

>> Katie Harrington-McBride: 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 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 not 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 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 restrooms 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 panelists who will be arrayed here. We'd 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 tail wind, we'll finish in time so that there is Q&A time. People who are watching on the webcast should feel free to e-mail 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 one of the members of the Privacy Roundtables team. In the event of a fire or an 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 can we know that you have 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]

>> Maneesha Mithal: Thanks, Katie, and thanks to 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. And 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's got a lot of energy and enthusiasm, and he's the Chairman of the FTC, Chairman Jon Leibowitz. Chairman Leibowitz is no stranger to privacy issues. Since he started at the FTC in 2004, he's spoken on a host 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 whois databases, and we had a really spirited discussion. So with that, let me introduce Chairman Jon Leibowitz. [Applause]

>> Jon 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, people who have really worked on these, Lee Peeler, Marty Abrams, Susan Grant, the eminent and

distinguished Marc Rotenberg, Jeff Chester was around here, Dave Morgan. So, really, I think this is going to be a 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 founders 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 -- and I'm quoting -- "Numerous mechanical devices threatened to make good the prediction that what is whispered in the closet shall be proclaimed 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 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 *Olmsted*, 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 -- "The right be let alone was the most sacred of rights and the right most valued by civilized men." In the 1960s, as Americans started to lose faith in government, and the 1970s, with the abuses of government surveillance powers, together with the advent of the computer age, created more firment around citizens' privacy rights, vis-a-vis, government. And the Private Act and the Fair Information Practice Principles -- the FIPPs, I like saying "The FIPPs." You want to say it with me, the FiPPs? You don't have to do that -- 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 Targeting Principles and take a broader look at privacy, or look at privacy writ large. And let me explain why. One of my advisers is about to buy a home computer with a quad core chip at 2.66 gigahertz. It costs under \$2,000. In the early 1990s, 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 consumers 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 targeted -- 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 moreso than when he dissented in *Olmsted*. 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 profits of targeting ads? How many people understand the network's role and other intermediaries' role 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 track the consumer's meanderings around a 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 *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 YULA, that disclosure wasn't sufficiently clear or prominent giving 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 e-mails. So consumers didn't consent with an adequate understanding of the deal they were making. Now, nobody argues that 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 in choice approach and later the harm-based approach or regime, haven't worked quite as well as we would have liked, but

it could be that this issue is a lot like Churchill's description of democracy, and he said, I think, "democracy is the worst 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, try to think it through in a way that is better for consumers, fairer to businesses as well. We all agree that consumers don't read privacy policies or yulas, for that matter. And I think most people now acknowledge that you can't focus on traditional PII, such as name and address, when particularly 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 consumers' 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 discussions 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, Mozell Thompson, here. So we are delighted that you could be here. former FTC Commissioner Mozell 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 when I -- unless you're already standing up in the back of the room, then raise your hand. If you could stand up or raise your hand when I mention your name. Loretta Garrison, Peder Magee. Peder, you're right in front of me. Good! Katie Harrington-Mcbride, who started us off this morning. Katie Raddy, Michelle Rosenthal, Miomi Leftkovitz, Jessica Skretch, and Randy Fixman as well as Assistant Director Chris Olsen, who's around here somewhere, back in the corner over there. Associate Director Maneesha Mithal, who introduced me. Maneesha, where are you? You're in the front next to Jessica Rich, that's right. Of course, Deputy Director and former DPIP Associate Director, Jessica Rich, David Vlastic, who is in the back over there, who is the architect of so many things in the Bureau of the Consumer Protection. We're delighted you came over from Georgetown to be part of the Commission. 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 that you're part of the group that's thinking through privacy, particularly privacy online. I want to thank you all for 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?

>> Female Speakers: Yes.

>> Jon Leibowitz: 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 very much!

[Applause]

>> Katie Harrington-McBride: 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 the people on panel one to take their seats so that we can be ready to go as soon as Mr. Smith finishes his presentation? Thanks.

>> Richard 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 a collection of data and the use of data by multiple vendors. You know, simply to make a cell phone call might involve five different companies, typically, that collect data as part of making, completing that phone call. And what I hope to do in the introduction here is to go 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, you know, starting up with Brandeis -- it's technology-driven, that we're seeing a lot more interesting uses of the data and a lot more collection of data, an explosion of a 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 are driving this data collection ecosystem. One illustration of technology that I wanted to point out here -- 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 1-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. They hold information about what we're talking about here today, the data that's collected as part of transactions. Well, what is 1 terabyte of data that you could buy today? That's equivalent to 300 million sheets of text, of printed out text paper. That's one piece of paper for every citizen of the United States that could be held on one hard drive. Now, we make hundreds of millions of these drives per year. And as the Chairman has pointed out, it's basically now free, 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 that 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. And it's -- really, there are 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, you know, in the last 15 years, from the internet being something that was in universities to something we all use, and we no longer -- we used to connect up to the internet through modems, and now we do it through cable, you know, cable connections and DSL connections or wireless connections. And that's the other important communications network that we have is the wireless O-network that allows us 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's collected in our world. And the purpose of the chart is to show from the consumer perspective, you know, what they see as data collection, and then things that are happening also behind the curtain. And in this -- 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 much 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. But in the ecosystem, we have the center here, the consumer, which is the data supplier, and they provide the information to, you know, as part of their, as they go about their daily lives. There are a variety of what we call data collectors here. And they can be all sorts of organizations, you know? They can be businesses that we interact with every day. They can be in the area of medical. They can be our doctors or our pharmacies. We get into government collect 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 could 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 are really 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. And this is an area that a lot of consumers are only vaguely aware of. And then we go out to the outer circle of the chart here, and we see all the different -- we see some of the different users of this data, who buy the aggregate data. You know, 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 and to this aggregation data, and it can be an extension of credit, it can be advertising. It could be a whole host of things that the data users then bring back to the consumer. And in some cases, the consumer is aware of these services. In other cases, they're not, not particularly aware of. And the one thing that's important here is that we have, you know, both the primary user of data and secondary uses of the data. You know, 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, it's a secondary use. What we're also 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, like a lot of folks had to start taking pills to regulate various health issues. And so, one of the things that I have to do is get my prescriptions filled at the local pharmacy. And here we have a part of this data ecosystem how information is used to perform that service, some of which are very -- 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 the prescription. I then take it to my pharmacy, where information is entered into a 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 gets renewed for up to say a year. And it's up to the pharmacy and their computer system to keep track of those refills. And so, one of the benefits, then, I get as a consumer is I don't have to go back to the doctor for every prescription. So, when the pharmacy fills the prescription, they enter the data into their computer systems. And one thing they do, a new service that the pharmacy's are 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 is this, you know, paying for my pills through the health insurance. The health insurance company's 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 various -- 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. 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 is in an area that's been controversial. Some legislation has been done against. But the idea is that the pharmaceutical companies, you know, 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, you know, Facebook and MySpace or LinkedIn, which provide a way for people, for friends and colleagues and even strangers and whatever, to communicate. Basically, provide a community where people can discuss in a semi-private area, you know, 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 that 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. For example, Google people, some of the first things you

see will be profiles at places like Facebook and LinkedIn. But then also, there's other parts of the information that is only available to, you know, people that you trust, you know, friends and people who you agree to be connected up to. But a whole other aspect going on behind the curtain in the social networking sites is the use of information from 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 in, you know, either in the profile or the forums. And another area that becomes very interesting is, many of these websites 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, reported by advertising and what folks are using these websites in many cases don't realize is, these applications also have access to some amount of the 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's become much more important over the last, say, three or four years, is mobile phones or SmartPhones in particular. A SmartPhone is basically a computer that's portable and just happens to have a cell phone attached to it. But the key thing about that computer is 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 SmartPhones 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. And so, you have a very powerful combination there for doing data collection. You have a smart device that can run applications, arbitrary applications, you have a communication network which allows it to phone home, and you have something that provides location. And so, we have -- 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 -- a couple different applications using SmartPhones. 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's providing coupons. And

the application runs. And as you execute it, it will provide you with a variety of coupons, and you can do things like say, "Here's the kind of coupons I'm interested in." [Timer beeps] Excuse me -- I still have 30 seconds. [Laughter] In spite of that. The idea is, you say what kind of coupons you like, whether it's restaurants, bars and so on. And 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'd want this one -- but it's 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. They also have to opt in to this service. And so, the idea is that it's a Friday afternoon and you want to get together for dinner that night, you can go see if everybody's -- who's close by and then meet up. Again, what else is going on behind the scenes -- you know, it's a free service, so there's advertising that goes on behind the scenes. And so, the ads are shown as part of the map with the idea of trying that for you, where you can meet your friends at. In addition, one other service we looked at allows you to also upload your position to your social networking home page. So, not only can people with phones 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 -- you know, if you go back 20 years ago, we would be accepting. But it's out there. And it's something that people, if they want to participate in, can. With that, I'd like to move on to the first panel here. And thank you very much for the opportunity for speaking. [Applause]

>> Chris Olsen: Thank you. Can everyone here 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 people to squeeze in if there are open seats in the middle, I'd ask folks to try and do that. We have some panelists, I see, in the back there. Some reserved seats up front 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'd like to thank everyone for coming. First, I'd 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 are very pleased 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 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 Privacy Group. Anita Allen could not make it here this morning, unfortunately, and we apologize for that. I'd 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's 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 in their everyday lives is gathered, analyzed and shared among companies for marketing and other purposes. We'll 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.

>> Jeffrey 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 was, of course, not only the patron saint of the 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, it was the Kodak camera and the tabloid press that made him concerned that what used to be whispered in the closets was now being shouted in the rooftops. By 1927, in his famous Olmstead Dissent, it was a different technology -- namely wiretapping that made it possible to listen in on telephone conversations without physical trespass. But Brandeis was astonishingly prescient. In a remarkable passage, he predicted the invasions of the Internet. He said that ways may someday be developed by which it will 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 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 wiretapping 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 are 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 am going to begin with a scenario that many of you will recognize. We'll ask our panelists to talk about it, and then Chris and I will alternate with other scenarios. Here is 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 friend's medical 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 protocol address of every user who watched it. In the face of privacy concerns, Google and Viacom negotiated a plan to anonymize 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 Lewinski 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. But these disclosures that we're thinking about today -- AOL search terms, Google search terms, YouTube volunteers 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?

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

concerned that they will be, you know, labeled, identified, that that piece of data will be combined with other data, you know. I think when you talk about search data, you're talking about search data over time. I'll get back to in a minute whether or not I think it has to be hacked in order to do this, because I think that, you know, 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 you know, 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 mean, 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's a technologist, trying to figure out how all this was connected together, ran into a network -- not one of those who publicly is talked about. But Yahoo! And Google now are creating these spaces where you can see what you're being searched against. It was none of those that we know. And most prominently, it said they were searching on medical marijuana and marijuana. I mean, it's sort of on its face for the individual we're talking about, and about 50% of the other things that were on that alleged profile made absolutely no sense. But you know, that's a single data point that was plainly connected to her through cookies. And, you know, it's pretty appalling. I could have gone on her computer and seen that, but we also want to know what's happening with that data.

>> Jeffrey 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?

>> Susan 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 maintain 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.

>> Jeffrey Rosen: Nice way of putting it, the chilling effect can harm both these interests, and anonymous reading, and also businesses that are trying to encourage the use of these technologies. All right, so let's start to think about potential solutions. Anonymization is obviously one. Can anonymization address these fears, or is the distinction between personal identification and nonpersonal identification is 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?

>> Alessandro Acquisti: Well I did these -- I do agree that we are in a -- the cost of what constitutes sensitive data has changed. We could take P.I., simple personal information, which may not be very sensitive, and can aggregate an interesting way and obtain identifying information or very sensitive data, passwords. That said, I do see anonymization, more as an economic problem than a technical problem. I'd like to explain what I mean so it doesn't sound like another case of economic strength being an imperialist science, focusing every other discipline, including computer science. The point is that the research in the last five, ten years in computer science of privacy and anonymity has made enormous progress. We do have a very good theory over when a certain system can be provably shown to be anonymous, and we have the technologies to protect the data. However, the conditions under which data can proven to be anonymous, like in economic models, don't often alter reality. In a sense, the attacker can often bypass these kind of constraints, these conditions, can use additional data that the creator of the model did not consider. And in the world of sophisticated data mining, cheap storage technology and incredible amount of self-revelation, in blogs, Twitters and a lot of social networks, it is very easy to bypass this kind of protection. And now, my message, it's not, therefore, that, you know, privacy is lost, get over it, and I don't mean to use "impossible" in this world, is instead that privacy and other technologies may not be assure accruable anonymity in any condition, but can make work of really defining data harder. It's more costly, which means that it reduces the incentive for another entity to try to defy that which has

been protected. And more important than that, the best privacy technologies, the best bets, do not simply lock data. They try to allow certain data to be shared, which is usually for further consumer and further corporation, while they stop and protect other data. We can -- I'm a strong believer in technology, and I do believe that we can use technology to meet the interests of both parties.

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

>> Richard Purcell: For search -- well, first of all, anonymity is not yet well defined. And so, we struggle to a great degree with making a lot of assumptions, like privacy, like happiness. A lot of these words are words that are more subjective than objective. So, it would be -- first of all, we have to begin to think about what anonymity means. And frankly, we have to start thinking about -- 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 has 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 and preventing any exposure? Whether a time-outs can matter, whether it be 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 of that. What I worry about mostly 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 health care understanding, as well. This is a very serious problem that has to be overcome.

>> Jeffrey 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 they can sell ads and also avoid these dangers? I wonder, Michael Hintze, if you could talk us through some possible solution? Should there be data retention policies, so that the data may not be retained more than a period of time, therefore, it can't be accessible, even if demanded? Collection or use restrictions? Increased transparency? What, in your view, are productive solutions?

>> Michael 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 collect 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. But 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 most innermost 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 up front. 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 with the ability to link search queries over time -- and when you've got, 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's been out there on the internet for 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 of 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 majors 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.

>> Jeffrey 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?

>> David Hoffman: I think it depends how you address the question. You can always come up with a period in time that is 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 about -- 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, you know, 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 needs 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 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 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 -- falling into the category of personal information have been tremendously burdensome in different regulatory structures. If we can instead focus on what is the information that's potentially going to impact an individual, either beneficially or to their detriment, and then 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.

>> Jeffrey Rosen: Last question for this first scenario. Jim Harper, you are our Brandeisian 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?

>> Jim Harper: Well, thank you for that Libertarian softball, first of all.

>> Jeffrey Rosen: Sure. Anytime. That's my job.

>> Jim Harper: No, I prefer not to argue at level back and forth, well, too much regulation would be too harmful. It's undoubtedly true that moving in too early in an area where we don't know well enough what consumers' interests are and what the future of technology or business models are. That would be damaging. I think everybody recognizes that. So -- 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 -- 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. Should it -- is this big enough problem? Should there be anonymization? Let companies challenges each other's anonymization practices, facilitated by the press, facilitated by advocacy and sometimes 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 with history of advancing technology.

>> Jeffrey Rosen: Great. Thanks so much for a fine first discussion. For our second scenario, Chris?

>> Chris 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 users' 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 fiancée, ruining the surprise. Recently, after protested 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 scope of use or unanticipated use issues that this presents?

>> David Hoffman: Well, I'm struck by a story that I heard from a colleague of mine who's one of, I think, the most world-renowned experts in data protection and new media, who said they were meeting with some business people, and it took an entire day going through on the whiteboard to 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 business 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 there's -- we've 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 -- understanding that 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.

>> Chris Olsen: Thank you. You commented on the difficulty that consumers have in understanding the scope of data flows, and that raises the question about whether there are things 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?

>> Leslie Harris: Well, I mean, I think there have been sort of some green chutes 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, you know, limitations on collection, limitations on use, limitations on retention, transparency, you know -- that I think if we would shift the focus, you know, the policy focus -- and that, I think, would include the FTC focus -- yeah, it's very important for good companies to be, you know, 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. You know, I think these tools are important. You know, we just initiated a campaign to get more of them out there in the marketplace. But you know, that's not a whole answer to this, by any means.

>> Chris Olsen: And some of the efforts that you talked about and we discussed earlier, the efforts made by Google and Yahoo! are --

>> Leslie Harris: Very important.

>> Chris Olsen: Are important, but I guess it raises the question about other activities in the marketplace. What about 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?

>> Leslie Harris: We regulate them.

>> Richard Purcell: The --

>> Leslie Harris: [whispering] We regulate them.

>> Richard Purcell: We regulate the hell out of them.

>> Leslie: That's what I was muttering over here. Regulate.

>> Richard Purcell: I've been doing this for quite a long time, in major corporations and with major corporations. And the Federal Trade Commission wants informed consent. I mean, if we had informed consent, we'd be a lot happier. And there are serious limits now because of the complexity of the data flows that David mentioned, because of the issues that Leslie's 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'd much prefer to pay my lawyers their fees to just put up a really complicated and dense privacy statement, and that way, I'm covered." But "I'm covered" is insufficient. You've got -- my opinion -- we've got to encourage companies to start taking on a more courageous role in not only educating their workforce, 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. And we'll hear later today on some of the panels with Jules and others how that is beginning to take some traction. 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, you know, kind 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.

>> Chris 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, you know, the two scenarios that I played out, are just that, they're two scenarios. You know, is there a larger concern represented here? Are these anecdotal stories? You know, how do we measure the significance of this issue?

>> Jim Harper: Well, I think a thing to do with these scenarios is to flip how we look at them and recognize the role of trial and error in 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, they say, "you know, data can be re-identified, you know that Yahoo! case." And we race at meetings to talk about, you know, how the Beacon thing

went. And also, broader communities in the public learned 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, much as we like to and 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.

>> Chris Olsen: Thank you. Alessandro, you had a comment you wanted to make?

>> Alessandro Acquisti: Yes. I would like to raise a slightly dissenting opinion on the topic of notification and transparency, which are good things, important things, but they are not enough. And I say this knowing that education identification can work. The studies we are doing at CMU -- and also indicate that that can help consumers get closer to their state of the privacy preferences. However, I see notification control, transparency, as the necessary conditions, but not sufficient. And I say this not as an activist, but as a researcher. Right now, a wealth of behavioral data and politically based showing what are the gaps between what consumers want, in terms of privacy, and their ability to achieve these stated intentions. And there is, first of all, a problem of isometric information. We often know if our data is used and how, and maybe we can address that problem with education, transparency and so forth. But there are other programs that simple transparency and notification doesn't help address here. There is the problem of irrationality, and the idea that we are bounded in our ability to act on information. And there are a number of cognitive behavior analysis that do affect decision-making sometimes and end up making people choose things that they later regret. And it happens often in the case of privacy, because privacy costs are often long-term. We don't feel immediate loss when we reveal data. Nothing bad could happen, but if it happens, it's usually later in time. Sometimes, much later in time. And it has proven again and again by research that we are very bad at making decisions when the benefits are immediate, but the costs are much later in time. And there's an issue that it seems the privacy costs are coming through varieties. They raise -- in terms of value, but very high frequency and variably, you know, spam, for instance. Or they are very high in value, very dangerous, but very low in probability,

such as being arrested for a case of mistaken identity or other extreme scenarios. And both cases are difficult for us to deal with, because cases where there the risks are high, but low probability, we tend to dismiss them and overestimate the probability, considering it even lower than what it is. In cases where the instead the probability is high that an event occurs, but the cost is more, such as a spam or other similar examples, we tend to overstate that, because we don't understand how the costs actually accumulate over time. Each of them is both. But over the period of time, they accumulate. And to give an example, not privacy-related -- many smokers do realize that smoking causes cancer. They realize that each cigarette increases, by a minimal amount, the probability of developing cancer. But the challenges that understanding that the next cigarette you're about smoke will really be part of a longer chain of all the cigarettes you will be smoking over the rest of your life. In the privacy case, we have a similar condition. We do realize that revealing more information will accumulate over time, but actually, we don't move into the next step of acting on that concern.

>> Chris Olsen: Thank you. I would love to let all the folks jump in here. We're on a tight time frame, 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.

>> Jeffrey Rosen: So, our third scenario comes from the world of list brokers. Imagine this -- you're suffering from depression. In the course of your online research about depression, you fill out a survey that includes personal information, which you hope will get you the help you need. Soon after, you receive aggressive pitches online and through e-mail, promising cures for your mental health problems. You wonder, where did this information come from? It turns out that there's a list that marketers can buy to identify people just like you. Here's an excerpt from an actual description list. "Medmet have 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 products 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? [Laughter]

>> Susan Grant: Well, this is not a new concern. This concern has long existed with telemarketing and mail marketing. I think that 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's 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 the -- 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.

>> Jeffrey Rosen: That's great. Jim, can you give a whole-hearted account of what the benefits might be?

>> Jim 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. [Laughter] 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've been a skeptic, 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. There are certainly, 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.

>> Jeffrey Rosen: Leslie, harms and benefits -- why don't you advance the thought about whether this approach that both Susan and Jim has suggested, a sectoral approach, identifying particularly vulnerable consumers, or particularly sensitive categories of information, might be a way of balancing the costs and benefits?

>> Leslie Harris: Well, I do think 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 altogether, 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 the 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, you know, that we should somehow -- I mean, I just think you've got a binary choice here that doesn't make sense to me. I think that some kinds of advertising can happen, but it's got to be very serious, option 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'd be willing to get offers from, or you're comfortable hearing about health -- 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.

>> Jeffrey Rosen: We can imagine that certain kinds of intrusive 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?

>> Michael Hintze: I think the answer is yes, and the discussions around ads and ad targeting have addressed some of those, as some on the panel have already suggested. You know, around different sensitive categories or vulnerable populations. I think, you know, 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, you know, 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. And so, I think it really comes down to responsible practices versus irresponsible practices, recognizing that's hard to write down in rules and legislations and regulations.

>> Jeffrey Rosen: Great. So, what's now on the table, squarely, 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?

>> David 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 a 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, you know, 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 decision maybe based on cost and the functionality of the toy. It's this concept of, 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 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 with higher level principles and then with people getting together to talk about in individual situations, how do you realize those principles? You know, transparency being very important, but just being one component of those principles, in with certain technologies 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?

>> Jeffrey Rosen: Great. Well, Richard Purcell, it falls to you to propose a model regulation for this thorny question of niche marketing. Is there effective consent, or should it be explicit? You can cut it out for us.

>> Richard Purcell.: Sure, great. [Laughter]

>> Jeffrey Rosen: Have fun.

>> Richard Purcell: Great. Really, I think that David's points are very well taken, well said, well taken. It's very important. People should -- 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 waving 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. And for the most part, reusing sensitive data should be proscribed out, it's just off the table. At that point, we could start the real argument.

>> Jeffrey Rosen: That's great. For our fourth scenario, Chris?

>> Susan Grant: It is possible to make one point?

>> Jeffrey Rosen: Unscripted question, certainly.

>> Susan Grant: We're talking about data brokers here, and I just want to make the point that because there is 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.

>> Jeffrey Rosen: That's great. Chris?

>> Chris Olsen: Yeah, I wanted to interject with one, 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 and archives of information and maintain audit trails for business decisions and to recover possibly deleted data?" I wonder if David or Michael can address, as they are two of the industry reps, about that question?

>> Michael 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 you do need -- 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, as I mentioned earlier. But within each scenario, there's -- 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 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.

>> Chris Olsen: So, a risk assessment process, depending on the data.

>> David Hoffman: Can I just add one thing to that? I do think it's an important thing for us to think about, 'cause I think we also need to look very carefully at any requirements that force 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 up front to minimize their collection to begin with, so --

>> Leslie Harris: Make my point -- [Laughter]

>> David 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.

>> Chris 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 an item you bought was defective, but the merchant didn't agree and wouldn't give you a refund. The merchant adds you to badcustomer.com, a list of consumers who 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. [Laughter] 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 it. Do you want to talk about this a bit further?

>> Susan Grant: Sure, and there are lots of other secret lists, as well. There is 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 FRCA, Fair Credit Reporting Act requirements. So, not only is there is 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.

>> Chris Olsen: We talked about sensitive or vulnerable categories of consumers. Does this type of list create concerns about potential, you know, socioeconomic distinctions being made, vis-a-vis, certain consumers, whether they're entitled to specific benefits or services?

>> Susan Grant: I'd 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 know, you've been denied or treated this way because of a 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.

>> Chris Olsen: Leslie, did you want to add something?

>> Leslie Harris: Well, I just think the key here has got to be some kind of access in correction rights. And I don't think this is just aimed at particular populations. If we talk about what we need to move beyond individual practices and into law, I obviously disagree with Jim that we ought to be doing privacy by trial and error. I think we need a baseline law. And a key part of that has got to be access in correction, and that's got to apply to everybody, including data brokers. And that's just a -- I think a key element. You will always have, you know, 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 mean, 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 we don't have the tools, and the FTC, I don't think has the tools, to truly 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 of this data is being used for, you know, I really think it's incumbent on 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's accidentally revealed. So, we talk about AOL or we talk about the Facebook, which are sort of, you know, kerfuffles 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, you know, whether that's law or a new set of -- for the FTC. We've got to get a different information base we don't have.

>> Chris Olsen: Thank you, and 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 you a chance to comment.

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

>> Leslie 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.

[Laughter]

>> Jim Harper: I was just interested in making a brief comment, though, on the idea that the Fair Credit Reporting Act-style protections would be appropriate for the kind of data in this scenario, and I would be concerned with applying those kinds of protections, perhaps, in TOTO, because the Fair Credit Reporting Act prevented state tort law as to credit bureaus and prevents people from suing on the basis of defamation or interference with prospective economic advantage. The causes of action 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, so --

>> Leslie Harris: I agree. No state preemption.

>> Jim Harper: Deal. It's done.

[Laughter]

>> Chris Olsen: Let's move now -- time is running short. Let's move now to the last scenario.

>> Jeffrey 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 credit-worthiness, 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 practices, 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 fund-raising 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 call this our Brandeisian, but when Richard Smith mentioned the mobile friend locator, I thought Brandeis would have shuddered. His form of social networking was being -- 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 Athenian democracy. I mean, that was sort of the extent of his social networking. [Laughter] Do you want to give a defense of what these sort of targeted ads, based on your friends' buying preferences or your buying preferences in real time might be? What are the benefits?

>> Jim Harper: No. I don't want to do that. I want to raise an additional concern that has not been discussed yet today, or essentially. 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. Of 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 e-mail and the "cloud" is a huge, 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 Segoin, who is here, released a report that I may get 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 million 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 on the terms -- if it's available to governments on the terms it is now, that is a surveillance system that we have -- 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.

>> Jeffrey 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 whole-hearted defense of what the benefits of mobile advertising might be?

>> Michael Hintze: Whole-hearted, I'm not sure. [Laughter] 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 when you might actually use it. So, I'm not going to say that location-based advertising is a bad thing. I think on the 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. I mean, 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 issue.

>> Jeffrey 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?

>> Alessandro Acquisti: Well, potentially, you can think of how to collect -- to say adverse prices to show and desired advertising. However, the point I want to make this way by saying, was that this scenario is a good example of what I was referring to earlier, talk about technology, good price of technology. Don't simply dock information. They allow a nice balance between sharing some data, protecting our data. In the specific case of behavior, location-based advertising as seen in the literature recently, protocols and technologies based on this blind signature algorithms, which were developed back in the '80s by David Chaum and led to further research into anonymous payments and anonymous voting and anonymous credentials. So, we do have technologies that allow you to be authenticated, authenticate the transaction, know that the consumer is in a certain location and

desire certain type of advertising, without defining 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 this is where it maybe be solutions. Where certain to push the market into adopting this technology may technically work.

>> Jeffrey Rosen: That's great. So those technological solutions are helpful. Let's think about others. David Hoffman, can I ask, what about a risk-based approach, privacy impact statements? What are other regulatory approaches to this problem?

>> David Hoffman: Well, I think what you're asking is, for individual companies that are going to either be releasing technology or designing the services on top of it, are there ways that that can be done in a more privacy-friendly way? And I think that's absolutely right. And I think we need to see that in the terms of the greater context of accountability, which is this idea of how are you structuring that into your individual 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, you know, 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.

>> Jeffrey Rosen: Richard Purcell, you've been our deus ex machina in many of these areas. How could principles of accountability be implemented specifically?

>> Richard Purcell: Well, they need to be implemented, without a doubt. Keep in mind, accountability can be reciprocal. So let's say 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 responsibilities I expect out of them. And if they could agree to that, then perhaps we'd 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, "ugh, 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 are creeped out by it. So, 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 am going to be tracked by my mobile provider, perhaps I need to track the officers and directors of the mobile company, as well, to 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.

>> Jeffrey Rosen: We have time for one last comment. Susan, as a representative of America's 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?

>> Susan Grant: No. I think that if we want to talk about how to get companies to respect consumers' 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 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 travel company going bankrupt and all the information that's collected about their travel, then 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 the information that they either unwittingly supply, or are asked to supply for another purpose, and we really need legal protections.

>> Jeffrey Rosen: That's great. Well, ladies and gentlemen, as you know, privacy discussions can be abstract and unfocused, unbalanced, or they can be illuminating and precise. And I think 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]

>> Chris Olsen: And I want to add a word of thanks to Jeff Rosen for helping to moderate this panel, as well. Let's give him a round of applause. [Applause] We're going to have a very short break, try and keep it to ten minutes, and we'll restart the agenda at 11:05. Thank you.