at consent very carefully. Again we should be informed by consent in the healthcare sector and what that has become and some of the problems it has posed for consumer privacy.

I think there's a couple things. First: In terms of consent, one of the questions that I've always had is: Are the consumers being told, for example, that they're going to be put on a list of people with mental health ailments? Are they told that their information will be sold for a period of time that does not have necessarily an ending point in sight?

Are they told that they will not have the opportunity to revoke consent at any point, so I think that unless a consumer is given, for example, the delineation of the boxes that were to be put in and sold in, I don't know that that is sufficient consent.

Additionally I think there are other issues in terms of mediating consent online, which are well known issues that the Federal Trade Commission has looked at in JLB and FCRA already. I think it's difficult.

So I would say in taking the most lenient view of the consent process and trying to get everyone the benefit of the doubt, let's say the consent is possible for this kind of data online. Let's assume that, and go

from there.

If consent is possible online for sensitive health data, for example, I think the bare minimum would be that a consumer would have the right to know what list they're going to go on, for how long, and would have the right to revoke their consent.

MS. RATTE: Would you like to comment?

MS. BARRETT: First of all, we only have about eight what I would call general categories, mental health is not one of them, but they're very general categories in the nature of allergies, diabetes, things that a large percentage of the population has, and a large percentage of the population might be interested in information about because the purpose of this is to get them marketing information about products and services that they may or may not have been aware of.

But I think Pam makes a very good point, and that is consent is important, and we do the same sorts of things that Experian does in terms of screening sources, but choice along the line also is because if the consumer felt comfortable about it at the time and they maybe their allergies go away and they're tired of getting marketing material, they should certain have the right to do this.

This is a DMA standard to opt-out from

marketing, and we allow consumers to come to Acxiom and either opt-out all together from all of our marketing products or opt-out selected ones from some of the different ones. If they just want to get off of online targeted advertising , they can do that. If they want to get out of the telephone directory we produce and sell to many websites for white page and yellow page searches, they can get out of just that, or they can get out of absolutely everything.

MS. RATTE: We've been joined now by Chris Hoffnagle by phone so I wanted to give him an opportunity to comment. Chris? Chris? Our phone hook up may not be working so well. Well, until we make contact with Chris, we'll move on to another topic.

Jennifer, could you outline for us what kind of screening you do of your data sources -- here he is.

MS. GARRISON: Go ahead.

MR. HOOFNAGLE: Can you hear me?

MS. GARRISON: That's better. Speak a little louder please.

MS. RATTE: I don't think it's working. Chris? Chris, hello?

I'll ask a question that we got from the audience until we figure out this issue. Could someone comment on what percentage of the data broker industry

is represented by the unregulated products that we're discussing here today as opposed to FCRA covered products? I don't know who wants to field that one.

MS. BARRETT: I will start. We have both a products that fall under FRCA, employment screening, background screening for employment as well as tenants, and we have what I think historically is called unregulated products, which would fall into the marketing arena.

To some degree I object a little bit to the term unregulated, and I think my product people back at the office would argue that point vehemently when I walk in with a whole list of things that they're supposed to do and follow relative to those products.

While some of them may be legally regulated, for instance, there are certain public records that are prohibited by state law from being used for marketing purposes, so obviously we have to follow those regulations. There are also a variety of other contractual obligations that come with the data since we're not an originator of the data, and as your wonderful chart on the wall so beautifully depicts.

So we have lots and lots of specific rules and prohibitions on what we can and can't do with the data, and then later on top of that, the fact that the Direct

Marketing Association has a whole set of ethical practices relative to both the collection and the use and the sale of data, we don't feel very unregulated even in what most people think of as regulated products.

MS. RATTE: I guess the question then is: Are their segments of the market that are truly unregulated? Because it's true that Acxiom has the standards that you've been talking about, you adhere to the DMA guidelines, but part of the conversation we need to have here is whether they're actually actors out there who aren't adhering to these guidelines, who are operating totally outside of regulation. I think Pam has a comment on that.

MS. DIXON: Yeah, it's a challenging question because there's too much that we don't know. I would love to see a list of all folks who are doing -- well, we don't even have a list of folks who fall into the Fair Credit Reporting Act. We don't have a list of the specialty database under the FCRA, so I don't see how we can really get our hands around what this universe looks like, other than to give you some very broad ideas.

So here's the broad ideas, and I apologize for not being more specific, but if you look at customer relationship management databases, this is an extraordinary source of unregulated data on consumers.

Another I think area is transactional databases and data co-ops, purchase history, so, for example, you activate a credit card, and it's not your credit card company that's doing this. They're regulated. It's the folks doing the activation, the third-party. They're unregulated, so I really think that you're looking at a universe where you have some very large entities such as Acxiom, Choice Point, actually a lot of folks at this table, who do have regulated products, credit bureau, things that have permissible purposes or non permissible purpose under the Fair Credit Reporting Act.

But I think when you start talking about, for example, badcustomers.com, a list of charges that have been disputed, folks like The Work Number that compile salary information. There are -- I think there's a large significant universe of unregulated database, but the exact size I have no idea.

MS. RATTE: I think we're going to try again to make contact with Chris. Chris, do you have any comment on the unregulated portion of the market?

(Discussion off the record.)

MS. GARRISON: We understand he's listening to this via the webcast not over the phone so there's a delay.

MR. HOOFNAGLE: My comment seems to be about a

minute delayed.

MS. RATTE: Did he have anything else? We will plow on. I wanted to spend a few minutes talking about what new data points online sources are bringing to your existing databases.

MR. HOOFNAGLE: I can't hear, but I can't actually hear what anyone is saying. It's tough over the webcast so I don't have two way audio.

MS. RATTE: We'll keep going. I wanted to spend a few minutes talking about new data points. The previous panel talked a lot about online sources for data collection. We've also heard of new types of information collection such as through social networking sites and even the smart grid, the granular information that may be available on consumer's energy consumption and the possibility that that might be used for marketing.

So I was hoping that you could comment on not necessarily on whether you're using those new data points now, although that would be interesting, but what rules would apply to that sort of data as you merge it into your existing databases. Rick, did you want to start?

MR. ERWIN: Yes, very simple. We apply the exact same rules that have worked very well for 30 or 40

years in the offline world, because those rules are based on principles of balance, accuracy, security, integrity and communication with the consumer, so principles enduring things like shifts in media channel, and that's what we found, whereas 20 years ago we would have collected data from people self reported from paper surveys that they would fill out on whether or not they liked to golf or whether they had dogs or whatever it might have been.

Now, all of that data for us is collected from the Internet, but it's done using the exact same collection principles as would have been done before, and as it relates to publicly available information from social media sites, I can tell you that we periodically evaluate that, and thus far have not found those sources to square with our own information values so we don't acquire those sorts of data.

MS. RATTE: Which information values are at stake here? I mean, is it a matter of data integrity or is this something to do with the privacy interest?

MR. ERWIN: It's almost always a combination of all of them, and certainly in this case, in this example I am giving you, that's very much the case.

MS. RATTE: Okay. Pam? Jim?

MR. ADLER: I just wanted to say that in many

respects the data that's out there about social networks is in some sense flattening the world a little bit, and what -- we sort of the last hundred years have lived in and grown to expect the anonymity of population density, and what the web is really bringing is a community that's new, and a lot of that data is new, and we bring a lot of that data to consumers.

So we see a lot and I hear a lot of well, I want to know everything about you, but I don't want you to know anything about me, and we see a lot of that, and we're struggling with how you square those two. We have a lot of people show up at our sites that want to learn more about people for all kinds of contexts. They may want to date them. They may be -- they may be a long lost relative they're looking for, and there is a plethora of data out there that comprises your digital footprint, and we are at the very early stages of this.

And it's very important that we look at it from the context of where we've been, but there's also a tremendous value in the connection that it brings.

MS. RATTE: We have a question from the audience. Oh, Pam do you want to add?

MS. DIXON: Yes, thank you. I think one thing I would like to just point out very, very quickly -- actually two quick things. One, there has been a lot of

discussion of self reported data, but I think it's very important to understand that consumer choice is fatally undermined. When you start talking about data collection from core service provisions, so, for example, if you are going to be in the Tennessee area and you are under the Tennessee Valley Authority Smart Grid, which is going online right now, your electric data and the data of the smart appliances with their unique IDs and all that good stuff that you're using in the smart grid application is going to be collected and massaged, and they have grand plans for the data.

They've already discussed this, and is there something wrong with that? Who knows? Smart grid is very knew. We need standards, and this is just looking at this, as most of the people in this room know, we signed onto comments with the Electronic Privacy Information Center with a lot of detail about this, but the bottom line is is that's not self reported data. That's just a consumer trying to get electricity.

A similar situation is with Cox Digital Telephone. If you sign up for that service your data will be analyzed, for your calling patterns who you're calling, you're calling patterns and what kind of turnover you can be expected to have.

The consumer choice there is not to have digital

phone, and I don't think that's a great choice, so I think we have to be really careful about making a distinction about -- especially core service provision and whether or not there's consumer choice, but I'll be very brief. The second point is to look at harm.

There's a front page story in the New York Times about an elderly vet who signed up for one of these surveys and got his name on a list, and his name was sold over and over and over again to list brokers kind of as a soft target, and he lost his entire life savings, so I would say that in general, self-regulation is not effective for 100 percent of all actors in the universe, and we've got to avoid consumer harm.

And I think avoiding consumer harm means rules that apply to all.

MS. RATTE: Jennifer has had her card up for a while, and then I have a couple of more questions before we get out of the data collection, which is really the first of our topics so we'll need to speed it up here.

MS. BARRETT: I'll try and be quick, but I think it's a good point relative to there's a lot of new types of data like the grid data that's coming on the market, and I think it is imperative that industry take a look at that data and develop some self-regulation, even if ultimately it becomes formally legislated or regulated

requirement.

We're very active in the mobile area relative to the new location data and what does it mean, how should it be used, what kind of controls should the consumers have, and I think that social network data in other places where we have new types of information that we have not seen before.

I want to make one though brief comment because there's been a lot of talk about data collection, and it kind of leaves the impression that once you collect data, it then can be used for anything, and so we get into this whole debate about secondary uses, and I think we run and manage our entire business in two very separate segments: One relative to marketing and can apply standards like the DMA has relative to both collection and the use of that information and opt-out and so on, but the other side of our business, which not everyone has, is relative to risk.

And part of that is the FCRA regulated part, and part is not. It's a identify management. It's verifying someone's credentials when may sign up at a website or enter into a contract with someone, and they want to verify that this is a legitimate person. It's know your customer under GLBA kinds of rules.

And what people want is very different in those

two sectors. In the marketing area, and I often see we want all this granular data and we're worried about the secondary use of it, but the reality is if a marketer doesn't have enough data to make a profit on the cost of developing an approach, create a copy, production of it, testing of the ad and then a roll out which requires tens of thousands, if not millions of people into a particular category, they're not going to use it for marketing because they're not going to spend the money to develop a campaign that loses the money.

On the risk side, we have a different equation because when we're talking about maybe watch lists or other kinds of data, having someone on that side of the equation can be very few a number of people it can be very valuable to, and we tend to lock both of those all together and want to treat them or want to establish rules as if it was one big pot, and I think we run the risk of not ever getting to the right answer for each sector.

MS. RATTE: I think that's an important point. I want to get a question from actually someone watching on the webcast. I believe one of the panelists indicated that they use information found on the web as a source. How do they ensure that this information was legitimately acquired? I think that might have been to

you, Rick.

MR. ERWIN: In our case, the way that you phrased it as a question or phrased it, information that we found on the web would not characterize what we're doing. We find that market research surveys that are published on the web seeking people to respond to them, no different than if someone calls your home and says, I want to ask you who you plan to vote for or I want to ask you if you're a pet owner, the Internet is a very effective and efficient way to collect that information and a number of our sources do so.

And we get those sources in the manner that I mentioned before, making sure that the information that we collect from them has always been collected against our -- in consistency with our global information values, and the single most important one of those I think for this questioner is the notion that the consumer filled the survey out because it was a market research survey that was going to be used for marketing purposes.

That's our experience.

MS. RATTE: Jennifer, do you have something to add there?

MS. BARRETT: Yes, I just want to add that I think that obviously, as all American goes online,

whether we're a consumer or business, more and more data that used to be collected historically offline is now collected online, and part of our due diligence process, and it's gotten to be quite tedious, but we feel it's important to do, we're collecting information from companies that originally collected it online. We weren't getting it online, but it originated online, so we actually go out and review the privacy policies at those sites. We reviewed 60,000 privacy policies in the last twelve months. So if anyone wants to know about what privacy policies do or don't say, we have some folks that are extremely knowledgeable about it.

MS. RATTE: I think there are probably a lot of consumers out there that would want to know what privacy policies do and don't say.

I have a question for actually the whole panel, for Jennifer, Rick and Jim: Do you identify for consumers the sources for your information products? So for example, is there anyway that you communicate to consumers how your databases are enriched with other kinds of data sources, or if a consumer comes to you for some reason and wants to know how they acquired the profile, can you point them to any sources? Jim, I'll start with you.

MR. ADLER: Sure. I think that's something

we're grappling with, and consumers clearly want to know. Certain of our agreements prohibit releasing that information, and I think -- certainly I think consumers would, A, want to know what type of data, was it a commercially available public record or web procured information, and B, ideally if there's any kind of a dispute around the data, the correctness, the accuracy, they would want to know what is the source of that.

And I think we're just at the beginning of providing a level of transparency we talked a lot about transparency in earlier panels, and I think you're going to see a lot more of that. Consumers are getting much more comfortable with what's out there, but they want to know how do -- is this all of it? What is my digital footprint?

How do I gain knowledge of it, and more importantly, if there is an issue, how do I correct it if it's incorrect? How do I maybe even comment on it if it is correct? So that when someone does access it, there is a dialogue there, and they could right now I think secrecy breeds a lot of mistrust , and I think consumers don't know what their footprint is, and it nags at them, and I think we are -- as time goes by, we're going to be providing more and more information to consumers about their own footprint.

MS. GARRISON: Can I ask a follow-up question on that? You said certain of your agreements prohibit releasing the information. You're a B-to-C business. What are those circumstances where the information is not made available to consumers?

MR. ADLER: Like I said, we either get data from public records or from publicly available information or commercially, and some provisions in our contracts, the source is not one -- there's a nondisclosure provision of that contract, where they don't want that information being disclosed. I think that that very well may have to be revisited as we move forward as consumers want to know more about their footprint, they want to know where the source is so they can have a little more visibility in to it and be able to take proactive actions if they choose to.

MS. GARRISON: Rick and Jennifer, as you also answer that question, could you address that issue as well?

MS. BARRETT: Certainly. I'll speak to Chris, although he's on the phone and can't talk, he calls this data providence in terms of knowing upstream where the data came from, and we track every single solitary piece of data that we bring into the company and where it came from for lots of reasons, not the least of which is

being able to know and answer a consumer's question, where did you get my data.

And I think it is something that the industry needs to move more aggressively on. We've been dealing with the where did you get my data for years, and I was pleased about -- it's either 18 or 24 months ago when the DMA made the requirement a part of their ethical guidelines when a consumer asks a company that receives a piece of marketing material from them, what the consumer receives from the company, where did you get my name or where did you get the data that originated this marketing campaign to refer that to the source.

We actually want our clients who we sell data to to refer consumers to us, because our clients can't answer that question, and we want to get it answered, and if a consumer has an issue or a problem, we want to get to the bottom of that problem, so our consumer care group fields lots of calls relative to, where did you get my data, and we're happy to deal with those, inform them of those sources and tell them in the case of say public record or other sources exactly how to get in touch with their sources if they want to move further upstream.

MS. RATTE: Rick, did you have anything to add there?

MR. ERWIN: Only that in our experience, the consumer -- we have a similar Experian consumer services center that takes inbound calls with questions like this, but in most cases, what the consumer wants to know is not the company from which we bought it or the governmental agency in the case of public record data but rather the category, so typically our answer of is it was either a public record source from the white pages or from the census or whatever, or it was from a survey that you filled out last November or it came from a trusted company that you do business with and gave permission to use your information.

In I would say 95 plus percent of the cases that's sufficient, and we quickly follow it with a proactive question of, do you want to be taken off of our list, and if they choose to do that, then for conservatism sake, we don't simply remove them from that one source or database. We remove them and their entire household from all of our databases permanently, until they ask to be reinstated, which they sometimes do.

MS. GARRISON: On that last point, do you actually identify a particular company or do you just say it's a company that --

MR. ERWIN: No. As I said we identify the category of data it was from, and in every case I have

ever seen, that satisfies the consumer because in our experience, they're typically not trying to track down an individual company. They're simply trying to understand a little bit more about how this data is used to target advertising to them, and they're quite satisfied when they find out what type of data it is. Either at that point they're satisfied or once they have chosen to opt-out of our database system they're satisfied.

MS. RATTE: I think Pam has a comment before we get more into the issue of opt-outs.

MS. DIXON: Thank you. Our experience, just to provide a little bit of the consumer's perspective -- our experience is quite different. We spend a lot of time on the phone helping people that are having reputational harm issues, so for example, people that have been blackballed because some complete crazed person has posted ridiculous things about them on the net, usually an ex boyfriend or girlfriend or husband or wife, something like that.

These cases are very tough to tackle, and additionally, victims of various forms of identity theft come to us with very similar questions, people who have bad reputations in some of these kind of murky corporate databases where they don't have access to, they want the

company names because they want to clean up their files.

And I cannot express to you adequately how frustrated consumers are by the lack of ability to trace down the root of the data and pull it up and get rid of it.

MS. GARRISON: Thank you. I would like to turn to the opt-out, how it's -- what you offer, how you offer it, but there's a threshold question which some in the audience have asked, that is: How do consumers even know you exist and how to find you?

MR. ADLER: Can I start? I'll start with that because they can find us pretty easily. I think there's is Comscore said about 12 million people came to our site monthly, a little higher than that these days, so we're pretty easy to find. We power a lot of people's search around the web, so once they find us, then what can they do once they get there?

And we recognize that this, is a really important developing area where we need to provide -- we're going to get into opt-outs in a minute, but once they find us, then the question is, what can they do to proactively take control of their footprint.

I think it is what is coming for the industry, and we need to step up and provide that because consumers clearly are frustrated, and when they do

realize that, oh, wow I do have a digital footprint, yes, it matters for reputation reasons, and for everything that binds our society, trust and success in our society depends on your reputation, that's clearly being driven more and more online, and we need to provide folks the ability to control their digital footprint. The first step of that is to have transparency into it.

MS. GARRISON: Jennifer?

MS. BARRETT: Yes, there are a couple of different ways, and it somewhat bears our product, for instance our telephone directory that we license to large companies that provide white page online services, says powered by Acxiom and you can click on that and it takes you to us and our opt-out, so on and so forth.

We are actually moving a little bit more directly into the area of direct to consumer, and we now offer the consumer to get the same background screen that an employer or landlord might get themselves if they so choose to, and actually in today's employment market, a lot of people want to have that in hand when they go and apply for jobs.

In the marketing arena, we encourage all of our clients, as I said earlier, to refer the consumer to us if there is any question about where the data came from,

and we are referenced and linked to by most of the privacy websites so that the consumer has the opportunity to get to us via that vehicle as well.

MS. GARRISON: Can you estimate about how many people opt-out say on an annual basis?

MS. BARRETT: It varies a little bit from year to year, but it's in the 20,000 to 30,000. We've dealt over the last ten years with about a half a million consumers, either for opt-out or access and correction purposes.

MS. GARRISON: Rick?

MR. ERWIN: Yeah. I'll just add, Jennifer summed it up nicely. Our experience is about 7,200 consumers a year choose to opt-out, but they can find the link to Experian to do so, either on any of the Experian marketing websites, the phone numbers we publish, the DMA Choice service which is readily accessible.

As Jennifer pointed out, the websites of every privacy agency I've seen have links to this, as well as nearly all if not all State's attorneys general websites, and on Friday, just out of curiosity for myself because it's been awhile since I did this, I Googled marketing opt-out and direct mail opt-out, and on the first two pages there were numerous links.

So as the American consumer goes online, as most of them have in one way shape or form, there are many ways for them to opt-out.

MS. GARRISON: Let me just do one follow-up. I wanted to ask a little of each of you: What of the databases that you maintain can a consumer opt-out of, and what's the method, the process by which they can opt-out, and what exactly are they opting out of? So I know it's a three part question, which is the worst thing you can do, but, Rick, why don't we start with you.

MR. ERWIN: So first of all, they can opt-out with us in several ways. They can do it over the web. They can call us on the phone number that they'll find anywhere that we have a link for this, and when they do that, if they opt-out, they opt-out of every marketing database on which we have their name.

MS. GARRISON: Is it only for marketing or are there other databases that they can opt out of?

MR. ERWIN: Well, we have a risk side to the business as well, but just speaking about marketing data for a moment, they can call our marketing opt-out sites because the rules governing these different databases are different, and they can say, I want to be taken off of these databases, and their individual name as well as

their entire household contact record will be taken off all of our marketing databases forever, unless they call to be specifically reinstated.

Then the other principal way is that we would receive their opt-out as part of a suppression list that comes to us. For example, the DMA's mail preference service or DMA Choice provides a suppression list of opt-outs that they've captured, and we regularly, monthly process those suppressions through our database to ensure that names that came through that way are suppressed.

And then further the State Do Not Call and the federal Do Not Call Lists the same type of process flow.

MS. GARRISON: But the DMA list is a five-year period, correct, on the mail suppression? So do you honor five years under the DMA when you get the list from them, or do you in fact make it permanent as your own?

MR. ERWIN: We would honor the DMA's five year rule because that was the way in which the information was collected, and if you will, the arrangement that existed between the consumer and the DMA at the time.

MS. GARRISON: And the opt-out is tied to the consumers' name or to something else?

MR. ERWIN: To the household in which they lived

in our case.

MS. GARRISON: So which would mean household would be an address.

MR. ERWIN: Yes.

MS. GARRISON: So if they moved what would happen?

MR. ERWIN: It would follow them because in the manner in which we compile the information, we would notice where they've moved to, and if they had been an opt-out, we would not reactivate them as a marketable consumer just because they took up residence in a new location.

MS. GARRISON: Thank you. Jennifer?

MS. BARRETT: For the risks out of our house we do not allow opt-out. Opting out of -- identity verification applications, lists of terrorists and others is just not appropriate, but we do offer access and correction because we want to make sure the information is right, but you can't get off those lists, just like you can't get out of your credit report or credit file.

On the marketing side of the house, we offer both broad opt-out of everything we have in the marketing arena or granularly, as I said earlier, some of the individual products and services. It is a

forever opt-out, and we do accept opt-outs just like Experian does from DMA and others, and we honor their timeframe, whatever it is. We received also FTC and state Do Not Call opt-outs and so on.

Our opt-out is at an individual level, and but in some instances the data is aggregated by household, and when it's only sold by household if one individual, opts out, it opts out the whole household. However, there are other instances where we're selling at an individual level, a husband can opt-out, and a wife would not.

I'm sorry, what was the third question?

MS. GARRISON: The method, and I just want to clarify, the opt-out is tied to the address.

MS. BARRETT: In our instance it's tied to the person.

MS. GARRISON: To the person.

MS. BARRETT: Right.

MS. GARRISON: So if the person moves the opt-out --

MS. BARRETT: It may follow them if we know they moved. It may not, and we clearly tell them in the process when they opt-out originally, that if they move, we recommend they come back and re opt-out just to be certain.

MS. GARRISON: Then the process by which they can opt-out?

MS. BARRETT: Oh, the process is, Email us. You can call us or you can go online and download a form. We do have a form that would require you to fill out that asks for certain information. We have had myriad of experiences, interesting experiences over the years with opt-out.

One of the most interesting was an employer who sent us a list of 375 employees, including their Social Security Numbers, requesting we opt them all out on their behalf, which we promptly sent back and advised that that was not going to happen, but we do ask the consumer to sign and send in the form for the process.

In that process, by the way, I'll mention we send them a booklet which people can go online at Acxiom.com and take a look at it. It's intended for consumers it talks about how their information is used, how we use it and others, not just Acxiom, how it's collected both on and offline, and what other choices they have to opt-out.

So we feel like educating the consumer and having an informed choice about opt-out as opposed to just saying oh, I think someone said I should get out of Acxiom, so let me go opt-out from Acxiom is important.

MS. GARRISON: Jim?

MR. ADLER: So on our site, there's sort of two flavors. One is the public records side, and it's again individual. We don't have marketing lists, so that's really not appropriate, but if you want to opt-out yourself, we require proof of identity so we get the right person to opt-out. That could be by fax, just a faxed proof of identity. It's forever.

There's also on some of our sites just white pages data that you can typically opt-out online during some -- from some of our partners that publish our white pages data. There's some -- like Jennifer said, there's some information you can't opt-out of. You can't opt-out of criminal records, although we do respond to expungement requests.

Did I hit all your points.

MS. GARRISON: I think so, yes. Pam, you had some comments?

MS. DIXON: I do, thank you. I'm going to scroll back a little bit to the audience question about how does a person find all these opt-outs. It was said today let 10,000 flowers bloom. What I always says is if we have 10,000 databases blooming, how on earth is a consumer supposed to find out about all of them? It's very, very challenging, and so I have a proposal for the

Federal Trade Commission, just what you want to hear, huh?

For some time now we have really wanted to see two things: One is a registry of entities that are regulated under the Fair Credit Reporting Act; two, a registry of specialty databases that are regulated under the Fair Credit Reporting Act. I think that if the Federal Trade Commission could determine who's regulated under the FCRA, and then create such a list, I think it would help consumers enormously.

There is not an industry stomach for doing this. We've asked. There has been no appetite, so I think it's going to be left to the Federal Trade Commission to do that.

In terms of unregulated databases, I think that this is -- when industry talks about self-regulation, I would throw down the chalice and say, this is your opportunity to create your own list of every database out there, and provide a single site for consumers, and there will be challenges, but someone is going to have to do that at some point because the consumer harm here is too great, particularly with the bad actors.

There are just some incredibly bad actors out there who have never heard of the word opt-out and wouldn't even dream of letting a consumer do that, and

we have to be more worried about them than anybody else, but to get back to your current question, to kind of reel that back, there's a couple of issues that we have traditionally had with opt-outs. One is cost. I really do think that opting out for consumers needs to be free, period, end of sentence.

It's not a search, I know. They have two opt-outs. One is the slow opt-out that's free by mail. The second is the expedited opt-out, it's 20 bucks. I don't know about you, but that just doesn't hit me the right way, and I don't think that's entirely fair. I think it's worth discussing.

Secondly, the use of opt-out information for further developing a database is incredibly problematic. Under the Fair Credit Reporting Act and under the annual credit report, this kind of thing has been taken care of by the Federal Trade Commission writing good regulations.

We don't have this same regulation in the opt-out space, so there are some bad actors out there who they're like, oh, we have a fabulous database on you, make sure you're not backlisted, opt-out here. Here's all the amazing amount of information that we need for your opt-out and oh, by the way we're going to use that too, so I think that we need to have some

regulation about how opt-out works for consumers.

In terms of the third point that I would make is that if a company is operating primarily or substantially online, an opt-out should be available to a consumer online, not just by mail. There are some companies out there who the only way you can opt-out of their online products is through snail mail, and we actually have an open letter to the FTC about this issue with some companies, and I think that that's something that also needs to be addressed. It's a more subtle point, but it's still an important one.

Opting out should be easy, and I really like the idea of a permanent opt-out. Thank you.

MS. RATTE: I appreciate that Jim and Jennifer have their cards up, but I think we need to move on to the issue of access and correction, which has come up a few times today. I was hoping that the panelists, maybe starting with Jim, could talk about what access and correction rights consumers have with respect to their data products.

MR. ADLER: Right now not much to be honest, and I think the discussion of opt-out is sort of the first stage of that or at least access is important. I wanted to -- before the panel, I wanted to see how many people can run their own reports on our site.

It's a number I would like to get, and that question may come up, but I it's something that I want to run down. I think people want to know about their own profile. I think that's really important. They may want to opt it out. They may want to opt-out certain pieces of it. They may want to correct some of it, dispute some of it, comment on some of it as I mentioned.

I think that this is an area where we need the best minds to come together and discuss it. We just went through our TRUSTe audit, and it was tough, and they went through top to bottom, and the seal was issued a couple months ago now.

The reason I wanted to get them engaged in the company is that this is the beginning of this dialogue. Certainly the seal was not the objective. This is the beginning of the dialogue around how do you appropriately provide access, what should be free, what shouldn't be free, what should be some value added services that we could add on to this?

When you bring groups like this together, they have the purview of many industries. It was said this morning that trial and error is one of the best tools. There is a lot of tools in our toolbox, and trial and error is one of the ones at the top, but when you bring

in this together, they have the purview of many trials so that we don't make so many errors.

And I think that's really important when you're talking about providing consumers really valuable services like how do I get access to my profile, how do I identify who I am in order to add purview to it, and then how do I dispute certain elements of it, and then ultimately correct them?

MS. RATTE: Jim, before we move on from you, I just wanted to ask going back to the opt-out question, under what circumstances could a consumer opt out of your database?

MR. ADLER: Like the last question, all they have to do is fax in proof of identity, and it's opted out, and it's per individual, and it's gone forever, and it's free today.

MS. RATTE: How long has that been in place?

MR. ADLER: Certainly since I've been there, last year or two or three years probably.

MR. RATTE: Jennifer?

MS. BARRETT: Let's take first the risk and the non marketing and marketing products. We offer full access and correction services after authentication of the consumer's identity for all of our non-risk products, but we get very few come for accuracy, and we

actually pay a lot of attention to those for correction purposes because that says we have something wrong in the data, and if it didn't come to us wrong, then we want to know about that so it's a good quality control for us.

That offering goes back to the 1990s, back in the old IRSG days when that was part of some of the self-regulatory issues way back then.

On our marketing products, we do not offer access or correction. We offer the opt-out and we offer what we call a robust notice which is a description of the kind of data that we probably or might have in the file about you, and if you don't want us to use it for marketing purposes, then the correction is essentially a removal or opt-out.

MS. RATTE: Rick, you're nodding. Do you operate the same way at Experian?

MR. ERWIN: It operates much the same way on the marketing side, and I would just go a step further to say access and control for marketing information is neither appropriate nor practical. Jennifer did a great job of saying why it is totally appropriate and practical for credit databases and for fraud databases because if there's inaccurate information in a credit or fraud database, someone could be denied a loan or

employment or something else that they may have a right to, so the information has to be absolutely correct.

There's one thing that people could walk away understanding about marketing databases that they may not have understood coming in is that the marketers themselves do not care about the individual information therein. They care about segments of the population that would be likely to respond to a marketing offer because they just want to be more successful and more relevant to their clients.

The challenge that we have with access and control for market databases is there is no one standard of truth that could be established, and unlike in the credit and risk world, it's not as important to a marketer to be that accurate, and most of the marketing information in our databases is presented in estimates or ranges, and that's good enough for marketers so that they're not marketing women's clothing to men or vice versa, things of that nature.

So access and control is just sort of not appropriate in the marketing world, but to allow it would open it up to a standard of accuracy that would violate our own values. We couldn't ensure the accuracy of the information when it was provided by somebody who you couldn't verify of course.

MS. GARRISON: So to follow-up on that point, then if you had really good robust demographic information, would that satisfy the marketer's needs? You said a moment ago that it didn't need to be that accurate, but you just need to be able to make these distinctions between say a man and a woman when you're marketing clothing.

MR. ERWIN: Yes, and I used that example as a broad category of demographic. The same thing would be true of age and estimated income and things of that nature.

MS. RATTE: Over the past couple of panels, we've heard about new tools such as the Google ad preferences manager that allowed consumers to go in and tinker with their marketing profiles, and in a lot of cases we're hearing that rather than going in and opting themselves out, consumers are in some cases adding to the information, and actually giving you more.

So do you see a demand for consumers to update the marketing preferences in this context? Wouldn't you want more accurate information if you could get it?

MR. ERWIN: Well, their preferences and what the information itself is are two very different things. I think when we talk about preferences, certainly we at Experian believe that we're always working towards

better notice and choice and adherence to consumer's preferences, and an example of that is just the way the DMA has moved from a mail preference service to one that in the future will enable opting out of individual brands offers.

So preference is one thing, and yes, we broadly support -- we will never stop improving the amount of preference that we make available to consumers about how they're marketed to. We believe that's one of our values.

MS. RATTE: Pam's had her card up for awhile.

MS. DIXON: Thank you. Thank you very much. I just want to make a couple statements. I think Jennifer has said something that is important that needs to be listened to, and that is that the risk databases are different than the marketing databases.

I think she's right, and something that we've said for quite some time now is that there's a bit of a risk loophole. If you look at any statute, there's usually an exemption for risk based databases or risk based consumer data to be collected and used, and it's really hard as a public policy to have a position against this because there's good evidence that some of that data is useful.

Here's where the problem is, and I think here is

where the Fair Credit Reporting Act like structure or something similar to that or taken from that mold would be very helpful.

So, for example, let's say we have -- I call it the risk loophole or the antifraud loophole, so we have a risk database. What's your product name?

MS. BARRETT: We have several, Identity Verification.

MS. DIXON: So let's talk about Identity Verification. We go to Identify Verification database. There's also a company named ID analytics that does this, so these are folks who are just trying to verify identity for employment and other purposes, probably law enforcement purposes as well.

I know several healthcare providers that are using these kind of structures to authenticate doctors and patients so we can't stay no to this, but I think what we can say is this: Okay, we're going to let you use this consumer data that's risk data, but we're going to regulate it, and here's how we're going to regulate it.

We are going to say that the data is going to be subject to governing laws that require permissible purposes. The permissible purpose is anti fraud. You can't then take the anti fraud data and use it for

marketing purposes or other purposes, and I think that companies like Acxiom would have not any problem with this because they're not doing that.

So if you have good actors, I don't think this kind of regulation will be a problem, but we've seen very small companies put up a shingle, and I'm talking like one and two persons shops, and saying we're anti fraud specialists, give us your data and we will work with it. Yeah, they'll work it, but not in ways that the company working with them or consumers would expect.

So I think that there can be some regulation of risk products that's very beneficial to the entire sector. I think that's it for now other than I would say that the one push back I would give to you respectfully is that I do think that categorization of data is becoming much more granular, and I think we're really entering a world where we're micro targeted as opposed to the broader segments of the past.

I think that's something we'll see change either now or tomorrow.

MS. RATTE: Okay. Jim, you had your card up or Jennifer?

MR. ADLER: Jennifer, do you want to go?

MS. BARRETT: This is just to kind of follow up to Pam's comment. We wouldn't object to regulation on

the risk side. In fact we're already regulated because one of the things we do is, as part of those risk products, we include credit header data which is upstream regulated by the Gramm-Leach-Bliley Act which can only be used for fraud purposes, as she said.

Now, if you don't include that data in a risk product, then you may be outside the scope of that regulation, but I think most of the big providers do because it's a great source of identifying kinds of information that's very current and very accurate.

MS. RATTE: Okay. Jim?

MR. ADLER: I just want to reel it back to what Alan Davidson talked about on the Google ad preferences. As he said, it's still early, but people are not panicked and not opting out, but they feel quite empowered by those kind of tools.

One of the things that we are introducing is a streamlined opt-out for vulnerable populations. We recognize that information is powerful. We're working with domestic violence groups and elected officials, law enforcement to make sure that their opt-outs are streamlined, and as we get our arms around making those tools useable, we would grow them into a consumer offering as well.

So I think there's a lot of innovation to be

done here, and it all centers around, hey, what is my profile, being able to identify it and then access it and control it and have direct influence on it, and I applaud what Google is doing and we are trying to do something similar on our site,.

MS. RATTE: We have one minute left, so I'll just do one more question, and this sort of plays off the point that Pam just made, but also some conversations that we've had with the folks on this panel informally about what they're doing to screen their data suppliers, and we understand that there are a number of data suppliers who don't meet your standards, so you won't purchase from them, which means there are actors out there that aren't playing by the rules.

So I'll close with the question: Do you favor increased regulation in this space and if so, elements should the new rules include? I throw it open to the panelists? Anyone?

MS. BARRETT: I'll start it. I don't know that we need new regulations but what we're doing is screening -- well legally, are they collecting the data is a legal manner but then also what does the privacy policy say? And if they have a posted privacy policy, I view that as something that the FTC could already take action on in terms of understanding: Are they following

that policy appropriately.

We also where -- if we encounter a policy that we're not quite comfortable with, we actually try to work with the company to say, we think you should fix it this way, and it's all shades of sort of gray. It's not really clear to -- they don't even say it or they say this and do that, so there are various aspects that we feel like in certain instances we can just work with them and improve the process.

MS. RATTE: Anyone else? Pam?

MS. DIXON: I think self-regulation has brought in the larger companies but not the smaller companies where so much harm has accrued. That's where you see the really bad actors, just the ridiculous cases of harm where consumers call us and their lives are a wreck. I think we all would like to avoid that.

I think the only way to do that is at this point is through some kind of model that takes a Fair Credit Reporting Act like approach and says, Look, here are permissible purposes, here are non permissible purposes, and we'll have to be nuanced, and I'm not saying this would be easy, but I think it's an approach that would have a very good chance of working.

I think the Fair Credit Reporting Act has been a very good privacy law and has been very functional and

helpful for consumers, and I think that it provides business with reasonable guidelines, and I think we can do the same thing here.

MS. RATTE: Okay. I think our time is up so in closing I would like to apologize for Chris Hoofnagle and invite him to submit any thoughts or reactions to the panel discussion through our written comment process, and please join me in thanking our excellent panelists. It was a great discussion.

(A brief recess was taken.)

PANEL 5: Exploring Existing Regulatory Frameworks

MODERATORS:

JESSICA RICH, Deputy Director of Consumer Protection, FTC

PEDER MAGEE, Division of Privacy and Identify Protection, FTC

KATHRYN RATTE, Division of Privacy and Identify Protection, FTC

PANELISTS:

J. HOWARD BEALES, III, Associate Professor, George Washington University School of Business

FRED CATE, Professor, Director of the Center for Applied Cybersecurity Research, Indiana University School of Law, Bloomington

CHARLES CURRAN, Executive Director, Network Advertising Initiative

MICHAEL DONOHUE, Policy Analyst, Organization for Economic Co-operation and Development

EVAN HENDRICKS, Editor and Publisher, Privacy Times

BARBARA LAWLER, Chief Privacy Officer, Intuit

MARC ROTENBERG, President, Executive Director, Electronic Privacy Information Center

IRA RUBINSTEIN, Adjunct Law Professor, New York University School of Law

MS. RICH: Okay. We would like to start panel 5. Everyone take their seats please. Hello. So I'm Jessica Rich of the FTC, and these are my co-moderators, Peder Magee, Katie Ratte, who you met from prior panels, and we're hoping that this last but not least panel at the end of the day will be the best, and keep everybody awake and send you away with good thoughts.

On this panel we're going to explore the virtues and the drawbacks of existing regulatory frameworks and how they might help us think through the issues. Obviously the existing laws and the approaches that have been taken are highly relevant as we think about future approaches.

Questions we want to think about are: What have we learned over the years as we've implemented and applied various privacy models? Have these models kept pace with our changing daily landscape? What's missing from these models? Are there elements that need to be added? How can we use our experiences with these models to identify privacy approaches that will work well in today's world and would also stay flexible enough to accommodate changes in the future.

I have a really outstanding panel to help me discuss these issues, an all star privacy panel. In alphabetical order, we have Howard Beales. Howard is a

former Bureau Director at the FTC, as I think most people here know, and he's currently a professor of public policy at GW. He's one of the principal authors with Tim Muris of the so-called harm based model for privacy which we'll talk about.

Fred Cate is down there. He's a professor of law and director of the Center For Applied Cybersecurity Research At Indiana University. He's also senior policy advisor to the Center For Information Policy Leadership at Hunton & Williams.

Charles Curran, known as Chuck, is the Washington based executive director of the national -- the network advertising initiative or NAI. He leads NAI's efforts to develop and enforce self regulatory standards for online behavioral advertising.

Michael Donahue, I can't even see Michael, there you are. Since 2001 Michael has been a policy analyst at the OECD, specializing in privacy, information security and consumer policy. He's also a former FTCer, not that we wouldn't have invited him anyway.

Evan Hendricks is the editor, publisher and founder of Privacy Times, a Washington newsletter that covers a wide range of privacy subjects including the Fair Credit Reporting Act, actually most notably the Fair Credit Reporting Act. .

Barbara Lawler is chief privacy officer at Intuit , and Quicken and QuickBooks and former CPO at Hewlett Packard. She actually rolls up her sleeves and does all the things that we're talking about, so we want to hear from Barb.

Marc Rotenberg is the president and executive director of the Electronic Privacy Information Center, EPIC, and one of the most vocal and visible privacy advocates in the world I'm going to say.

And Ira Rubinstein is a senior fellow at the information law institute and an adjunct law professor at NYU Law School, and he spent 17 years at Microsoft also as one of its main regulatory and privacy lawyers, so all of these people bring enormous experience in privacy and have been around during the various privacy debates over the years, so it's wonderful to have them on this panel.

Let me just lay just a little bit of ground work for what we're going to talk about which is most people here know that the U.S. has a number of laws governing privacy in certain sectors, the so-called sectoral approach. Laws include the Fair Credit Reporting Act, HIPPA, Gramm-Leach-Bliley, the FTC Act which we've used in the privacy and data security area, even though it's not an inherently a privacy -- it's not inherently a

privacy statute, and many, many state laws.

There's no general privacy law in this country, and so the FTC at least in applying the laws that we enforce has used a combination of enforcement, education and encouragement of self-regulation and has used basically two approaches over the last two decades in doing this.

The first is the fair information practices approach, and as I think you'll hear from some people on the panel, we have our own version of the FIPPs, and they differ from other versions of the FIPPs, and ours was notice, choice, access and security, and the focus of that approach was on transparency, consumer choice and accountability, and during the time period we were supporting the FIPPs, which was primarily in the '90s, but actually many of the laws we enforce are at least partially based on the FIPPs.

We also supported at least at a certain time legislation based on it so it presumes legislation and self-regulation based on these FIPPs. So also the other approach that has dominated the FTC's thinking is the harm based approach, and that focuses on enforcement of existing laws based on an assessment of tangible harms with the goal of reducing or stopping those tangible harms.

In thinking about the issues as we go forward, we obviously also want to look at other models, not just the two models that have dominated the FTC's thinking. There's the EU data directive. There's the more traditional FIPPs model which is actually something that DHS has been implementing recently. There's the APEC privacy framework, and there's the EU U.S. safe harbor and safe harbors in general that need to be considered in at least self-regulatory approaches, so that's just providing a little background for our panel, and so let's go at it.

I would like to talk first about the fair information practices which is really the grounding of a lot of privacy thinking in law and kind of give an overview of its limits and its benefits and maybe ask Fred Cate to do that.

MR. CATE: Thank you very much, and thank you for the opportunity to be here. Frankly the sort of notice and choice model has come under such attack all day long, I almost feel guilty adding to it at this point, but I will overcome that.

I think we can really focus on three areas of criticism. One is that we've tended at least tentatively in the U.S., although I think it's almost equally true in Europe, so I wouldn't limit myself to

the U.S., to reduce a broad range of FIPPs down to a far fewer, and realistically I think for many companies it's really come to focus on notice and choice as being the two that have been the greatest focus on , and frankly I think the Commission has put a great deal of emphasis on notice and choice.

So to start with, we have the problem that we're not using the full FIPPs approach where we've cabined it down too small, and in some ways -- some of this really goes back, this has been a U.S. view of privacy ever since Alan Westin wrote privacy and freedom and said privacy is the right of individuals to control uses of data about themselves.

So there's a long and rich heritage to this. It's just a very narrow view towards privacy, especially today. I believe a second problem with this is that it hasn't worked terribly well in practice, and there's lots of reasons for that. People don't read the notices. They don't understand the notices. They're not equipped to make choices.

They don't care when it comes time to actually make the choice. They become like those click through screens. Do you want to download the software, yes or no. You click yes, you get it, you click no, you don't, so it's not really a choice anyway. It's really just an

illusion of choice.

Because of the Commission's approach and also states treating notices as legal contracts, notices have gotten more and more cumbersome and complicated and detailed and therefore less and less intelligible for average consumers, so there are lots of examples. I don't think I need to belabor this I think other people have made this point well today.

The third I guess I would point to is it's forgetting that consent or notice and choice are only tools, that they really shouldn't be the goals of privacy protection. If you said to someone, why do you want your privacy protected, there aren't many people, and certainly outside of this room, there probably aren't any people, who would say because I want my control enhanced.

They want privacy protected so they won't be harmed. They won't be injured. They won't be affected in a certain way or an unexpected way. It may not be a tangible harm, but I think few people would say that the goal for them of privacy protection is that their choice will be enhanced. Rather they want their data used predictable in less harmful ways.

Another maybe example of that is look at all of the things we exempt from the choice model, so you look

at a law like Gramm-Leach-Bliley which really effectively only gives consumers one choice to opt-out of the transfer of information to third parties for certain limited marketing purposes.

The entire law otherwise leaves everybody absolutely free to do what they want with data, provided they have a notice, and that just seems the ultimate in non privacy protection dressed up as privacy protection. Let me stop there.

MS. RICH: Well, perhaps then we should roll back and talk about the FIPPs as the model exists elsewhere, that's not so limited to notice and choice, and what benefits that approach brings, and I'll ask Marc Rotenberg to launch that and maybe Evan to follow-up after Marc.

MR. ROTENBERG: Well, thank you, Jessica. I also want to thank the FTC for putting together this very important event. I want to mention I think it was unfair to charge us for coffee. Now you know there's a lot of TARP money out there, in fact $200 billion more than they thought yesterday. Maybe some of that for future FTC privacy roundtables could go for a coffee fund.

MS. RICH: Next time you testify, if you can work that in.

MR. ROTENBERG: I will.

MR. HENDRICKS: It's not the Treasury Department.

MR. ROTENBERG: I think the FTC needs coffee money. Let's just think for a moment. I think we took this terrible detour on privacy protection in the United States that began roughly ten years ago where we looked at fair information practices and we know what they were because they came from the U.S. The most famous example of the establishment of fair information practices turned out to be the European privacy laws, the EU directive.

But the EU directive was based around a set of principles that were developed in the United States in the early 1970s where people begin to think about the long-term consequences of automating personal information, and they had a lot of very good insights. They didn't say, for example, we're terribly afraid of privacy, therefore we should prohibit the automation of personal information. They said, we need a regulatory framework that makes it possible for us to make use of this new technology and safeguard privacy.

That was the starting point how people thought about fair information practices, and they said therefore we're going to establish a set of ongoing

obligations for organizations that choose to collect and use personal information, and if they choose to collect personal information in an automated environment , these obligations are going to include things like record accuracy and update and use limitation, no secret databases, and all those things and we will give individual's rights.

They'll get to know about the collection and use of their personal data. In this regulatory scheme purposely asymmetrical because it recognizes when you transfer your data to an organization, the organization now has control of a little bit of your life, right, some private details about you, and you have some right I think to expect that you're going to be able to exercise some control over that.

That essential understanding of the purpose of fair information practices, which you will find by the way in most U.S. privacy laws as well as the EU directive, was essentially ignored, papered over, tossed in the back closet, thrown over the ship with concrete attached around the legs, to construct this new model of notice and choice to enable self-regulation.

And notice and choice was based on this wonderful myth. The myth was that if we gave consumers enough information about how their data was going to be

used, they would begin to exercise market force to encourage companies to adopt better privacy practices.

It exists not as a paired down version or as a partial version of fair information practices, but actually in opposition to fair information practices. It's a completely different approach, and we've run this experiment for ten years, and I listened to the people on the earlier panels talk about the need for experiment.

Well, I believe in experiment. I think experiment is a wonderful thing, but is there anybody today, ten years later, who believes that this approach to privacy protection works? I don't think so. I honestly don't.

So I think what we need to do is recapture the essence of fair information practices, and I think if we do this, some marvelous things will start to happen, because one of the other lessons we've learned over the last ten years is that where you have enforceable privacy regulations, businesses get very clever and technologists get very clever, and they come up with ways to deliver products and services that don't require the collection of so much personal data.

They find innovative ways to enable payment schemes and viewing and everything else online that

doesn't put such a heavy tax on the collection and use of personal use data, so I think if we get back to that point I think a lot of these other problems that we're having today, with privacy and new technologies actually become easier to solve.

MS. RICH: Before I go to Evan, let me just ask you, though I understand some of the data minimization and data retention policies obviously that goes beyond a notice of choice type of regime. But when you're talking about no secret databases providing access to consumers, transparency, what are alternatives besides notice of a concrete way to implement those things in a way that would be enforceable by a regulation?

MR. ROTENBERG: 25 years ago I wrote a bunch of laws that incorporated all of those elements. Data destruction is right there in the video privacy protection act of 2711, I'm sorry that's the section title, 18. But the year is 1987. We had data destruction, we had minimization, we had use limitations, I mean all that stuff. The way you write a privacy law is by looking at the list of fair information practices and trying to figure out, you know, how many you can incorporate into a statute. That's the way the privacy guidelines were done in the '84 Cable Act. It is not the way it was done in

Gramm-Leach-Bliley. I joke with people, the wonderful think about privacy with Gramm-Leach-Bliley is you get all these paper notices, you can tape them over your windows and you have a little more privacy in your home, but that's not the way the law was supposed to work, right?

MS. RICH: But I'm saying, and maybe somebody can help me here, that to a certain extent statements which are principles like no secret databases, providing consumers access and must be transparent, that for many people inevitably leads to notice, and if there's different ways to do that, to create transparency, other than notice and other than some of the creative things we are trying to do in behavioral advertising with an icon and all that, we should talk about that.

MR. HENDRICKS: Well, I think that's a good place to start because when we first started fair information practices in 1973, the first rule is there should be no secret databases, and we've come full circle now because in the online environment that's what we're doing. There's lots of -- and the differences might not be your identifier, although that's ultimately the goal, getting personal identifiers, but if it's tied up to your IP address or your device, it still can identify an individual user.

So the point is I think the answer is that you put the fair information practice principles into law and make them enforceable, and it's good in a way, I agree with Marc that we took an unfortunate turn away from the full set of fair information practice principles.

Now, it's good news because the FTC has tried every other way. They tried FIPPs light. They tried notice and choice. It didn't work. We saw Gramm-Leach-Bliley notices when you don't have full information practices. That didn't work, and it ended up generating more confusion and not protecting privacy.

We seen certain voluntarily things like the IRSG principles. You've tried every other way, so what are we specifically talking about? I think we're talking about fair information practice principals. We're talking about not just -- the only thing is this is about government regulation. Yes, you're putting duties on organizations if they collect personal information, but you're also giving rights to individuals.

And the thing is if you're an organization and you're collecting information, the online world connects someone to their device or their individual identifiers, you have to create a right of access, and you can do that with a beacon to say, this entity is collecting

information about you, you can see what they got.

That's a great starting point to start overcoming the secret database problem. I think that's where we all have to start. I think you heard a theme all day long from people, we're part of a coalition, the privacy coalition, working with Jeff Chester, Pam Dixon, Susan Grant.

Also said we would like to see based on our best law in terms of fair information practices is the Fair Credit Reporting Act, and we're not talking about credit reports, but those principles of access to your information, correcting it when it is wrong, data use limitation and purpose specification, is this only for advertising? It may get enforceable. It can only be used for advertising.

If it's only for advertising, there's certainly less chance of harm than what we're seeing coming out of the reports today of Sprint providing 8 million data points to a government site, it's information professionals know that information is collected, they will come to get it one way or another whether it's the government, whether it's a divorce lawyer, other civil attorney.

And I think in closing the security, where the FTC's done a good job by using privacy polices to pin

security duties on companies, but the other thing is enforcement. I think whenever you're talking about something or collecting information on hundreds of millions of individuals, individuals have to be able to enforce their own rights.

And the Fair Credit Reporting Act, we have a private right of action and you have attorneys fees, and that's appropriate in that context I think we have to look very hard at that because I don't see any way where no government agency will ever be big enough nor would we want it to be to enforce rights for that many individuals.

We also have other models, the National Labor Relations Board is a way where people can go to have a government agency investigate for them and see if their rights have been violated, and we talked about how Tim Muris and Howard Beales brought us the harm test, but they really became folk heroes when they created the Do Not Call list. The do not call list was ten years overdue, and it brought an easy way for individuals to enforce their rights under a ten-year old law, and people didn't really have an enforceable way of enforcing those rights until they created that, so that's another model that we need to look at.

And so all those principles are there. I think

we tried everything else. The chickens have come home to roost, and now it's time to do the right thing.

Thank you.

MS. RICH: Marc mentioned the international, and it's highly relevant to what we are talking about, so, Michael, maybe you can talk about the common principles in international frameworks, and they are going to be a little different, but that you're working with OECD, APEC, whatever you want to talk about that could inform our work here.

MR. DONOHUE: Thank you, Jessica. It's really quite simple in the international environment as I will show you. This is a chart that was prepared by our colleagues in the Spanish DPA in advance of a project that they've been working on to develop yet another new international standard, and actually it does look complicated, but really it's simple because what you don't see are too many white spaces.

That's simple because it means that most of the different international instruments that are out there do reflect the same basic fair information practices, although obviously the way they've been implemented in national legislation differs.

But to take a very hurried tour through some of those, I'll start naturally at the OECD where in 1980 we

developed a set of guidelines that have so far we think stood the test of time. At the same time many people who were running back and forth between Paris and Strassburg to go to the Council of Europe to develop convention number 108 which has many of the same basic principles, although it's a binding convention rather than guidelines as we have at the OECD, so those were sort of first generation of principles.

The OECD ones were not so familiar in the way in which they read now, although the underlying content is similar. The first is collection limitation. I won't go through what each of them mean, but data quality, purpose specification, use limitation, security safeguards, which we have heard a lot about, openness, individual participation and accountability.

The guidelines also have a section covering trans border data flows as well as unfair discrimination, which don't get very much attention but which are there as well.

Now, of course there have been other international instruments that have come into play since then. The UN has a set of guidelines dealing with privacy. We've already heard about the 1995 privacy directive from the European Union, and some of the principles that you don't see articulated as such in the

OECD that come from those instruments include a notion of proportionality, the protection for sensitive information, and independent supervision.

So those are some other principles that are out there in the international space. More recently of course APEC worked to develop its own privacy framework which is very much modeled on the OECD, but also has this focus on harm which is not present in the same way at the OECD, and finally our colleagues in the data protection community have come up with a standard released just last month where they're trying to show the feasibility of getting real international agreement on a set of principles.

Most of them would be recognizable from the design to pull together the various instruments there. There are some new things in there in terms of what they're calling proactive measures which focuses on issues like privacy impact assessments, codes of practice, educational awareness and all other kinds of internal governance mechanisms so that's sort of a novelty in some respects for an international standard.

Maybe I should say one last thing is that we've done a number crunching at the OECD to realize that the guidelines are turning 30 next year, so we going to be celebrating that an anniversary but also taking a hard

look at some of the changes many of which have been described over the course of this day and preparing report.

That will then feed an actual review of the guidelines themselves, so I very much hope that we can take advantage of some of the insights that are being gathered here, elsewhere in Europe as well. The European Commission has begun a consultation on some of these very same issues to look at how best to address privacy going forward.

MS. RICH: Thank you. Barb, so Michael is talking about all these efforts to develop an international standard. How has the increase -- first of all, the increase in multinational companies and the increase in trans border data flows for reasons of cost and other reasons? How has that changed company's view of the need for an international standard?

MS. LAWLER: Companies are really interested and concerned about trans border data flows is because of, as we've talked about, the multi-dimensional nature of data. Data moves around the globe in an instant. If we actually use the example of a data center, many, many multinationals are consolidating data center and large processing operations in let's say in Texas.

So let's say your major data center is in Texas,

but there's isn't a responsible multi national company that doesn't have one failsafe or fall over data center if not two, then more than likely that would be in another country location.

When we think about the idea that data is in one place, i.e. the main data center but also has backups in the backup data center, what you really have is a situation where the data is in one place and in many places at the same time.

It may be unsettling to think about the idea that in some ways, data is never really at rest, so when you think about the idea that data is in one place and in many places, around the movement and management just simply of data centers and then the potential for different conflicting overlapping nice matrix -- I really appreciate you sharing that -- most companies actually have to build their own specific matrix that adapts and looks at what are the state requirements, what are the federal requirements, what are all the different country requirements, and try and make some actual common sense of the requirements and at the end of the day, it's incredibly complicated, time consuming, inefficient to do that.

We know our customers are asking and demanding full-time 24-7 availability, so international standards,

not five international standards, which we kind of have now, but some sort of harmonized standard is really something that would not only benefit business but ultimately provide more consistent experience for consumers.

MS. RICH: Okay. So we'll come back to the fair information practices, but let's move over and talk a bit about the harm based model, and we have the perfect person to talk about it, Howard Beales, so why don't you tell us what it is and why you -- well, you talk.

MR. BEALES: Okay.

MS. RICH: Howard is my former boss. I'm not going to tell him how to exactly say it.

MR. BEALES: Thanks, Jessica, and thanks for the opportunity to be here today. Let me begin by pushing back a little about your description of what the model is.

MS. RICH: I knew you were going to do that.

MR. BEALES: I don't think there is anything in the harm based approach to thinking about privacy that says we can only -- it can only deal with tangible harms.

If you think about the very first case we brought under the consequences based approach, it was a case against Eli Lilly that involved the release of

Email addresses of Prozac users, a lot of them .GOV addresses, and there is no tangible economic harm that goes with that as far as we know or knew or still know.

There is a subjective preference on the part of many people that that kind of information shouldn't be out there, and that it seems to me is what that case is about. Subjective values are important in a lot of places. They are important guides to what we do in the economy in products and services, and privacy is no different about that.

What's important about subjective preferences though is you have to think about them a little bit differently, and you have to be sure that it's a real preference expressed in the marketplace. Think about an analogy for a clear subjective preference, which is products that are kosher. A lot of people care, completely, completely subjective. Yeah, there's a difference but it's a subjective preference, not one that's got tangible economic or health and safety consequences. It makes perfect sense to protect that preference for if you sell somebody something and say it's kosher, it better be.

It makes very little sense to say that because some people have a preference for kosher, all products should be kosher, and that's sort of the leap that's

happening in the privacy debate. We're saying there are people out there that really care about privacy, no doubt there are, and therefore all of the information, products and services have to satisfy those preferences for everyone. That's a big leap and a very different approach to thinking about the subjective value than what I think makes sense.

The second thing about the consequences based approach is I think it makes you think about what you're trying to accomplish that I think is an extremely useful -- extremely big part of its value and Do Not Call was maybe a good example. If you think about Do Not Call in the conventional privacy approach, well, this is a secrecy problem. Hide your phone number, don't let anyone call you and you won't have any problems.

It doesn't work that way. If you think about it as what we're trying to avoid is a phone call that I don't want, it points in a different place as to how you address the problem. Part of the reason it's important to be clear about what is the harm is what is the harm is going to affect the most effective and the least cost ways to avoid the harm, and so unless you can be -- unless you can articulate the particular problem that you're trying to fix, what it is that you're trying to

protect in this subjective preference or objective, it's going to be very difficult to come up with a solution that works to address that problem.

I mean, one of the examples of that that's been talked about a lot today is this first-party, third-party distinction. What exactly are we trying to protect there? Is the problem the sharing of information or is the problem the existence of the information, that there is a database that includes this information?

If the problem is existence and the potential for access by hackers or governments or whoever else, the first-party third-party distinction doesn't make any difference at all. It simply doesn't affect the consequence.

If the problem is sharing, then well let's focus why is the sharing a problem in that particular context where the information is going to be shared lots of places along the way of doing things that we all think ought to happen, like the transaction actually ought to get processed.

MS. RICH: Howard, can I ask you: In the harmed based model, who decides? Does the harm based model provide clarity to companies as to what their duties and obligations are? Is it the regulator that decides after

harm has occurred? What is the -- what the guidance that you put out to companies trying to protect privacy?

MR. BEALES: Well, it seems to me that the fundamental guidance that you put out is don't use information in ways that are going to be damaging to your customers or damaging to the people that are the subject of that information. I mean, I don't think it's that hard a principle to follow.

It's not substantially harder than don't write deceptive advertising. Yeah, it lacks a certain specificity. It doesn't tell you what is the type size for a particular disclosure, but I think it's pretty clear what people are supposed to be doing. Don't use information in ways that is going to be damaging to your customers.

MS. RICH: And as in Eli Lilly, if they didn't have a deceptive statement, that was a deception case, would that -- in the absence of new laws to make clear what's harmful, would the FTC have brought an unfairness case to say that that is illegal?

MR. BEALES: Well, as you know in -- my great regret was you didn't find the unfairness case and information security until I was out the door.

MS. RICH: We found it. We were just investigating.

MR. BEALES: Yeah, I think you can bring that case as unfairness, if there's really something going on there but you need to be -- you need consumer behavior in the marketplace, choices consumers really made or tried to make, and not survey data that say some people care at best.

MS. RICH: Marc, you're knitting your brow, so I think you need to say something.

MR. ROTENBERG: Boy, Howard, I miss you. So let's just think about the problem with trying to approach tangible harm to privacy. If there is a tangible harm, financial which is something that courts like, it's almost by definition not the privacy harm. In other words, when we're talking about privacy or the loss of privacy, the interception of a telephone conversation, the disclosure of someone's HIV status, I can't imagine how we begin to assign a dollar value in the abstract.

We can say, oh, the person lost the job. Then we sit down and sort of figure out what the value of the job was, but that's somehow apart from the harm that we think of as the privacy harm, and so the answer to this question again, and you have to go back a little bit but it's there, is that privacy laws have traditionally set out stipulated damages, and they have said we don't know

what the exact amount is. For example, when someone receives an unwanted telephone solicitation after they've told the company they don't want the unwanted telephone solicitation we'll say $500, and that's exactly what Congress did in 1991, and it led to some enforcement action and eventually led to your Do Not Call List.

But that's a very concrete way of trying to understand how we create effective mechanisms for enforcement, so I appreciate it. I mean, it's not always been quite so literal and certainly in the Prozac case it wasn't.

But I want to put one other issue on the table, because if we don't get to it today, I think it'll be unfortunate. Construction of privacy law in the United States is not just about isolated harm to individuals. We tend to talk about it that way. We tend to talk about a person's personal interest in their own data, and the discussion gets very kind of individualistic.

But the origins of U.S. privacy law actually started in a very different place. The big concern in the United States in the mid 1960s was the creation of a large centralized database. People said they did not want the government to have a big database on everything that they were doing, tax records and pension accounts

and everything else. So what eventually emerged was a structure of privacy law for the government to try to compartmentalize all of these different activities to avoid a centralized system of profiling and a tracking of individuals.

I think it's pretty reasonable to begin the discussion at this point as we think about the role of privacy law, in addition to the impact on individuals, how do we feel about very large corporations that are creating exactly the same type of databases that breakdown these comparments in our private lives that build these detailed profiles that are almost exactly the reason that we develop privacy laws 40 years ago, and actually I would be interested in your view because I suspect with respect to the government activities, you would agree that we try to keep these partitions in place.

That seems to be that was exactly the distinction that was made in those laws is between government databases and private ones. There was -- it's not like there wasn't data matching going on at the time on a pretty extensive basis on offline data with catalog data exchanges and a whole host of other things.

It wasn't -- this isn't a new problem. This isn't something that's just emerged with the Internet.

It's something that's gotten new attention, but it's the same beast, and that was the decision that was made.

We want to treat the government differently. I do think that makes a whole lot of sense to treat the government differently, and some of the things like notice are that are really important when it's the government because you want somebody to be able to find out what the government is doing this with the information and be able to say that that's a problem are much less valuable when you think about an individual consumer finding out about how the data is going to be used.

It's not the same value that's being advanced by the provision of notice in those two cases.

MS. RICH: Can I just ask, let's see, Fred, to comment on -- perhaps to expand on this notion of uses of data that may not be covered by the harm based model because I don't think we've given out some specific examples of that, and I know you've written on this, Fred?

MR. CATE: Thank you. I want to start by echoing Howard's point which probably makes Howard now incredibly nervous, but once we say harms don't have to be limited to tangible economic or physical harms, you then have a much broader approach under this harms or

Howard has used the term I think consequences based approach, so you can identify there are certain consequences, there are certain results which we are going to say would trigger regulation.

And just to tie this back to the earlier discussion, you would in those areas potentially say choice is not an option. There's some harms which are simply so harmful we don't give you the choice about them, so think about most consumer protection law. You walk in to buy a television. You can't consent to be defrauded in the store. The FTC doesn't offer you that option, that you can consent to receive fraudulent advertising or false or deceptive advertising.

So in some areas, not across the board, I wouldn't suggest that for a moment -- but in some areas we can undoubtedly say they're just certain activities that really should be off the table or certain obligations that should attach irrespective of consent. I think security obligations would be a good example.

There are also activities which frankly consent just doesn't seem relevant to, not because the activity should be either expressly permitted or expressly prohibited, but because consent doesn't seem like a useful model.

The example which Barb gave, which I think is a

terrific one, about back up data, currently under our approach to privacy policies, we would expect the company to describe this to the consumer. We use a third-party to back up our data. They may store the data some place else, here's how they would do it. Then we would ask the consumer to consent or engage in the transaction knowing this.

I don't think there's a person on earth other than maybe Marc who would actually care about the details of the backup data. What we want to know is the backing up of the data is done pursuant to certain substantive obligations, and if you don't meet those, there's enforcement of those, not a description of the type of backup tape you use and do you consent to that or not. If it's Cobalt, that's okay, but if it's not, you want something else.

MR. ROTENBERG: If it's Cobalt you don't want to consent, trust me.

MR. CATE: Thank you. I go to Marc for all my purchasing decisions in the technology world. Again if I can make one last point, and I will shut up, which is to my mind it's the structure and the process that matters frankly more than the specifics; in other words, we might disagree on what goes in what bucket, and there would be a lot of room for disagreement, but if you had

a rule making procedure or some process by which you could debate that, you could do something just like this but in a more focused way.

But the point that matters is that there is agreement that there needs to be some area that's outside of consent and that there is a process by which to identify that, and frankly to keep updating it, to keep reviewing it so that you don't lock in something in one law that's there forever.

MS. RICH: Well, that's right and that's one of the things that the who -- I guess the harm based model still leaves you with the who decides because it's going to be the FTC enforcing the FTC Act unless you have some structure in place, especially if you broaden the concept of harm and it becomes everything.

Let me before we --

MR. BEALES: It doesn't become everything.

MS. RICH: Okay. We're putting words in Howard's mouth. Now it's everything out there. I think Fred has forecast that there's some new possibilities for a model we can talk about where we take certain things off the table as was said in a prior panel.

Before we get there we want to talk a little about is self-regulation because there's been a lot of discussion today about that self-regulation hasn't

worked, it's been ten years, et cetera. We do have a lot of experience with self-regulation. We have two people here, Ira and Chuck, who will be able to tell us a lot about self-regulation.

I want to ask Ira, just overall, I know you just wrote a big article about it, how effective have self-regulatory approaches been in the current environment, and does self-regulation need to be backed up to be meaningful? Does it need to be backed up by government regulation, and otherwise how do you deal with people who don't join?

MR. RUBINSTEIN: Thanks, Jessica. Let me make three points about self-regulation. The first is that it's been widely criticized not only today but over the years, for weak standards, for ineffective enforcement and for inadequate remedies, but at the same time I think it's probably a permanent aspect of the U.S. regulatory framework, and there's a couple reasons for that.

One is that U.S. Internet policy has always been very friendly to ECommerce which tends to view regulation as costly, as inefficient or as harming innovation, and I don't think that perspective has really changed.

The second is that, and I think we saw this

today too, when there's uncertainty over what the best policy is or what the impact of regulation might be, for example, in the online behavioral advertising area, self-regulation seems very attractive because it allows experimentation and it doesn't freeze laws once and for all.

But that said, I think it's important to see that, and this is my second point, that self-regulation is not monolithic. Where we're most familiar with largely voluntary efforts at self-regulation such as from the DMA, the OPA and more recently from the NAI, but I think it's better understood on a continuum based on the degree of government intervention, and there are other models available.

So one is that the government sets substantive standards but leaves enforcement to industry, and the model I have in mind for that is the EU U.S. safe harbor agreement, which defines very clearly what the privacy principles are but relies on self-regulatory mechanisms for enforcement purposes.

Another is the statutory safe harbors up the Children's Online Privacy Act, COPA, where the government defines clearly not only the substantive standards, but also how to handle oversight and enforcement.

I've done a case study of these three models and come to the conclusion that the statutory safe harbor really responds best to the typical criticisms of self-regulation but also does best against a variety of criteria, completeness of coverage of the substance privacy standards, overcoming free rider problems which you alluded to, how do we get outliers to join, oversight and enforcement and transparency as well.

So one recommendation I would have is that if Congress enacts a new privacy legislation, it should continue to encourage self-regulation via a statutory safe harbor, but in doing so it shouldn't just replicate the COPA experience because that had flaws too, and the main flaws were, first of all, that very few companies signed up.

They're under a hundred companies who have taken advantage of the COPA's statutory safe harbor, and I think this is largely because firms view the benefits as too limited, and that's partly due to the fact that the requirements are simply too inflexible, and to address that, I would suggest that the privacy community could learn a lot from the experience in the environmental field where they're been wrestling with similar regulatory issues for much much longer.

I'll just close these comments with two points I

want to emphasize. The first is the idea of privacy covenants, by which I mean a covenanting approach where government and industry sit down together and negotiate a regulatory agreement often under a threat of stronger harsher regulation if an agreement is not reached, and then typically with other stakeholders at the table, and Pam Dixon mentioned this earlier when she talked about the friction or tension that arises when you have multiple stakeholders.

And more meaningful compromises can emerge from that process, and this may sound a bit farfetched, for example, if FTC were to try to persuade NAI to include public advocacy groups at the table when they do a next round of codes of conducts for privacy principles, but there is a model for it in the recent global network initiative where under both threat of regulation and very severe, negative news coverage, Google, Microsoft, Yahoo sat down with academics, with privacy and human rights groups to talk about global principles for addressing privacy and anticensorship rules under the experience of cooperating with the Chinese government.

So it's not unprecedented by any means, and it's been tried quite a bit in the environmental area as well.

The final point I want to make is that it would

also be interesting to experiment with regulations that differentiate between good and bad actors, so we've heard a lot of concern about whether there will be a one size fits all approach if regulation is followed, but I think the way to avoid that is to build in criteria that treat different performers differently. That of course raises the question of how to measure that, but we'll put that aside for now, and to adjust the set of carrots and sticks that are used as incentives to motivate more firms to fall into the good performer category.

And one way to do that might be to consider a traditional use of safe harbors which is as an exemption of liability, so if legislation was to include a private right of action or liquidated damages, that might be -- firms that fall into this defined category of having either undertaken a covenanting proven and won approval from other advocates for their approach would be exempted from that liability, and it would be limited to firms that don't participate in that well defined safe harbor or other measures for good performance could be devised.

MS. RICH: Thanks. Now, Chuck, Ira just said that self-regulation works best. He recommends that it should be supported by regulation. Are you going to take that?

MR. CURRAN: I'll take that for $200. First off, to be clear, there's no unitary model of self-regulation for all online advertising, but I think it is important that if -- there's an idea in Ira's article that he talks about in the covenanting process of the advantages of the flexibility of having performance objectives. What we've seen in the context of OBA specifically is that I think the dialogues with advocates with the Commission through town halls like this that helps us in effect formulate a performance objective, for example transparency.

It's been called out repeatedly that there is insufficient information about the nature and substance of the categories used for OBA, so the industry responds in response to this objective, has been with some degree of differentiation based upon the company specific technologies to serve up, and you see it with Google's ad management platform.

You see it now with Yahoo's iteration on that same concept with even more bells and whistles, and you have see it even with smaller companies like BlueKai, so you have companies responding relative to their own technology, but trying to satisfy the performance objective of transparency.

Same thing for the persistence of opt-out

cookies. The critique was you're not providing a stable enough platform for the browser to remember these preferences, and so here too, some industry advances, some advocates, Chris Sagoian is here who has developed pro bono code, and we at NAI and industry are now in effect bringing to market the same concept with our own in effect flavors to recognize what we think is the best way to address consumer need.

Finally, Fran Hans notice which of course who is the big kahuna of issues that people want addressed in the context of OBA, and thereto, we have a complex ecosystem involving advertisers, publishers, ad networks. We obviously need the consistency of a common iconography, a common messaging for consumers to understand, but at the same time we need some flexibility to implement the backhand so that companies participating in a disclosure ecosystem can express that information in different ways, whether they would like to put it in an interstitial or on a web page to transit information.

So I think overall the ability through the self-regulatory process to address general principles rather than any particular technological mandate I think is really the core virtue of the system that we are trying to encourage.

MS. RICH: But in the absence of any regulatory scheme, what do you do about people not joining? A consumer thinks it goes to NAI, and the consumer opts out, and then there's all these people not -- who aren't members?

MR. CURRAN: So I think here there are two different problems. One is the sort of free rider problem, and the other is the edge rider problem.

If you move to a system, certainly the NAI has been in existence for some time, but in the past year, with the in effect active participation of thousands of companies through the DMA, the IAB, we have much more of a platform of common ownership of the responsibilities of self-regulation and enforcement.

And I think that speaks to the issue of the free rider problem, the ability to -- for companies to avoid the obligations and the work that they have to do to be part of the virtuous ecosystem.

The edge rider problem I think that becomes more front and center when you achieve that ecosystem wide, self-regulation, and there as is typical with other problems online that the FTC has addressed, it's not as if there aren't -- there are remedies that address aggressive practices, material omissions, deception, existing tort law.

There are often remedies, but it is also true, and I think that the DMA and the IAB certainly bring the experience to this that once you have a general ecosystem wide adoption of self-regulation, you do in fact have a system in place where the desire of the participating companies who are making the effort to name and shame and to identify, and in effect to create processes that relate to nonparticipating members and to call them out for their conduct and to investigate them and to refer them to you.

So that's I think where we get to the solution for the edge rider.

MS. RICH: I want to get to some of the new models that have been proposed, so I'll get to you, Barb, in a minute, but, Evan, do you have a very brief comment on this issue of self-regulation?

MR. HENDRICKS: Yeah. I think -- well, I think there's another model that's out there that hasn't -- we don't talk much here because it's the Dutch model. The Dutch model was -- Jessica, I think your questions go to the fact that if you don't have standards in place, what are the standards for whatever self-regulatory model is.

In the Dutch model, the European country, they had the fair information practices in law, and what they did to implement it is they told the different -- this

is several years ago, they told the different sectors of the economy to come up with their own industry wide set of practices on how they were going to comply, and they opened a process so it wasn't just them talking to each other. The public was involved and so then they had to submit that to in their case the privacy or Data Protection Commissioner and then ultimately it was hashed out and became a stamp of approval, but the principles were set and the standards in the industry working with anyone else who was interested including the advocacy groups worked out the code of practices and then it became an enforceable code of practice.

So I think that is something that has a lot of legs, and what we need when we need to have real standards. We need to have enforceability, and we also need to have flexibility given the environments we're talking about.

MS. RICH: That's a very good point. Barb, do you want to talk now about I know that is it -- is it the Business Forum For Consumer Privacy? The Business Forum has come up with a use based model that it's proposing, and it would be great if you could briefly describe that so we get a chance to talk about it.

MS. LAWLER: Sure. What I actually wanted to comment on before I get into the use and obligation

centered model is I wanted to build on something that Ira mentioned a moment ago and make sure that we're accurately capturing the self-regulatory environment, and so one of the areas we haven't talked much about are privacy seal programs where we think about fair information practices, the traditional fair information practices, and programs like TRUSTe programs, BBB online when that existed.

Those self-regulatory programs in many ways did a better job of applying and do a better job of applying fair information practices than perhaps some actual regulations do today, and I wanted to capture that before moving into the use and obligations model.

The purpose of the use and obligations model is really the culmination of a lot of thinking and effort over a number of businesses of organizations over the last three or four years to really look at how do fair information principles, fair information practices work in the 21st Century in the digital economy, so what the model really does is it focuses on the idea that use rather than collection driven by notice and choice, that use is the driver for the other fair information practices, so let me talk about what that means.

As we think about traditional privacy models today, we spend a lot of time talking about that. We've

talked a lot about the failure, the limitations of notice and choice, and the excessive focus on notice and choice. In a notice and choice collection based model, you have to know where that information began, where it started to understand what obligations might go with it.

In a use centered approach, it is different because it says through the life cycle of the information from the point it is collected through different organizations that have some responsibility and accountability to handle that. Obligations carry throughout that, and that's driven by use.

The use and obligations model, if you read through the paper, and we have some nice graphics that actually talk about different types of major use categories focused on fulfillment, on internal operations around risk management. We talked about risk management actually in the data broker context, fraud prevention, and also security and legal obligations, and also what we do in the model is actually outline how notice, choice, access and correction as well as enforcement and oversight concepts fit in, but are driven based on the different categories of use so let me stop there.

MS. RICH: If you focus on use, and of course

the collection use debate has been in play for a long time, but what do you do about -- we talked earlier, two of our examples I think in the first panel were the AOL breach and the Google subpoena. How does use affect data sitting there and then ultimately landing in the wrong hands?

MS. LAWLER: One of the benefits for organizations in applying a use and obligations model is what it actually does is, if handled right, forces the organization to sit down and talk about, think about what information they are collecting, how they are using it and to frankly have a data strategy and information management plan.

So that ideally a situation like AOL and the release of research information, there might have been a different set of criteria, a different set of framework that might have driven that.

When we look at enforcement, a couple things that we think are important in the use and obligations model is the current environment we have on fair information practices really places a lot of burden on the consumer to police the market.

And we think that organizations, responsible organizations have an accountability and responsibility to be more responsible and to actually relieve consumers

of the burden while at the same time providing transparency so that individuals can have more informed decisions, more nuance decisions, but that organizations frankly are being more sophisticated, more thoughtful, more comprehensive in their approach because consumers should expect a safe marketplace, they shouldn't be the ones to police the marketplace.

MS. RICH: One of the things that is intriguing about the use based approach is that it does attempt to identify categories of uses that perhaps should be subject to lesser restrictions and are consistent with consumer expectations such as fulfillment, security, give different names for it, but maintenance of the website, et cetera.

We talked in an earlier panel about simplifying things. We talked in every panel about simplifying things for consumers, and we'll keep talking about that, this is for everyone because I think this goes to potentially new different models that we might think of.

Is it possible to identify -- to get things off the table for consumers by identifying uses that we think are entirely consistent with consumer expectations and don't need to be in a privacy policy and don't need to be susceptible to choice, by the same token uses that -- could we agree on uses that are so harmful that

everyone agrees they should be prohibited, and thereby boil down to a much smaller category -- Fred was talking about this, a much smaller category of uses or collections, things that consumers have choice about so that it's manageable? Could we work with something like that? Marc?

MR. ROTENBERG: Well, I'll answer the question but I want to first say that I absolutely agree with what Barb just said, that consumers should not be expected to police the marketplace. I think that's one of the best criticisms of self-regulation, that there has to be some independent entity, maybe like the Federal Trade Commission, that would have the responsibility of policing the marketplace.

Now, with respect to the use approach, yes, that's one of the elements. In fact if you read a privacy law, it will typically have an exception to a limitation disclosure that says that a disclosure that's necessary or incident to the provision of the service is fine. I mean, if you're going to -- if I want you to ship something to me, you're going to ask me for my shipping address, and you're going to disclose it to the shipper so I can get from you what I wanted.

MS. RICH: So long as the shipper doesn't use it for any other purpose.

MR. ROTENBERG: Yes, but in fact a lot of these privacy norms reflect common sense understandings about how people interact with businesses. I think a lot of Joe's work is fascinating because what it tends to reveal is that in fact most people have pretty high expectations of privacy, and most people assume that those expectations are respected.

The actual story, of course, is very different, but also to make this very important point, Michael's chart which lists all these different international privacy frameworks, still settle around 8 to 10 main fair information practices. They actually don't vary that much, which is a remarkable fact about the modern information economy, and that is that if you look at how different countries that are participating in this information economy have understood privacy protection, whether on a country basis or a regional basis, they've come to surprising similar conclusions, which I think is a very important insight for the FTC.

The last brief comment I want to make is to the extent that governments are not engaging in some of the most pressing privacy issues that we have today, I actually think civil society at the recent meeting of the privacy commissioners in Spain issued a very important document.

This is called the Madrid privacy declaration, which really identifies the current challenges to privacy protection where some of the gaps are and what governments need to do, so I think if you take Michael's chart with those 8 to 10 fair information practices that are fairly well known, and you put next to it civil societies's critique of what else needs to be done you will cover a surprising amount, so use is part of it but I think if you stop there, we're back to having kind of a notice and choice approach to privacy protection.

MS. RICH: It seems clear that there's certain consumer benefits like access and transparency, an event -- that's just the wrong term, that do require interface with the consumer, and so apart from the things we can agree on, I mean I think there's a lot of discussion about not collecting data you don't need and some of these other principles, let's say those are all enacted.

In terms of the interface with consumers, what can we do to simplify that? And so I'm wondering if you take some of the categories and uses based model and I would not -- I think marketing is controversial so they put that in the use based model, but Barb, the other ones are fulfillment, fraud prevention, subpoenas.

MS. LAWLER: Security and legal requirements.

MS. RICH: Security, if you took those, which I think are less controversial than the marketing and then what else is there? What are the uses that --

MR. ROTENBERG: Jessica, that is not necessarily the right approach and what I'm trying to suggest and an engineer I thought had a really good insight in talking about privacy. He said you actually want less on the dashboard and more on under the hood, and what he was saying is that you don't want to confuse consumers with a lot of complicated privacy choices and decisions.

You want them to engage in whatever transaction the merchant is holding out, which is good for the consumer and the merchant, right, with a privacy safeguards built in, and you see the problem with this approach --

MS. RICH: I think, Marc, I'm with you. I'm saying that assuming you have some substantive protections, there's still going to be certain things perhaps that you can't agree on. Maybe we can agree on things that are okay, maybe we can agree on things that aren't okay, but there may be that middle ground, for example, marketing, where there's still -- there might be consumer choices, and the question is can we narrow -- can we narrow the areas where there will be consumer choices by perhaps having substantive rules

about everything else and thereby not put so much burden on the consumer? Evan?

MR. HENDRICKS: Well, I think Barb had mentioned fulfillment. What was the other ones?

MS. LAWLER: Marketing.

MR. HENDRICKS: Marketing? Pam Dixon talked about earlier fraud prevention. It's a dangerous loophole, but yeah, but things like fulfillment, and even Marc mentioned that in his comments. It's basically the data is being used to complete a transaction that's very consistent, and I think on the other side we've talked about sensitive information that has been identified in different realms as things like your religion, your political affiliation, your health condition, financial condition, minority group, your ethnicity, sexual preference.

Those are some of the categories that you look at taking off the table which are not these days, but on the other hand I think the answer is no, in the sense that ultimately for a national policy, I agree that the Supreme Court said that in 1988 and the reporters committee case, which is Freedom of Information Act case that the meaning of privacy begins with the ability of the individual to maintain reasonable control over their personal information, and in terms of the proper policy,

there is no substitute for a reasonableness standard.

You have to have -- if you go to a website because you want to see about a sports score and then you get floated an ad about sports, is that such an unreasonable -- I don't think it is? I don't think it's that big a deal, but if your elderly parent has a condition or you have a friend that has AIDS or someone and you have go to an AIDS website, but you're identified as someone who has aids and that's sold to an insurance company, I think most of us agree that's unreasonable.

So for the larger picture, the answer is, no, there has to be a reasonableness standard. There has to be that kind of flexibility in there, and I think that ultimately I spoke to earlier there has to be a mechanism, the individual can initiate enforcement of his own rights.

MS. RICH: So we have talked about a bunch of different types of models that we could consider, assuming we're developing a new model. Obviously we've talked about the notice and choice model. We've talked about harm based. We've talked about the use based model. We've talked about the Dutch model which is based on self-regulation.

We've obviously talked about more comprehensive

FIPPs of the sort that it had been enacted in many places in the world, and we talked about -- Fred and I at least have talked about perhaps taking certain things off the table with substantive rules but perhaps leaving choice for other things.

Any other models that we should just throw out there for exploration?

MR. ROTENBERG: Yes. The idea that you can have anonymous online transactions, right, which is actually a very powerful concept, but the reality for most consumers, and I used to track these numbers, they're issued by the Department of Treasury, up to about four or five years ago the majority of transactions that consumers engaged in in the United States were cash based.

If you got into a cab to come to this meeting, if you went across the street to buy lunch, if you went to get a newspaper, all of those transactions allowed you to purchase a product, someone to get paid and there was no disclosure of personal information. That was the majority default for most transactions.

I think it's worth spending at least a little bit of time thinking about how we could recapture anonymous techniques, and in some areas our society it turns out to be vital. For example, voting online and

maintaining a secret ballot. You have to solve the problem of protecting privacy to make the secret ballot work.

So I think for the FTC to spend some time as a lot of other privacy agencies have around the world on how to make provable anonymous transactions work would be a very good model to pursue.

MS. RICH: Is that a regulatory model or is it a technology driven model?

MR. ROTENBERG: It's both actually. It's an excellent question. My view is that you get better privacy technologies from a background of privacy regulation. In other words, if you make it difficult for companies to collect and use personal data, they will come up with innovative solutions that are less dependent on the collection of personal data, and if you say, we're really enthusiastic about companies that can make anonymous transactions work, I think the market will respond.

But it will take some leadership, and the thing that will surprise people in this room is that a lot of privacy advocates actually are very strong supporters of technological innovation. We just want to see innovation that promotes privacy, right? Commerce is great, let's also do it in a way that promotes privacy.

MS. RICH: I guess we shouldn't forget other privacy enhancing technologies that could either be done in a self-regulatory way or through -- by incentives through regulation.

Does everyone want to take 30 seconds -- whoever has their card up now 30 seconds quickly so we can end semi on time? Howard put it down. Howard?

MR. BEALES: You were going down the table.

MS. RICH: Everyone quick.

MR. BEALES: I just wanted to say the taking some uses off the table, so some uses you don't really have to have notice or choice about or consent about, that makes perfect sense. To me the way to think about it though is not expectations.

I mean, I think consumers want most of the products they use. They want them to work. They don't have expectations of about what goes on under the hood, if you will, and they shouldn't have to have expectations about what goes on under the hood. We ought to protect them from bad consequences, but that really ought to be the focus.

MR. CATE: Jessica, just on the model point, I don't think you implied anything different from it, but it seems that we should be clear. These models don't have to be mutually exclusive, and so while I think

notice and choice is somewhat exclusive of others of these models.

It's really sort of overlaying then in a way that makes the most efficient, effective appropriate protection. The other comment is you used the word simplify, and you scared me to death when you Emailed out that question, that you were going to ask about simplification because first of all I think it's absolutely right.

It should be a goal to simplify the role of the consumer, the role of the individual in privacy protection. Privacy is remarkably complicated because information is so complicated, and therefore I think at least we need some sense that there's going to be a lot of different approaches in different sectors, different times. We've talked about the difference between public and private sectors, distinguishing between good actors and bad actors.

I think we're overall unlikely to simplify the area. Simplifying the role of the consumer I think makes great sense.

MS. RICH: We will have to leave simplification for the next roundtable. I didn't get there. Evan?

MR. HENDRICKS: I want to take 30 seconds please tell me when there are ten seconds left. I'm talking

about a dynamic that always happened when the FTC has considered this. In the 1990s, they were afraid, they were too deferential to the Internet business and therefore they didn't go with a strong privacy machine -- if you look at who came to your workshops, then a lot of them don't exist anymore, and they got their way but had nothing to do with privacy.

MS. RICH: You came.

MR. HENDRICKS: Yes, that's right. Something with IRSG principles. There was a lot of deference to that sector of the economy. They went with the self-regulatory thing. Most of those people aren't there any more either, and it's happened over and over so I think this time I think history shows that you shouldn't be -- we heard a lot of testimony earlier about how concerned the ad industry was that their ad rates are going down. Yes, it's a sector that's in huge transformation right now as is the industries that depend on it but I don't think we should be bending over backwards or going the other way with our privacy policy and sacrificing protection for personal information based on these transformations going on in the industry.

MS. RICH: Barb?

MS. LAWLER: So to finalize the discussion around the use and obligations model, I want to

encourage folks to actually download the paper, grab a copy, read it. The question was have we captured all the uses, and we think we've captured all or virtually all of them, but we actually encourage and welcome feedback. There's more work to do on the model, and I wanted to make sure and leave folks with the idea that this a use and obligations centered model built around all the fair information practices. It's not the use only model.

MS. RICH: Ira, remarks, last word, quickly.

MR. RUBINSTEIN: I just wanted to echo Fred's point that the models are not mutually exclusive and also point out that with the statutory safe harbor approach, you are forced to define what the FIPPs are, but then as in the Dutch model, the approved codes of conduct is where you experiment, so the use and obligations model might be such an experiment subject to FTC approval.

MS. RICH: Interesting. This has been a great panel thanks very much.

(Applause.)

MS. RICH: We haves some closing remarks by David Vladeck, our Bureau Director.

MR. VLADECK: Thank you, and I will get you out on time. You will all be out of here by six because

we're now down to the hard core. This has been a remarkable exhilarating and in some respects exhausting day. It's the beginning of what we hope is an important dialogue on consumer privacy, and we thank you all for coming.

I want to begin, however, by thanking the FTC staff that made today possible. This is truly an all star team. You've seen many of my colleagues up at the podium today. An enormous amount of work went into organizing this conference. Please join me in thanking them for such hard work.

(Applause.)

MR. VLADECK: I also want to thank all of today's participants. We had very high expectations for this conference, but the dialogue today exceeded even our loftiest goals. I think all of us learned a great deal today. I certainly did. Who knew privacy had its own vocabulary. We've learned about issues like boxing, scripts, ecosystems, edge riders and daisy chains, all very interesting concepts.

But last, but certainly not least, I want to thank each of you for coming today. We have very hard questions to answer here. The last panel I think, as the predecessors, exemplified just how difficult the questions we have to confront are. We will need your

help in finding the right answers. We urge you all to help us as we move this process along. We look forward to your comments. We look forward to your thoughts.

So let me just make some overarching conclusions about what we gained today and what questions face us in the future. We began the day by discussing a wide variety of ways in which these important but powerful tracking tools bring benefits to consumers, but we also discussed the risk of possible misuse of information.

Panelists pointed out that the benefits include free content, better search results and more relevant advertising. These were all consumer benefits, but the panelists also mentioned real risks including the disclosure of information consumers believe is private, and the chilling affect on people who might modify their own online behavioral for fear of being tracked. These are real risks as well. We need to confront them.

We also heard that the traditional distinction that has been drawn in privacy law between personally identifiable information and anonymous information may be a thing of the past. These observations raise questions about how to build in transparency, consumer control and accountability into the process without sacrificing the benefits.

Our task is made even more urgent by the researchers who talked today that confirmed our intuition that consumers do not really understand the data collection process. One panelist pointed to some misperceptions about the phrase privacy policy. According to this panelist, many consumers believe that if a company has a privacy policy, it means the company does not share data with third parties. We know better but consumers do not.

There was also a general agreement that consumer disclosure as we know it simply does not work.

But as today's panelists pointed out, and I think a lot of the discussion we just heard confirms this, just because it's broken doesn't mean that we should scrap it or discharge it. Transparency is challenging but we need to think more creatively and innovatively about how to deliver important information for consumers when they need it and in clear and in simple terms.

We heard about new efforts to make effective and meaningful disclosures. On the positive side, we heard that companies like Google and Yahoo are creating pages that consumers can click to see what data these companies have about them. That is to the good, but there is work to do as consumers are not clicking

through to this data in large numbers.

The economists also pointed out the limits of disclosure. They noted that consumers engaged in boarded rationality where they tend to discount long-term negative effects of giving up their privacy. I also have questions about timing. Is notice and at the time of collection adequate or should we think about notice at the time of use? These are questions that we have to confront.

Online behavioral advertising remains a highly visible issue. Since the FTC released its report in February, the industry has responded with a number of initiatives including efforts to improve consumer notice about these ads and to provide more effective choice to consumers. We welcome these efforts.

There are, however, concerns, particularly about how some of the industry frustrate consumer choice by using technologies other than cookies to gather information online and by collecting and using sensitive data for behavioral advertising.

There was a lot of discussion about what is sensitive. As with beauty, we learned that beyond certain categories, sensitivity may be in the eye of the beholder. Indeed one speaker mentioned the example of Rogaine. Now, I might not care, if others know that I

use it, but I would add parenthetically that if I do, it apparently doesn't work, but someone else might care.

The data broker industry is largely unknown and invisible to consumers. Yet there's a lot of diversity in the types of information, uses of information and even the rules that apply to how such information and in some cases highly sensitive information is. Managed this is an issue that may warrant our attention.

Finally we heard discussions about various approaches to managing the privacy and security of consumer information, the self-regulatory approach as has occurred in the advertising space, fair information principles including notice, choice, access security and enforcement, and the experience of other national regimes and the importance of harmonizing standards so as to not impede international commerce. These are all questions that we will be confronting.

In short we had a robust debate with interesting arguments, on all sides, just the kinds of debate we hoped for. We welcome, we invite this kind of dialogue, and those planned for our second roundtable to be held on January 28 in Berkeley, California.

Again I want to thank everyone who contributed to the success of this important conversation and we

look forward to seeing you next month, next year in Berkeley. Thank you very much for your patience.

(Applause.)

(Whereupon, at 5:55 p.m. the roundtable was concluded.)

CERTIFICATE OF REPORTER

DOCKET/FILE NUMBER: P095416
CASE TITLE: EXPLORING PRIVACY ROUNDTABLE
HEARING DATE: DECEMBER 7, 2009

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the steno notes transcribed by me on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: DECEMBER 23, 2009

_____

DEBRA L. MAHEUX

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

_____

DIANE QUADE