>>RICK QUARESIMA
If everyone could take their seats. We want to start on time. We'd like to welcome everyone to the final panel session nine on the future of behavioral advertising format. We'll begin with three brief presentations then we'll move to a moderated discussion. I'd like to first introduce everybody who is on the panel. Starting from my far right we have Katherine Albrecht from CASPIAN, to her left we have we have Mozelle Thompson from Thompson Strategic Consulting. We have Jules Polonetsky from America Online, to my right Alissa Cooper for the Center of Democracy and Technology. I'm Jamie Hine, I'm an attorney here at the FTC. To my left is -- to his left we have Robert (indiscernible), Scott Shipman from eBay, to his left John Thorne from Verizon. Joseph DeMarco from DeVore and DeMarco. To Joseph's left, Brad Schuelke from the office of Texas Attorney General and last but not least on the far left we have Tim Lordan from the Internet Education Foundation. I'm going to turn it now to Katherine Albrecht.
>>KATHERINE ALBRECHT
I'm going to kick this off with a bank. I have very limited time so I'm going to go quickly through these slides. What we're doing here in talking about online marketing and tracking consumers online, I think is going to be setting a precedent for what's going to be coming down the road in the future involving people and real world cookies. Probably the best there's a couple of examples of how people try to do this in the -- IBM can track people by their shoes so they can track them around the store and the idea was that they would actually step on a hidden unit in the floor that would be an applicator that sprayed electromagnetic ink on their shoe and put a little puff of air and dry it quickly so it would be unobtrusive, the consumer wouldn't notice it and they would have little devices around the store in the floor that would actually see where they browsed, how long they stood, what they looked at so that they could be tracked. Of course the ink would be invisible and consumers wouldn't know about it. Well they're not going to have to go to all that bother if things continue along this present path because with RFID tags now being planned to replace the bar code to be sandwiched into shoes and clothing you can do the same with less mess and bother. An RFID tag most people in the room are familiar with it, the idea is to at some point place one of these on to every consumer product manufactured on planet earth so there would literally be one in every pair of shoes, every belt, light bulb, every pen would be equipped with remotely readable miniature tracking devices containing information very similar to what is in a cookie file. Already they're appearing in passports, new passports issued by the State department contain an RFID tag. Over 20 million contactless credit cards issued in the United States contain this technology. And of course loyalty cards already sort of span that consumer marketing tool. It's a consumer marketing tool many people carry in their wallets. It's the topic of my dissertation at Harvard University. I discovered by the way, I'll throw this out with some or topics discussed, 75% of American consumers do not recognize their loyalty card is used to collect their personal information or to make a record of what they buy. And I would be happy to provide that data to anyone who would like to follow up

on that. One of the plans by NCR the national cash register corporation which is the technology partner for Wal-Mart is actually to use RFID on consumers in order to track them around the store and charge them different prices for different items depending on individual characteristics of those consumers. As gleaned from these tags. The idea is that if you have one of these in your wallet or purse or your backpack or your pocket because radio waves travel right through fabric, leather and plastic they would be able to read these tags on your person without your knowledge and presumably without your permission so that as you walk through doorway portals and here you see one we're used to seeing for anti-theft purposes, those can be upgraded to become RFID readers an read these tags. They are also now creating ones that can go horizontally so they can scan you in a nice wide open space, you would never know it was there. I'm going to skip this one. IBM probably does the best job in one of their patents in describing how this would be used to track consumers. And they've patented something they call the person tracking unit. What this person tracking unit is, an RFID reader that picks out these signals from people's belongings and place them in walls, floor, ceiling tile, shelving, doorway, literally anywhere and they discuss a desire to place these into public spaces like museums, theaters, libraries, elevators and public restrooms. So literally everywhere you go you can be scanned. The best way to understand how this works they spell out in their patent is because the HRFID tag has a unique ID number it's like a unique cookie number. And it can be linked to your identity so for example if you sell me a pair of shoes, that has unique ID number 308427 in a cookie embed into the soul, then any time in the future you see unique ID 308247 because that's the only object on that's right will transmit that number presumably then you can look that up in your database and you can sigh that number corresponds to a pair of size 8 Nike running shoes that Katherine Albrecht bought here last month. There's a good chance she was standing in it. So you can use it to track people. You can also use it as IBM describes here to look inside of people's purses. Their example was to look inside of a woman's sealed purse because all of the objects in her purse would carry one of these remotely readable tags on it you could do an inventory of everything she was wearing and care rig. Example if he's carrying a baby bottle you presume she's a new mother and target her for products. Japan has been testing this now with a slight twist. This is actually more like the video that we saw in one of the earlier presentations. Where the guy had the Post-It notes stuck all over him. What Japan has done fund bid the Japanese government in conjunction with NTT Do Como is they issued shoppers in the shopping district in Tokyo RFID reader cell phones and placed the cookie, the little cookies in the doorways of stores, as people walked into the stores their cell phones unbeknownst to them would grab information from the cookie and keep a record of everywhere they had been. Then when they walked into other stores all that information could be downloaded so a complete record of their travels, interests, what they browsed and where they had been would be available to other stores that were part of the system. Bank of America has a similar plan, this is also a patent. And this particular device you walk up to a billboard and it would identify collect gather and use personal information about

you. Again, using these real world cookies in your belongings. There are plans to scan the tags in people's garbage developed by BellSouth. This is idea when you throw these things away because the industry says we'll just put them on the packaging don't worry. When you throw them away they came one a plan to scan your garbage at the dump and figure how long it had taken you to use that bottle of shampoo or whether you traveled with the dog food. Those are examples they provide. I okay making that information of course available to retailer, manufacturers, distributors and the like for marketing purposes. This was one of my favorites. Phillips electronics looks forward to the day when in consumer's homes they will have appliances hooked up to the Internet so they can use the RFID reader capability so their idea here on a saw is that you could put some blueprints on there, download information, they say wouldn't it be great because you could be able to capture hidden information about other things people do in their homes. So someone eating cereal as a snack. They literally say on that table saw, you can capture, download it and make it available to marketers who can direct market to this person who likes to eat cereal as a snack. It is my belief this is extraordinarily harmful to consumers the segmentation model that says we want to know what people are doing all the time so we can scrape them off the hull of the ship. This is from the Harvard business review referring it to not profitable customers as problematic and like barnacles in the hull of the cargo ship that create additional drag. These are people not pulling their weight by being profitable enough to the companies. Then finally it appears to me that the marketing industry rather than posting these practices has condoned them referring to them as a practice called digital red lining, meaning marginal services and high prices designed to drive the unattractive customer somewhere else. So if we allow this to happen in the online world if we do not take steps at this point to at least say these practices are objectionable and to lock more closely at them, then down the road we could actually be creating an infrastructure in which everything we do would be tracked all the time. If you have any further questions on this we have two websites, spy chips.com about product tagging and we have a new website up at anti-chips.com which deals with the actual injection of these devices into human beings in the form of RFID implants. We'll talk more when we get to the Q&A section. Thank you. By chips.com and anti-chips.com. Thank you.

>>RICK QUARESIMA

We'll have time for questions afterwards. The second presentation from Zulfikar Ramzan from Symantec.

>>ZULFIKAR RAMZAN, SR.

Thank you for making it this long in the game. I was worried about giving a presentation at 3:30 on Friday. I'm only going to spend five minutes or so describing technologies. There's two particular ones I wanted to mention which I thought were relevant to this particular discussion. One is something called browser defender and another is called identity safe. I'll explain them shortly. Let me identity safe. Let me start with browser defender. The web browser is now the conduit for most people's online computing experience. They don't talk about using the operating system or windows, just what do I do on fire fox, I.E .,

so on. Attackers realize the same thing. They know if people are spending most time online using the web browser that is the most liable place for attackers to try to target individuals. What's interesting is not sure if most people know but the most commonly targeted person on the Internet is the individual consumer. 95% of targeted attacks go after consumers they don't go after businesses or banks, that sort of thing. 's all about the end person which is something most people don't realize so oftentimes these attackers are trying to leverage flaws in your browser. They're either software products out there, they often have technical vulnerabilities. Those vulnerabilities can be exploited by another piece of software. And as I highlighted some software is available through tool kits. So in fact you don't need to have technical sophistication to compromise someone's website or someone's browser. All you need is the ability to buy a tool kit on line or through an underground market. The going rate for one of the most recent tool kits was about a thousand dollars for the tool kit. And that include ad one year support contract so if you had any problems you could contact customer support of the tool kit seller. I'm serious. It did include a one year support contact. The reality, it's taken a lot of difficulty out of the equation the whole market has become in some sense commoditized. Attackers are not just going after -- it's not like I can tell you don't go to unknown site. A lot of attackers are going after well known sites. A few examples. The most famous one in the last year or so was the dolphin stadium website being targeted just around the time of the Super Bowl. So they were compromised the attacker was able to insert a piece of coat on the website so if you visited the site and your browser was not patched your computer would effectively become compromised and your attacker could control that computer remotely and make it do whatever it wanted which is scary. You have to do nothing more but look at the site at the wrong time. The other thing attackers are doing, this ties into this particular panel is use of advertising networks to make some of this happen. The realities that advertising is not just about a text image or not just about sound, the reality is advertisers have gotten so complex and so rich in terms of content they are effectively pieces of software now running inside of an advertisement so that piece of software will be malicious and an attacker can get that software on to a website and this actually happened with my space. My space hosted an advertisement that happened to contain malicious code. This that code can take advantage of a browser vulnerability and exploit that machine and allow an attacker to take control of it. Turns out when my space had this happen to them, a million people actually saw the advertisement. Those people maybe some of them had their computer security software to update and browser to update but I think the odds are most people didn't. So it's a scary thought. With that said, the good news is that we have technologies in place to try to deal with those kinds of issues. We designed a new technology called web browser defender. It does proactive detection so it can detect any attempt by a piece of malicious software to take control over your machine through your browser and block that attempt. Because it's proactive and behavior based it cannot only detect the known threats but also the unknown threats out there. I thought that was an important type of detection mechanism especially since most people are using the browser

these days. It's included in the Norton antivirus line of products and in the Norton Internet security line of products coming out in 2008. Finally, I want to talk briefly about something called identity safe. The reality as I mentioned earlier this morning, most people have multiple online identities. I have an identity with my email provider, I have got identity associated with let's say a merchant banking with. I have gotten identity associated with associate networking partner. Each one of those identities contains a set of information about email address, pass words, so on. One of the challenges we're seeing is because people have so many identities it's hard to manage them. How many people here have multiple passwords they use online, multiple accounts? Most of us do. How many peep value more than five? I would say some have more than that. That's quite a few accounts you have to manage. We've realized that's something that is very difficult for consumers to do sew we are building in technology now that has the ability to manage these online identities. And that can include things like taking care of your pass words, being able to detect if you're about to enter your password into a fraudulent website automatically being able to switch between different identities for different sites so you don't need to manage the stuff any more. We're trying to use technology to simplify a lot of problems users are facing because the reality is most people when they transact online their interests are not in their own safety and security and privacy they're interested in doing what they want to do online like buy a product, so on. We want to take all the guess work out and make the decision easier for typical end users. So that's actually all I wanted to say. And thank you for your time. [Applause]

>>RICK QUARESIMA

Our final is from Mozelle Thompson from Thompson Strategic Consulting.

>>MOZELLE W. THOMPSON

First I want to thank the FTC for holding these two days of sessions. It's been an interesting opportunity to have a good conversation about where things are going in the world of advertising, especially in targeted advertising. I see commissioner harbor here, it's nice to know at least for me that I still have the ability to clear the room.

[Laughter]

>>MOZELLE W. THOMPSON

I thought a good place to start was a few observations, that it wasn't very long ago, in fact November 1999 when the FTC did a workshop in online profiling. Stemming from that workshop in July 2000, the majority of the commission including myself sent a report and recommendation to Congress on online profiling. Outlining some of the NAI principles. But also I took the step of saying that we should have some legislation in this area to establish the baseline of privacy protections. Let's fast forward. I'm not a big one to say I told you so. But I do think that this -- this was an area we had an opportunity. And we may -- the opportunity is different now. Let's talk a little bit about what's happened since then. And I'll tell you why. The online industry has changed quite a bit. We have more privacy policies and privacy tools. We have seen an array of free services that are available to the public. That we've seen interesting new ways that users are generating their own material and finding ways to distribute it among

themselves. The technological changes also means there's greater ability to transmit and gather information. And greater ability for a lot of people to search for that information. But there are also a greater array of tools to manage information. We also see the users have changed. You know, we have a generation of people out there right now who have always known the Internet. Who have never known what it was like not to be online. And they have a mixture of impressions. On one hand they may not be as sophisticated in understanding some of their risks but they are much more savvy in how they use information and in a strategic way to decide for themselves what value they expect to get from their participation. Now, we may have some differences about whether it's a long-term value or short term value. But it's clear to me that we have a lot more people out there who are making those decisions every day. So I thought it was interesting to also sit through the past couple of days, and I was struck by also a few things that remain as myths, that remain unspoken. But I will like to talk a little bit about them. The first is the idea that profiling or tracking users or consumers is new. It's not it happens offline, it happens online. We may have more tools available to do it but since there's been commerce and ever since there's been advertising people are trying to figure out a better way to reach their target market and figure out the better way the spend their money more efficiently to do so. That has not changed. How it manifests itself in an online world and the tools available to do that, that maybe different and evolves over time. Second, there's a lingering impression among some people that the public is dumb. And they're not. They are perfectly willing to exercise choices. Some of them maybe misinformed or uninformed but they make rational choices based on what they know and assess is their own value at the time they exercise their choices. Another myth is that the FTC's role is somehow to take legal action without clearly articulated harms. And I don't think that's true either. What that means is there may not be consensus on what those harms and risks are, but the FTC has the broad number of mandates including the ability to shine the spotlight on the issues that we hear of today. But in order to take enforcement action there has to be some clear articulation. And finally, and this is the thing that concerns me then and concerns me now, is that the primary risk to consumers are not posed by the people who are here in this room. They're people who are engaged in unscrupulous practices, who have technologies that are there to surreptitiously spy and take information from people and they don't feel like they have any obligation to comply with any of self-regulatory or regulatory code that are out there. So what that means for us, I think in the future is a couple of things. There's still a large gap between what consumers and users know and what they need to know. While there are various sites doing an admirable job to try to better inform consumers and also public interest groups trying to do the same and government, there's still a great opportunity in a coordinated fashion to provide more sophisticated information to users. Second, there's still an opportunity for government consumer groups and businesses to innovate in this area. -- innovate in this area. You guys are the experts in what's going on and what are the things people are interested in. And I think the opportunity is to spend one-tenth of 1% of your creative talent trying to figure out

what is the new tools that you can come up with that will make it better for everyone. And finally, this is a challenge that I see advising especially technology companies. How do you create a market that actually rewards to the top instead of bottom? How do you create a marketplace that rewards companies who give strong privacy tools, that gives choices, that tell consumers what they're doing with information? I see some companies out there that are doing that and I think what I am seeing is more and more consumers are flocking to those companies because they represent a real -- something that always is important in any marketplace, the trust between the consumer and the vendor. Thanks.
>>RICK QUARESIMA
Thank you. [Applause] Thank you again to all our present tears. And I want to start with some things that have been referenced earlier but we haven't had a chance to dig deep. Some of that right off the top is are there alternatives to cookies likely to emerge as identifiers of consumers Internet behavior. So I thought you could make that a general question but I think I would like to begin with you, Jules.
>>JULES POLONETSKY
Let me share other secrets about cookies because you heard how the opt outs are imperfect and you heard of challenges cookies face. So let me put on the business hat as well. The interesting thing ant cookies is they're not perfect. They're not perfect for ad delivery or targeting. In fact, there was some comment that only 5% of people managed to understand how to control cookies. The reality is if you sit in a room of advertisers and marketers they tell you hey where are the cookies going? 20, 30, 40% industry is constantly debating studies that wonder where are the cookies going. Some are removed by anti-spyware programs that automatically remove cookies. A lot are being removed by people who have figured out how to use the browser controls. Lots are blocked by P 3P. The disadvantage of cookies is in some way a real advantage. Years ago you had to send lawyers go to courthouses to get data give us privacy. Good limitations of cookies today that there are all these tools built around them and they're not -- they're good enough. People have built business models, all the big companies in this room have business models and the vast majority of ad delivery and content analytics is built around this shaky, good enough because it works but it's quite imperfect. So I think it's a remarkable thing that 7 years later from the conversations that we had years ago you still see people using cookies. One of the reasons why I think some of the privacy compliance people like me and many of the company look at these flash cookies and other novel tracking uses and say wait a second, the cookie has some controls, it isn't perfect. But until you come up with some really good way to make an effective way for users to control that, that's not something that's fair to use in an extraordinarily robust way. So I think that looking into the future, you're going to see technologies -- cookies are very similar to cookies that actually have user controls. People are looking at mobile today obviously, and there are not yet ubiquitous mobile cookies. One problem that's being thought about is okay, probably mobile is an example people really will want my address remembered or the things that I don't

want to have to punch in so I can instantly get my directions or whatever the case is. What are the ways that you're really going to put somebody in control so as not to have them running in a different direction? So my prediction is that both the -- we really should spend a good deal of time focusing on how to ensure that the cookie handling model which is going to be with us for quite a while, the business models are built around it and a huge amount of preferences and control and browsers are built around it. So we really should engage more with getting the cookie structure right.
>>JAMIE HINE
Tim, our new mobile technologies using something else?
>>TIM LORDAN
I think since 2000 we did our first congressional briefing on location advertising back in 2000. It's remarkable to think ban then we were doing congressional briefing as a legislative issue on this issue seven years ago. I don't think we understood the issue but we knew being built into phones were different triangulation and GPS chips and ultimately after 9/11 we had the act that allowed every one of these devices to be located for E-911 purposes. And every year since then I swear I have been like this is the year this thing is really going to open up. And it just is this pregnant pause where this marketplace of all this -- this becoming a new cookie just doesn't happen. The marketplace is growing -- is glacial in its implementation. For consumers that might be a good thing. The other thing for the past week I have been carrying around a phone, it's one of the only like location services called Leupped (ph) and it -- sprint uses it, there's few, someone who -- or child protection but it's like a social networking type thing. It's pretty cool. I have a map on the phone, I can see where all my friends are. And it was really excited about it then after a few days I realized that not only did I and my friend live really boring lives, it didn't give me the granularity that I want that I thought would be interesting. Basically I go home, then to work, home, to work. Then the Federal Trade Commission. Really exciting stuff. So we have some 20 somethings in the office and they were going on a trip to Los Angeles and I said we have two of these phones can we take them to LA and we'll play around with it. I said yeah sure. Take it with you. We're go to a football game. Can I see her on the other side of the stadium? I'm like no, no, it's not that granular. What about a different part of the bar and I'm talking to a guy can I see where she is? No, it's in the that granular. And I think the thing is that these things aren't that granular first of all. When it comes to mobile phones. Secondly, I learned a lot here. And there's -- if you are going to track people, where they literally go in the physical space as you do on my space or on the Internet, you have to have some kind of delivery mechanism, right? You have to deliver the ad somehow. And how do you do that? Super market aisle versus the coupon feeders, you're walking down the aisle and they're shooting coupons at you and you're like -- or you get a text message. That's the hackneyed example, I'm walking by a Starbucks and they're going to send me a dollar off latte coupon. The professor from Amherst had a chart that said the things that the advertisements that consumers find most annoying, I think the top one was getting a text message, it's like getting a phone call at dinner. And how you present the advertisement, I

think there's a pretty compressed short window where you could do that and actually convert a sale. Somebody says data is good on line for three hours. If you walk by the Starbucks you have like ten seconds where they're on another block. How do you present the ad in a way that doesn't annoy them? So I think that's a combination of factors that's making this process really glacial. I see the most dynamic aspect of location, locating people and self-reporting. Online people are twittering, people are disclosing their information on their blogs, on their social networks sites. And that is the by far the fastest growing location technology there is. That's basically just pure social networking. What I would say is if you don't want peep to know your location on a social networking site, don't disclose it. One thing I find interesting in this new paradigm of social networking is people are like just vomiting their personal information online. Like digital data diarrhea. But even that is like diarrhea of the mouth, diarrhea of texting and the key board. People have to take responsibility for that. I think that's -- I'm going to stop there on digital diarrhea. [Laughter]

>>JAMIE HINE

I'm glad we didn't do this right after lunch. I'm going to come back to mobile in a bit but I would like to turn it to Alissa. And if you see other alternatives to cookies as far as tracking and monitoring Internet behavior

>>ALISSA COOPER

This came up yesterday, it's a model that we at CDC have taken a great interest in recent months. It involves ISPs. So a lot of what we have been talking about the last two days of this workshop is all about advertising on the web and how the big ad networks are -- they're big because they're on a lot of sites. So if an ad network can track you across the top thousand sites on the web, top 10,000 site, whatever it maybe, the more sites where they can gather information about you this theory is the better they can target advertisements to you, the more they can collect about you. If you think about your ISP, no one knows more or is in a position to know more about what you do online than your ISP. Because your ISP can see everything that you do. So if we're talking about competing with an ad network that has visibility on a thousand sites, your ISP has visibility on every site. And this is a model that we started hearing about recently where not that I know of it actually happening on any other major ISPs in the U.S. but an ISP partnering with an ad network company to serve the information that the ISPs gather to the ad network and the ad network can use that information to target ads just like they do on the web but now they can see everything that you do. So some of the companies that are doing that, there's one called NABU ad which thanks to jewels I learned about recently. Just got a second round of funding, $30 million venture funding for NABU ad. Ad ZILLA, $10 million in future funding. There's a UK company called form PHORM, which has a market cap of half a billion dollars. So seems though this ISP model where not just a few websites that you visit or your search history but everything that you do online could be involved in the creation of the profile about you and that's certainly goes beyond cookies, it goes beyond flash cookies, beyond any other Web-based technologies.

>>MALE SPEAKER

If anybody in the audience has questions, the mikes are open, please step up. I'm actually going to come back to the ISP-based technology shortly but I wanted to throw this out to anybody else on the panel who is aware of other technologies besides cookies that they believe is going to become prevalent in the near future.
>>MALE SPEAKER
I wonder if the question is cookie is really the cookie question. I'll explain why. If it's not a cookie it will be something else. Because there's still a demand that's ever increasing for what I call mass customization, that you have 10,000 users and each expect a different experience. And they expect you to deliver to them in a -- on a real time basis, and what that means is you're going to need to know something about each one of those people. So if it's not a cookie, technology changes every day but as long as there's a demand for customized services, especially in the online environment, that's always going to be a challenge.
>>MALE SPEAKER
I want to revisit the ISP model that Alissa had spoken about. This may -- this type of model, this probably raises both legal and business questions. So first I want to turn to the legal questions. I'll throw this for Joe DeMarco. Joe, do you Sony different legal framework for this at the ISP level?
>>JOSEPH V. DeMARCO
I headed the computer hacking unit in New York where I prosecuted wiretappers and computer hackers. And over the last few days I have been listening to and for the raising of the wiretapping and computer hacking issues as well as associated intellectual property rights issues. This really hits the nail on the head. That's because as complex and as difficult as the issues are of consent and notice when you're dealing with a consumer and another party like a website, and those issues are very difficult, the difficulty in terms of the legal analysis and the permissibility becomes yet even more complex when you're talking about the monitoring of content by a provider of pipe, whether that pipe is an Internet service provider or a telecommunications company. And when you start talking about things like deep packet inspection or any type of analysis of data flows, as that is traversing the network by the network provider. By an ISP or phone company you immediately raise the issue of the wiretap act. The wiretap act makes it a crime as well as a tort, a federal tort to listen in on people's conversations, whether those conversations are on the phone, or over the Internet. It applies to content and that raises a whole host of tricky questions. At one end of the spectrum you could say an IP address is not content so you're not looking at the contents of a communication, if you're just looking at people's IP addresses. At the other end, if you're a provider, an ISP looking at the content of someone's emails and you're not a party to that email, you probably are getting into some content issues. But I think it raises very important questions under the wiretap act. And ads -- my recommendation to everyone is as you think about the deployment of these new technologies which I believe are going to involve things like deep packet inspection which of course is just carnivore renamed. As you're talking about that and thinking about that, from the point of view of a provider you really need to think about are you similarly I heard the last panel mention of the ability of various companies to turn on cookies that had previously

has been disabled, that raises issues under the computer hacking statutes. So I'm not saying this technology is bad, I'm in the saying it's good, I think as you do the analysis about whether or not different legal regimes apply you have to consider whether you're monitoring content, how you're monitoring it, who is consenting, and interestingly in the wiretap cases you have a very robust and well-developed you need to get the legal analysis right. If you get it wrong you not only had a business disaster, you've not only committed a federal tort and are liable for damages, but you could wind up in jail. And I think that is going to be part of future analysis of behavioral advertising. (off mic)
>>MALE SPEAKER
Let's talk about rich media. Can someone talk about the role of data collection via current practices and future practices and the rich media, multi-media units that are now deployed and will further evolve? And also the role of virtual agents in terms of data collection. Thank you.
>>JAMIE HINE
Anybody want to take a crack at that? No? Don't all jump up at once. Okay. Then I'm going to actually circle back and just let me talk about some maybe the business ramifications. If assuming the legalities are there, what are the business ramifications of the ISP model catches on and maybe I'll turn it over to Rob first since it's directly in if competition with yours.
>>MALE SPEAKER
The Microsoft ISP model is new to me and I'm learning on a daily basis the new Microsoft model. But I will like to go back to one thing about the new technology and the law is Jules is correct. On line marketing is the key technology. I don't see that changing any time in the near future. That doesn't preclude other technologies or things happening in the future. So every business model may have different technology as we look into video-on-demand or mobile marketing or other types of technologies as we evolve in the space may require different technology besides the cookie. So one thing we need the make sure as we go into this that we understand what are the consumer expectations? And the part of this I think that's been left out is advertisers. What are the advertisers' expectations and where to they play a role in this? They play ad big role in this. As I've seen over the last two years I have been at companies are doing the right thing. They want to make sure they're handling data appropriately. And they're not only do we see it as a business value add to advertisers we do things right with privacy but these companies are coming to the companies that are doing things right like the other members of the NAI. And so as we go and expand into these new realms and future technologies, we need to make sure that we have things baked into the technology similar to understanding how privacy play as role around notice and choice, we have the same principles here and we want to make sure as we develop new technologies and go in new areas for advertisers, that we understand and provide the notice and choice to folks. And that we're transparent.
>>MALE SPEAKER
The big thing that's changed when it comes to ad technology, most of these issues in the data collection again have not substantially changed. But you down

do easily years ago was the smoothness of the implementation. An example, banner ads years ago were indeed a banner ad. We acquired a mobile company some -- maybe a year ago called Third Screen Media and I remember having conversations years ago when I was at DoubleClick about well, how could our mobile ad server make sure nobody accidentally sends us personal data and have like a screen that would catch stuff if someone sent it and going through the issues and here we are years later. I said expecting all kinds of interesting entry kit new challenges. Turns out their greatest advantage and the reason they're considered sot of a leader there's lots of phones and browsers and all kind of formats an it is a bear to actually get a couple of different creatives for one advertiser on to lots of different phones in different structures. That's new and the leaders are figuring that out on the mobile side that's what has actually happened on the ad side. Whether it's rich media, whether it's the ability to deliver video, the ability to create ads on the fly, the implementation and the ability to actually get the ad where upped it, perhaps years ago an ad server could deliver one of 200 ads that it has for the right advertiser. But if you were an advertiser, and you were going to deliver an ad with an ad server, you didn't have 200 ads for 200 potential types of customers. And if you somehow spent a lot of money with creative shops and you created 200 ads and had them sitting there, the ability to sort and get the right one wasn't possible. Today sophisticated advertisers indeed can more of together and create the ad so the technology has smoothed out so a lot of what was envisioned years ago is finally happening in a smooth way. There used to be a career called dark trafficker. People went to a special training course to learn to get their ads and use the interface to get their ads if you were an advertiser on a publisher site. That query is gone because most of us in the room could sit down and puzzle out and probably accomplish running and indeed there's millions of people who run ads on Google and ad.com by using some of the tools out there that's really what's happened with the richness of media.

>>MALE SPEAKER

Could I add a point? I don't know if this was where you're going. It used to be across the top of your screen. If what you're talking about is ad delivery in a form which substantially modifies or alter it is website being reviewed, for example, a blogger website which inserts ads into the blog spool which may or may not be clear to the extent that they're ads or not, I think you have a copyright issue. And I know copyright issue is not on the radar screen of most lawyers concerned about things like the wiretap act and computer law, but bloggers have content rights in copyright and in their blog and one of those rights applies to corporations as well, the right to control and the right to create derivative works so if you're talking pant advertising which is substantially modifying and possibly creating a derivative work of the site being viewed whether it's the site -- website of a big company or the website of a blogger, I think you have to do a copyright analysis too.

>>MALE SPEAKER

I fear something no we are as sophisticated but I have a little blog I barely use and I was able to put a piece of coat on it by grabbing it following some basic

instructions and putting it at the top and all of a sudden sophisticated video ads from the American Express and all kinds of interesting stuff is running on my website and I don't know how it's happening. I didn't do anything special. And all of a sudden click, click, and I'm suddenly hosting some of these creative ads that seem to be delivered in an instant.
>>JAMIE HINE
Let's take this legal issue somewhere else. [Laughter]
>>JAMIE HINE
Very related. Unfortunately Declan McCullagh was supposed to be on the panel but could not. Recently CNET addressed the issue of ad blockers and certainly as we're moving into an area where we can deliver multiple verses of rich media and hopefully consumers get the right version that the advertisers want to deliver consumers still have tools at their disposal to help mediate the experience. We talked about those. Five years ago, today you don't buy an antivirus program. You have and all in one solution. Declan's article talked about fire fox and the issue of ad blocking. And surmised that some people in industry are very concerned about these tools, that in essence if consumers are blocking the advertisements that maybe there are some legal challenges that should be made to look into the legality of some of these tools. I'm wondering, maybe Scott, do you have some thoughts about this? Particularly in light of your ad choice efforts to help reach out to consumers.
>>SCOTT SHIPMAN
I don't know if I have a comment to the privacy lawyer from eBay but certainly as an attorney and trained in high-tech law I think one of the challenges you have got certainly as was raised is copyright. You also have some claims certainly against anybody that's altering the content of your site without your permission. Something we run into quite often and we defend vigorously against the challenge you face with respect to the ad choice model we have rolled out is in that context we're actually the ones voluntarily creating a system where users would continue to see the ads but it's the data behind the ads that are altered based ton user's preference so it's a slight nuance from what you're asking so it may not be a direct answer.
>>JAMIE HINE
Maybe Rob can follow up on that. I guess we would like to touch on some ramifications. This changed the whole ECO system. And what happens if something like ad block catches on much more than it does today?
>>ROB PEGORARO
So I won't speak from a legal perspective probably because I only play a lawyer on TV and not in real life. From an ad blocker perspective from a business model we want to make sure that users are getting the content they want to see. And from user experience, is this going to affect the content they're going to see? For blocking ads and is this going to affect what content is out there? If that's the case that's not a good thing for consumers. I think one of the things that I think I have not seen -- actual at seen the article or read it but one of the things is how do we reach consumers? What other mechanism are out there? And why there maybe some good players out there who do that, maybe there's other

mechanisms out there that I know that at others may do to provide the ads and get the ads out there. It might provide some other model we don't know about today if we're blocking banner ads on websites.
>>JAMIE HINE
Let's shift that. Maybe Zulfikar you would like to comment from Symantec's perspective. Because you empower consumers to control their online experience.
>>ZULFIKAR RAMZAN, SR.
Turns out you don't need to install special software on your machine if you want to block ads. That's trivial, just change one text file and add some information and you can block a bunch of ads. The core issue we're trying to maybe attack a specific instance rather than looking at the core underlying principle which I think Mozelle was alluding to earlier, a couple of other things I wanted to mention that came up that are related is that certainly we've talked about cookies and it's been clear that cookies are one part of the online privacy issue but they're not synonymous with online privacy. There's other ways to achieve the same kinds of effects. So for example, it turns out that -- getting an echo here. Turns out for example that if -- I wanted to implement a cookie instead of using the traditional cookie, there's other mechanisms I can do the same thing without resorting to traditional cookies. Maybe that's what it is. I was like my voice sounds really funny. I don't know why that is. That maybe is a little less annoying. Sorry about that. So the point I want to make is that from a technology perspective it's important not to just look at specific and sensor specific technology but the overall principle because some of these technologies are inherent in the way the web is designed. I don't think we'll be able to get rid of these concepts per se. So I think that's important to keep in mind.
>>MALE SPEAKER
Jamie, following up on that, this isn't something new the ad blockers. Back 7 or 8 years ago when we were reaching the threshold of dial up and things like that, people were using I think the largest penetration of ad blockers at that time was really because people wanted to conserve as much bandwidth as possible so the ad blocker at the time weren't as much a privacy issue. There was also served as stop allowing banner ads and tower ads. But it was because people, they were bandwidth intensive and people are on dial up and they wanted the motivation for them to download and use an ad blocker was that they wanted a faster surfing experience. And so I think the motivation for using those tools, I think what's the difference between your concern about privacy so you buy an ad blocker. Why wouldn't you go in and manage your cookies? So I think it's same equation now in the absence of a bandwidth constraint.
>>MALE SPEAKER
I want to circle back, come to you commissioner, Thompson, we heard -- we've heard several information about research but particularly Larry (indiscernible) research that touches on consumers and their desire to control their online experience. And to have more control over their privacy. And this implicitly suggests that trust is an issue. You've touched on some of these issues but I think that there has been amazing explosion in the growth of social networking

sites. And as Tim eloquently put it, people are -- can't get enough about willing to share the details of their lives. And so I know that you have done some work, social networking sites and if you can talk a little bit about is there something unique about social networking sites? Do they engender some different or unique form of trust?
>>MOZELLE W. THOMPSON
It's no secret that I've been advising Facebook. And not all of social networking sites are the same. They don't track the same audience and the behaviors are different but what I do think is a myth that -- is that people like to go to social networking sites and just like throw up on a page. I don't think that's accurate. I think that the social networking sites actually provide more granularity that allow you to decide who is going to get what information and under what circumstances. Is in some ways represents what the new privacy model is. Because there are instances, and Joe alluded to this when he was talking about blogs and copyright. People want information about themselves out to people. But they want to control who it gets to and under what circumstances. And so when you talk about copyright and blog, on some -- in some ways a blogger may have a copyright right that he has but he may not want to assert it because he wants people to pass it along. Now, whether that's attached the advertising or not, maybe something different question. But so what we're seeing here, what I don't want this conversation to get too far to go too far in, it's not necessarily a binary equation to add yes or no or information yes or information no. It's really much more sophisticated question than that. It's the circumstances and to whom and from. And it's not going to come from the top down. You're going to get information from your neighbor across the street or your college roommate. And that may include advertisements or it may not. So that's a different kind of model than what you ear visiting a website and they give you a cookie or not. Scott.
>>SCOTT SHIPMAN
It's not often that I actually purposefully agree with Mozelle but I think I'm going to here. But also highlight that a lot of what we're talking about is not new. Let's take eBay 1998, completely open marketplace for people to buy and sell.
>>MALE SPEAKER
Did I wish I would have bought eBay in 1998?
>>SCOTT SHIPMAN
Any user of eBay that bought or sold or anybody that registered for the community meant that when they registered they were willing to give their contact details to any other member. It was a completely open transparent marketplace. So that meant that any registered member with the simple request via email would receive the other and vice versa. The contact details. Now, we fast forward in certain aspects parts of eBay's original social networking capabilities to today and we have dialed those protections up and removed some of that functionality because in fact as we listen to the customer they didn't want and certainly as the site grew from thousands of members to 250 million members, they didn't want that information available to everyone. They wanted that information available to people that they did business with. People that bid on an item or that won an item successfully and vice versa with the seller. So we look

at the history, we look at transformation how information has been provided ton Internet. In many ways it's no different than the DDD acronym that we heard a minute ago, digital diarrhea. But it's as Mozelle said it's contact spaced and people are providing information to other people based on the context of the transaction whether that's the social networking website, whether it's an address so that an item can be shipped, payment information, whatever it might be. One of the challenges, to jump back to the cookies question originally. Cookies is but one way and many ways a poor way of collecting information object Internet. The most efficient way is to collect the information directly from the customer. And that's a server. That's not a cookie. It's not being stored on the customer's computer, it's being stored back in San Jose or whichever location your servers are at. And that's the real way that companies can collect and enrich a database by collecting the information directly. So the sphere about a cookie, it's a technology that is working adequately for advertising, it's not a very good technology for collecting information or for storing information. So really what we're looking at is the use practices and what we're talking about is how are people using information for advertising? Are companies providing choices with that information and how it's used? That's what we're trying to do with the ad choice program is provide customers with that opportunity to reflect how the information is being used with respect to ads. Mine
>>JAMIE HINE
Katherine?
>>KATHERINE ALBRECHT
In the last couple of minutes I would like to bring this back around to consumers. If we're talking about the future there's more than just technology. We agree that technology will evolve, it's going to evolve into the more online space on to the real world but the bigger question that I have as a consumer educator and someone who deals with consumers every day is how do we help them understand what's being done? One of the reasons why cookies and all these other technologies are so worrisome to people is because they're invisible. They occur in the course of doing something else, one is sort of almost detaching on to you like a pair site when you're -- all you're trying to do is order a set of sheeting for your bed or just walk down the street and other people are taking advantage of your preference and activities for their own reasons. I think that's where we need to do -- there needs to be an educational component here. I was stunned that in something like a supermarket frequent shopper cart, now 90 percent of American households have these things an people use them all the time and yet here we are almost 20 years into having this technology, this simple technology of a shopper cart and 75% of households don't realize that the data is being collected so we can sit here and talk all day long and come up with terrific ways in technological run around to help people protect their privacy but until they understand that these invisible things are happening to them, we're not going to get anywhere.
>>JAMIE HINE

Katherine I know you have done a lot of work with shopping loyalty cards. Do you see any analogies here in what consumers understand about the value proposition, the trade off?
>>KATHERINE ALBRECHT
In a way what's happening in the online world and why RFID is interesting is because they're more invisible. I wrote a paper called supermarket cards, tip of the retail surveillance iceberg because the supermarket card the visible plastic card people have hanging off their key chains for many consumers is their only tangible connection that there is this entire universe of data collection occurring that the average consumer has no idea about. The tangibility there you would think would translate into a greater degree of awareness, that's why I focused on that. I was stunned, if you actually ask consumers why do you think supermarkets offer frequent shopping card? Which I did in my dissertation research? They say because first they want to reward me, second they want to offer me deals and get me into the store and third they just love me. And I -- at each opportunity I said can you think of any other reasons? I prompted them three times an only 14% of consumers said because they want to know what my shopping history looks like. And even when I came then after that and we did something called prompted knowledge on -- spontaneous knowledge do you know it and prompted knowledge was if I tell you do you know it? I said to people, does the supermarket make a record of your purchases every time you scan the card? 75% of people said no. And in fact many of them said come on, I'm not a conspiracy theorist. I'm not paranoid. And people were adamant in absolutely insisting that their supermarket would never do something so despicable to them. You would think they would understand that but they don't. And the reason I think is because when I looked into how the supermarket frequent shopper card was introduced throughout the mid '90s, it was not introduced as a data collection card, it was introduced as a join the club we want to reward you, we love you. And most people for good or bad they believe what you tell them. So if you say come on our website because we love you and want to have you shoot the little -- and be part of our contest or whatever they will believe you. So I think there needs to be a greater degree of opens of saying here is the trade-off we're making. Very openly. We want your data.
>>JAMIE HINE
Jules, you had something to say?
>>JULES POLONETSKY
In terms of consumer education I want to tell you about something a couple of years ago. The FTC put to rest a practice, a flaw that allowed him to trigger pop ups on people's computers looking like they were coming from the operating system and sometimes the offers were help make this pop up stop happening and it used a security exploit. So when we became aware we started getting calls from members saying stop these pop ups. And we said what's going on? We're not doing it. We're not responsible for this. And we came one a little script and people were really annoyed. We started marketing this script, we ran banner ads, are you getting these? And we showed them pictures, are you getting these ugly pop ups? Click here so that we can run this script. And a lot of people did

and guess what? A huge majority of the people kept calling us which was expensive saying turn off those pop ups and we kept running these ads and finally we said let's just roll out a script and turn it off to everybody and one or two security people said why did you do that? I was like wait a second we just stopped this terrible thing happening to so many people but just think about the education. People didn't like it and in the same context were saying to them, hey, stop the pain, click here and we'll fix it. So we need to do so much more and I think we're all guilty in industry doing a little too late and putting more energy into this. Look at a site called Carabella which I like, it's a virtual avatar created by privacy activism, a college student and she has to make privacy decisions about whether she gives data and does a good job at sensitizing a jaded audience about what they should and shouldn't do. So whether the banner ads we run work or videos, clearly the web 2.0 noticed that after -- the lead challenge I hope everybody across the spectrum agrees with.
>>JAMIE HINE
Okay. We only have about five minutes left. So I'm going to try to move quickly to final topic. We have heard a lot of talk about trust. Consumers will do business with trusted websites and companies compete on trust. So I wanted to throw that out generally. How can we encourage companies to compete on trust? But also to think about how consumers can verify that their trust is well placed? Some famous person said trust but verify so I think we want to throw that out. I think I'll start with John.
>>JOHN THORNE
First thanks for including Verizon in the conversation. The town hall has been terrifically valuable. I can tell you from my being here two days. Something Mozelle said earlier deserves echoing that answers your question. That's the consumers actually respond to different levels of privacy. We follow very closely the third party reputation surveys like the (indiscernible) survey, Verizon has been on the most trusted list every year since it's been done. Number one in our category of telephone company cable company for the last couple of years running. We get measured on whether we're at the top of that list. But two small anecdotes. One is our wireless business was invited to put all the cell phone numbers for our wireless subscribers into a central database where you can have a directory. Somebody offered money for this, call up the wireless subscribers in the white pages or 411 kind of service and (indiscernible) the head of our wireless business said no our customers won't like that. We got people switching from AT&T and sprint and T-Mobile to come to our service when they heard that we were not going to participate in something that turned their telephone numbers over to a central agency. Sara Dutch in the back of the room had (indiscernible) on behalf of our Internet service provider. With the recording industry. I'm not going to refight copyright issues though they -- some people think that with the recording industry was doing with automatic robots issuing searching the web and issuing subpoenas was a privacy concern. We thought it was just illegal. And we fought the IRA. The experience was users wanted to switch from I won't name names down the table there. Other ISPs who were less confrontational with some of the copyright holders about turning over names so

we have found in our experience, you get more customers if you protect privacy. It's a -- it's in our interest to be good with this. It's a way to grow the investment we're making.
>>JAMIE HINE
Commissioner Thompson.
>>MOZELLE W. THOMPSON
Trust comes at various levels. It begins with how you talk to your user, your customer, about what your obligations are. Then for every piece, every piece of technology, every piece of functionality that you do something that's consistent with what that promises. And I really like your comments, Katherine because it really is true, that it's not -- it's a series of things that consumers test on a regular basis. The FTC knows more than it wants to about supermarkets. And it -- and so that's one example. But I can tell you for example in the social networking space that there's robust privacy protections on Facebook and people actually use it. Now, is there a gap between some people who should be using it more and they don't? Yes. So one of the things that could happen that would really be fruitful is for the FTC to shine its light on good practices. Because there are companies out there who are doing good things so that consumers know that they have choices and that where things look like they -- practices that are helpful to them and tools that are available to them, that the FTC can actually talk about it. I think that that's valuable. And I also think it's valuable for the -- for the online industry generally to talk itself about what those array of tools are that might be useful. Because it really is hard to get after the bad actors. But if you can begin to isolate what some of the good practices are, that's fruitful. And I think it's a real challenge to create a race to the top because a lot of business would find it easier to deal with mediocrity.
>>JAMIE HINE
Anybody have a response to the second portion of that question? Which was sort of verify. We've heard issues about that there are possible harms associated with, about discriminatory pricing. Let's say you have a consumer who has opted in to everything that they wanted to opt in. How can this consumer make sure that some of the bad practices that we've identified earlier may not be happening to them? Anybody want to take a crack at that? Mozelle and I are Facebook friends and I implicitly trust him with my data.
>>MALE SPEAKER
We began with home work -- we do.
>>MALE SPEAKER
I would go back to -- again my disclosure from last panel carries over to this one but I think that is one of the biggest difficulties in this area is the lack of transparency, the fact that consumers don't understand cookies and the fact they can't see it and can't verify it. That's one of the things that in this area makes self-regulation a little bit more difficult than maybe even other areas is that if consumers don't have the technological ability to verify on their own an opt out or some other procedure then they're going to look for a third party to be able to do that verification for them. And to give them some form of trust. Transparency is really the key and the issue.

>>MALE SPEAKER
Can I add one other thing? One thing that's change that's really important is there are more people out there --
>>MALE SPEAKER
We're running over so one minute.
>>MALE SPEAKER
They speak up now. If consumers don't like something, if you're doing something that people get wind of it will be on a blog, there will be 100,000 users in two days complaining about it. That's got to be encouraged, not discouraged.
>>MALE SPEAKER
Transparency and choice is important but there's combination of other good work other organizations are doing but people are going to vote with their wallet and with their -- and if they feel they're being misused on a website they won't go back and visit.
>>JAMIE HINE
It is now 3 minutes past 5:00 so we're going to have closing remarks and if everybody could stay.
>>LYDIA PARNES
This will take a nanosecond. Thank you for staying until the end here. This has been I think a wonderful effort. Again, we want to thank the people on our staff who worked so hard on this.
>>LYDIA PARNES
I'm going to name them one more time. In no particular or order. Peder Magee, Lorrie Hines. Joel Winston, Stacey Brandenburg, Mimi and Tracy Shapiro and numerous of our wonderful honors paralegals.
>>MALE SPEAKER
Will they have cookies waiting for them?
>>LYDIA PARNES
No, I have a suggestion for everyone in that regard. We're very pleased I think with the good start that we've made over the last two days. We have learn ad lot more about behavioral advertising including some about how it works and the Consumer Protection issues that it raises. We have had some debate on the issues including whether disclosures work at all in this area. And whether existing models for managing privacy are adequate. We enjoyed the You Tube videos and greatly benefited from the participation from all who attended and hope that you found that the town hall nomenclature really carried with it a difference in your ability to participate, ask questions and interact with other participants. We heard some general agreement I think about certain issues which should help our efforts as we go forward. First, behavioral advertising is clearly a growing practice. And it is largely invisible to consumers. Though reasonable minds can differ as to whether the practice itself raises concerns there appears to be a fair amount of agreement that greater transparency and consumer control would be a good thing. Recognizing of course the limitations on notice and its value. There are also legitimate concerns about what happens to consumer data. Very legitimate concerns. That is collected for advertising. Is it limited to use in advertising or could it be used for some secondary purpose?

What if it falls into the wrong hands, especially if the data are sensitive or personally identifiable. Now, whoever was here at this town hall is obviously thinking very seriously about the challenges here and what the best approach might be for managing privacy in this area and so are we. Based on what we have heard we would like to see a reasonable approach to this issue. That is flexible, that doesn't stifle innovation, that gives consumers information and control without placing unrealistic demands on their time and their willingness to study and analyze long disclosures, that prevents harms from arising from the collection and storage of the personal data collected, and that creates accountability among businesses that are collecting and using the information. -- using the information. We think these are not unattainable objectives. Some of the ideas that we have heard over the last two days are promising. They include a do not track program, reforms to existing NAI requirements, and better consumer education as illustrated by the You Tube contest. And we need to examine these and other ideas more closely and we will and we encourage you, all of you to do so as well. And to continue to engage with us and suggest new ideas. At the same time that we think this has been enormous hi productive, I think that we also have a sense that we haven't yet seen or heard enough of the concrete and specific facts about information collection in connection with behavioral advertising. And its actual implant uses nor have we seen or heard concrete suggestions for improving Consumer Protection and privacy in these areas. So we're going to keep coming back asking for the concrete. I think there has been a certain guardedness opt part of many -- on the part of many companies involved in behavioral tiding. In describing in this form exactly what they're doing and maybe this is not a forum for our old boss Jodie Bernstein would like to say, open kamona but we want it opened so we're going to keep coming back and asking questions here. Finally you should go out and have a drink. This is, you know, or whatever it is that you do. I myself, I would go for ice cream. But this has been a long haul. Intense information packs and everybody here has worked hard so it's 5 o'clock on Friday afternoon and now you should all go off and do something far less wholesome than sitting in this room. So thank you, everyone, for your participation. [Applause]