

>> Jessica Rich: Everybody take their seats, please. Hello. So, I'm Jessica Rich of the FTC, and these are my co-moderators, Peder Magee and Katy Ratte, who you met from prior panels. And we're hoping that this last but not least panel at the end of the day will be, you know, the best. Keep everybody awake, and send you away with good thoughts. On this panel, we're going to explore the virtues and drawbacks of the existing regulatory frameworks and how they might help us think through the issues. Obviously, the existing laws and the approaches that have been taken are highly relevant as we think about future approaches. Questions we want to think about are, what have we learned over the years, as we've implemented and applied various privacy models? Have these models kept pace with our changing data landscape? What's missing from these models, are there elements that need to be added? How can we use our experiences with these models to identify privacy approaches that would work well in today's world and would also stay flexible enough to accommodate changes in the future. I have a really outstanding panel to help me discuss these issues, and all-star privacy panel. In alphabetical order, we have Howard Beales. Howard is a former bureau director at the FTC, as I think most people here know. And he's currently a professor of public policy at GW. He's one of the principal authors with Tim Muris of the so-called "harm based model for privacy," which we'll talk about. Fred Cate is down there, he's a professor of law and director of the center for applied cybersecurity research at Indiana University. He's also senior policy adviser to the center for information policy leadership and Hunton and Williams. Charles Curran, known as Chuck, is the Washington-based executive director of the national -- network advertising initiative or NAI. He leads NAI's efforts to develop and enforce self-regulatory standards for online behavioral advertising. Michael Donohue -- you can't even see Michael. There you are. Since 2001, Michael has been a policy analyst at the OECD, specializing in privacy, information security and consumer policy. He's also a former FTC'er, not that we wouldn't have invited him anyway. Evan Hendricks is the editor, publisher and founder of "Privacy Times," a Washington newsletter that covers a wide-range of privacy subjects, including the fair-credit reporting act. Actually, most notably the fair-credit reporting act. Barbara Lawler is chief privacy officer at Intuit, Quicken and Quick Books and former CPO at Hewlett Packard. She actually rolls up her sleeves and does all the things we're talking about. So we want to hear from Bard. Marc Rotenberg is president and executive director of the electronic privacy information center -- EPIC. And one of the most vocal and visible privacy advocates in the world, I'm going to say. And Ira Rubinstein is a senior fellow at the Information Law Institute and an

adjunct law professor at NYU Law School. He spent 17 years at Microsoft, also, as one of its main regulatory and privacy lawyers. So all of these people bring enormous experience in privacy, and has been around during the various privacy debates over the years. So it's wonderful to have them on this panel. Let me just lay just a little bit of ground work for what we're going to talk about, which is most people here now that the U.S. has a number of laws governing privacy in certain sectors. The so-called "sectoral approach." Laws include the Fair Credit Reporting Act, HIPAA, Graham-Leach-Bliley, the FTC act which we've used in the privacy and data security area, even though it's not inherently a privacy statute, and, you know, many, many state laws. There's no general privacy law in this country. And so the FTC at least in applying the laws that we enforce has used a combination of enforcement, education and encouragement of self regulation and has used basically two approaches over the past two decades in doing this. The first is the fair information practices approach. And as I think you'll hear from some people on the panel, we have our own version of the FIPs, and ours was notice, choice, access and security. And the focus of that approach was on transparency, consumer choice and accountability. And when, during this time period we were supporting the FIPs, which was primarily in the '90s, but actually many of the laws we enforced are at least partially based on the FIPs. We supported -- also supported, at least a certain time, legislation based on it. So it presumes legislation and self-regulation based on these FIPs. There's also the other approach that has dominated the FTC's thinking is the harm-based approach. And that is the -- focuses on the enforcement of existing laws based on an assessment of tangible harms. With the goal of reducing or stopping those tangible harms. And in think about the issues as go forward, we obviously also want to look at other models, not just the two models that have dominated the FTC's thinking. There's the EU-data directive, there's a more traditional FIPs model, which is actually something that DHS has been implementing recently, there's APEC privacy framework, and there's the EU/US Safe Harbor and Safe Harbors in general that need to be considered in at least self-regulatory approaches. So that's just providing a little background for our panel, and so let's go at it. I'd like to talk first about the fair information practices, which is really the grounding of a lot of privacy thinking in law and kind of give an overview of its limits and its benefits and maybe ask Fred Cate to do that.

>> Fred Cate: Thank you very much, and thank you for the opportunity to be here. Frankly, the sort of notice and choice model has come under such attack all day long, I almost feel guilty adding

to it at this point. But I'll overcome that. I think we could really, you know, maybe focus on three areas of criticism. One is that we've tended, I think, in the U.S., although I think it's frankly almost equally true in Europe, so I wouldn't limit myself to the U.S., to reduce a broad variety of FIPs down to far fewer. And, you know, realistically I think for many companies, it's really come to focus on notice and choice as being the two that has been the greatest focus on. And, frankly, I think the commission has put a great deal of emphasis on notice and choice. So to start with, we have the problem that we're not using the full FIPs approach where, you know, we cabined it down to small. And in some ways, I mean, this really goes back. It's been a U.S. view of privacy. I mean, ever since Alan Westin wrote "Privacy and Freedom" and said privacy is the right of individuals to control uses of data about themselves. So, you know, there's a long, rich heritage to this. It's just a very narrow view towards privacy especially today. I think a second problem with this is that it, you know, it hasn't worked terribly well in practice and there's lots of reasons for that. People don't read the notices. They don't understand the notices. They're not equipped to make choices. They don't care when it comes time to actually make the choice. They become like those click through screen, you know, do you want to download the software, yes, no. You click yes, you get it. You click no, you don't. So it's not really a choice, anyway. It's really just an illusion of choice. You know, because of the commission's approach and also states to treating notices as legal contracts, notices have gotten more and more cumbersome and complicated and detailed and, therefore, less and less intelligible to average consumers. So there are lots of examples. I don't think I need to belabor this. Other people have made this point quite well today. And then the third, I guess which I would point to is forgetting that consent or notice and choice are only tools, but they really shouldn't be the goals of privacy protection. You know, if you said to someone "Why do you want your privacy protected?" There aren't many people, and certainly outside of this room, there probably aren't any people who would say "Because I want my control enhanced." They want privacy protected so that they won't be harmed, they won't be injured. They won't be affected in a certain way or an unexpected way. It may not be a tangible harm, but I think few would say the goal for them of privacy protection is that their choice will be enhanced. Rather, they want their data used in predictable and less harmful ways. And maybe another example of that is look at the all the things we exempt from the choice model. So you look at a law like Graham-Leach-Bliley which effectively gives consumers on choice to opt out of the transfer of information to third parties for certain limited marketing purposes, the entire law otherwise leaves everybody

absolutely free to do what they want with data, provided they have a notice. And that just seems the ultimate in nonprivacy protection dressed up as privacy protection. Let me stop there.

>> Jessica Rich: Well, perhaps then we should roll back and talk about the FIPs as the model exists elsewhere that's not so limited to notice and choice. And what benefits that approach brings, and I'll ask Marc Rotenberg to launch that and maybe Evan to follow-up after Marc.

>> Marc Rotenberg: Okay. Well, thank you, Jessica. I also want to thank the FTC for putting together this very important event. I do want to mention, though, I think it was unfair to charge us for coffee. You know, there's a lot of TARP money out there. In fact, \$200 billion more than they thought yesterday and maybe some of that for future FTC privacy roundtables could go for coffee fund.

>> Jessica Rich: Next time you testify, if you could work that in.

>> Marc Rotenberg: I will, in fact. No, no, I think the FTC needs coffee money. But let's just think for a moment. I think we took this terrible detour on privacy protection in the United States that began roughly ten years ago where we looked at fair information practices, and we knew what they were because they came from the U.S. The most famous example of the establishment of fair information practices turned out to be the European Privacy Law, the EU directive, but the EU directive was based around a set of principles that were developed in the United States in the early 1970s where people began to think about the long-term consequences of automating personal information. And they had a lot of very good insights. They didn't say, for example, "Oh, we're terribly afraid of privacy, therefore, we should prohibit the automation of personal information." They said, "We need a regulatory framework that makes it possible for to us make use of this new technology and safeguard privacy." That was the starting point how people thought about fair information practices. And they said, therefore, we're going establish a set of ongoing obligations for organizations that choose to collect and use personal information. And if they choose to collect personal information in an automated environment, these obligations are going to include things like record accuracy and update, use limitation, no secret databases and all those things, and we will give individuals rights. They'll get to know about the collection use of their personal data.

And this regulatory scheme is purposely asymmetric, because it recognizes that when you transfer your data to an organization, the organization now has control of a little bit of your life, right? Some private details about you. And you have some right, I think, to expect that you're going to be able to exercise some control over that. That essential understanding of the purpose of fair information practices, which you will find, by the way, in most U.S. Privacy laws as well as the EU Directive was essentially ignored, papered over, tossed in the back closet, thrown over the ship with concrete attached around the legs to construct this new model of notice and choice to enable self-regulation. And notice and choice was based on this wonderful myth, the myth was that if we gave consumers enough information about how their data was going to be used, they would begin to exercise market force to encourage companies to adopt better privacy practices. It exists, not as a pared down version or as a partial of course of fair information practices, but actually in opposition to fair information practices. It's a completely different approach. And we've run this experiment for ten years. And I listened to the people on the earlier panels talk about the need for experiment. Well, I believe in experiment. I think experiment is a wonderful thing. But is there anybody today, ten years later, who believes that this approach to privacy protection works? I don't think so. I honestly don't. So I think what we need to do is recapture the essence of fair information practices. And I think if we do this, some marvelous things will start to happen. Because one of the other lessons we've learned in the last ten years is that where you have enforceable privacy regulations, businesses get very clever. And technologists get very clever, and they come up with ways to deliver products and services that don't require the collection of so much personal data. They find innovative ways to enable payment schemes and viewing everything else online that doesn't put such a heavy tax on the collection and use of personal data. So I think if we get back to that point, a lot of these other problems that we're having today with, you know, privacy and new technologies actually become easier to solve.

>> Jessica Rich: Let me just, before I go to Evan, let me ask you though, I understand, you know, some of the concepts like data minimization and data retention policies, obviously that goes beyond a notice and choice type regime. But when you're talking about no secret databases, providing access to consumers, transparency, isn't it -- what are alternatives besides notice concrete way to implement those things and a way that would be enforceable by a regulator?

>> Marc Rotenberg: Well, look, I mean, 25 years ago I wrote a bunch of laws that incorporated all those elements. You know, data destruction is right there in the video privacy protection act of 2711 -- I'm sorry, that's the Section, Title 18. But the year is 1997, right? We had data destruction, we had minimization, we had use limitations. I mean, all that stuff -- the way you write a privacy law is by looking at the list of fair information practices and trying to figure out, you know, how many you can incorporate into a statute. That's the way the privacy guidelines were done in the '84 Cable act, it's not the way it was done in Graham-Leach-Blyle. And, you know, I mean, I joke with people the wonderful thing about privacy with Graham-Leach-Blyle is you get all those paper notices, you can tape them over your windows and you've got a little more privacy in your home, but that's not the way the law was supposed to work, right?

>> Jessica Rich: But I'm saying, and maybe somebody can help me here, that to a certain extent, statements which are principles like no secret databases and providing consumers access and must be transparent, for many people, inevitably leads to notice. And we need, you know, if there's different ways to do that, other than notice and other than some of the creative things we're trying to do in behavioral advertising with Nikon and all of that, we should talk about that. Evan?

>> Evan Hendricks: Well, I think that that's a good place to start because when they first started talking about fair information practices in 1973, the first rule is there should nobody secret databases, and we've coming full circle because in the online environment, that's what we're doing. And there are lots -- and the difference is it might not be to your identifier, though that is ultimately the goal, your actual personal identifiers, but if it's tied to your IP address or your device it still can identify an individual user. So I think the answer is that you've put the fair information practice principles into law and make them enforceable. And it's good that -- in a way I agree with Marc that we took an unfortunate turn away from the full set of fair information practice principles. But now it's good news because the FTC has tried every other way. They tried FIPs, they tried notice and choice. It didn't work. We saw in the Graham-Leach-Blyle notices when you don't have full fair information practices, that didn't work. It ended up generating more confusion and not protecting privacy. We've certain certainly voluntary efforts, like the IRSG principles. You've tried every other way. So what are we specifically talking about? I think we're talking about -- we're talking about fair information practice principles, you're talking about not just -- you know,

everyone thinks about this is government regulation. Yes, you're putting duties on organizations if they collect personal information, but you're also giving rights to individuals. And the thing is, if you're an organization and you're collecting information, the online world to connect someone to their device or their individual identifiers, you have to create a right of access. And you can do that with a beacon to say, "This entity is collecting information about you, you can see what they got." That's a great starting point to start overcoming the secret database problem. I think that's where we have to start. I think you've heard a theme all day long from people who were part of a coalition, the privacy coalition, working with Jeff Chester, Pam Dixon, Susan Grant -- all said we'd like to see based on our best law in terms of fair information practices is the fair credit reporting act. And we're not talking about credit reports, but those principles of access to your information, correcting it when it's wrong, data use limitation and purpose specification -- is this only for advertising? Make it enforceable that it can only be used for advertising. Because if it's only for advertising, there's certainly less chance of harm than what we're seeing coming out of the reports today of Sprint providing 8 million data points to a government site. You know, information professional knows that information's collected, they will come to get one way or another whether it's the government, whether it's the divorce lawyer, other civil attorneys. And I think in closing, you have security where the FTC has done a good job by using privacy policies to pin security on companies, but the other thing is enforcement. I think whenever you're talking about something where you're collecting information on hundreds of millions of individuals, individuals have to be able to enforce their own rights. And in the fair credit reporting act, we have a private right of action and you have attorney's fees, and that's appropriate in that context and I think we have to look very hard at that because I don't see any way where -- no government agency would ever be big enough, and nor would we want it to be, to enforce rights for that many individuals. But we also have other models, too. The national labor relations board is a way where people can go to have a government agency investigate for them and see if their rights have been violated, and we talked about how Tim Muris and Howard Beales brought us the harm test, but they really became folk heroes when they created the do not call list. The do not call list made an -- it was something that was ten years overdue, and it brought an easy way for individuals to enforce their rights under a ten-year old law, and people didn't really have an enforceable way of enforcing those rights until they created that. So that's another model that we need look at. And so, all those principles are

there. I think we've tried everything else. The chickens have come home to roost, and now it's time to do the right thing. Thank you.

>> Jessica Rich: Okay. Let's bring -- Marc mentioned the international, and it's highly relevant to what we're talking about. So Michael, maybe you could talk about the common principles in the international framework. And they're gonna be a little bit different, but that you're working with OECD, APEC, whatever you want to talk about that could inform our work here.

>> Michael Donohue: Thank you, Jessica. It's really quite simple in the international environment, as I'll show you. This is a chart prepared by our colleagues in the Spanish DPA in advance of a project that they've been working to develop yet another new international standard. And actually, it does look complicated. But really it's simple, because what you don't see are too many white spaces. That's simple because it means that most of the different international instruments that are out there do reflect the same basic fair information practices, although obviously the way they've been implemented in national legislation differs. But to take a very hurried tour through some of those, I'll start naturally at the OECD, where in 1980, we developed a set of guidelines that have -- so far, we think have stood the test of time. At the same time, many people were running back and forth between Paris and Strasburg to go to the council of Europe to develop convention number 108, which has many of the same basic principles, although it's a binding convention rather than guidelines as we have at the OECD. So those were, sort of, the first generation of principles. The OECD ones are not so familiar in terms of the way in which they read now, although the underlying content is similar. The first is collection limitation. I won't go through what each of them mean, but data quality, purpose specification, use limitation, security safeguards, which we have heard a lot about, openness, individual participation, and accountability. The guidelines also have a section covering transporter data flows, as well as unfair discrimination which don't get very much attention, but which are there, as well. Now there, of course, have been other international instruments that have come into place since then. The UN has a set of guidelines dealing with privacy. We've already heard about the 1995 privacy directive from the European Union. And some of the principles that you don't see articulated as such in the OECD that come from those instruments include a notion of proportionality, the protection for sensitive information, and independent supervision. So those are some other principles that are out there in the international

space. More recently, of course, APEC worked to develop its own privacy framework which is very much modeled on the OECD, but also has this focus on harm which is not present in the same way at the OECD. And finally, our colleagues in the data protection community have come up with a standard release just last month where they're trying to show the feasibility of getting real international agreement on a set of principles. Most of them would be recognizable from the design to pull together the various instruments there. There are some new things in there in terms of what they're calling proactive measures, which focuses on issues like privacy impact assessments, codes of practice, educational awareness and other kinds of internal governance mechanisms. So that's sort of a novelty in some respects for an international standard and maybe -- well, I should say one last thing is that we've done some number crunching at the OECD to realize that the guidelines are turning 30 next year. So we're going to be celebrating that anniversary, but also taking a hard look at some of the changes many of which have been described over the course of this day in preparing a report that will then feed an actual review of the guidelines themselves. So I very much hope that we can take advantage of the insights that are being gathered here, elsewhere in Europe as well and the European Commission has begun a consultation on some of these very same issues to look at how best to address privacy going forward. Thank you.

>> Jessica Rich: Thank you. Barb, so Michael's talking about all these efforts to develop an international standard. How has the increase -- first of all, the increase in multinational companies, and the increase in trans-border data flows for reasons of cost and other reasons, how has that changed company's view of a need for the international standard?

>> Barbara Lawler: Companies are really -- whoa, I'll back up. Where companies are really interested and concerned about trans-border data flows is because of, as we've talked about, the multi-dimensional nature of data. Data moves around the globe in an instant. If we actually use the example of a data center, many, many multinationals are consolidating data center and large processing operations in -- let's say in Texas. So let's say your major data center is in Texas, but there isn't a responsible multinational company that doesn't have at least one failsafe or fall over data center, if not two, and more than likely that would be in another country location. When we think about the idea that data is in one place, i.e. the main data center, but also has backups in the backup data center, what you really have is a situation where the data is in one place and in many

places at the same time. It may be unsettling to think about the idea that in some ways data is never really at rest. So when you think about the idea that data is in one place and in many places around the movement and management, just simply of data centers and then the potential for different conflicting overlapping -- nice matrix. I really appreciate you sharing that -- most companies have to build their own specific matrix that adapts and looks at what are the state requirements, what are the federal requirements, what are all the different country requirements and try and make some actual common sense of the requirements. And at the end of the day, it's incredibly complicated, time consuming, inefficient to do that when your customers are asking and demanding full-time 24/7 availability. So international standards, not five international standards which we kind of have now, but some sort of harmonized standard is really something that would not only benefit business but ultimately provide more consistent experience for consumers.

>> Jessica Rich: Okay, so we'll come back to the fair information practices, but let's move over and talk a bit about the harm-based model, and we have the perfect person to talk about it. Howard Beales. So why don't you tell us what it is and why you -- and why you -- well, you talk. Howard's my former boss. I'm not going to tell him exactly how to say it.

>> Howard Beales: Well, thanks, Jessica. And thanks for the opportunity to be here today. Let me begin by pushing back a little about your description of what the model is.

>> Jessica Rich: I knew you were going to do that.

>> Howard Beales: I don't think there is anything in the harm-based approach to thinking about privacy that says we can only -- it can only deal with tangible harms. If you think about the very first case we brought under the consequences-based approach, it was a case against Eli Lilly that involved the release of e-mail addresses of Prozac users. A lot of them .gov addresses. And there's no tangible economic harm that goes with that as far as we know or knew or still know. There is a subjective preference on the part of many people that that kind of information shouldn't be out there and that, it seems to me, is what that case is about. Subjective values are important in a lot of places. They are important guides to what we do in the economy in products and services and privacy is no different about that. What's important about subjective preferences, though, is you

got think about them a little bit differently, and you got to be sure that it's a real preference expressed in the marketplace. Think about an analogy for a clear subjective preference, which is products that are kosher. A lot of people care. Completely subjective -- I mean, yeah, there's a difference, but it's a subjective preference not one that's got tangible economic or health and safety consequences. It makes perfect sense to protect that preference. For -- if you sell somebody something and say it's kosher, it better be. It makes very little sense to say that because some people have a preference for kosher, all products should be kosher. And that's sort of the leap that's happening in the privacy debate. We're saying there's some people out there who really care about privacy, no doubt there are, and, therefore, all of the information products and services have to satisfy those preferences for everyone. That's a big leap, and a very different approach to thinking about the subjective value than what I think makes sense. Second thing about the consequences-based approach is I think it makes you think about what you're trying to accomplish. That I think is an extremely useful -- an extremely big part of its value. And do not call is maybe a good example. You know, if you think do not call in the conventional privacy approach, well, you know, this is a secrecy problem. Hide your phone number. Don't let anybody call you and you won't have any problems. If doesn't work that way. If you think about it as what we're trying to avoid is a phone call I don't want, it points in a different place as to how you address the problem. Part of the reason it's important to be clear about what is the harm, is what is the harm is going to affect the most effective and the least cost ways to avoid the harm. And so unless you can be, unless you can articulate the particular problem that you're trying to fix, what it is you're trying to protect in this subjective preference or objective, it's going to be very difficult to come up with a solution that works to address that problem. I mean, one of the examples of that that's been talked about a lot today I think is this first party/third party distinction. Well, what exactly are we trying to protect there? Is the problem the sharing of the information? Or is the problem the existence of the information? That there is a database that includes this information? If the problem is existence and the potential for access by hackers or governments or whoever else, the first party/third party distinction doesn't make any difference at all. It simply doesn't affect the consequence. If the problem is sharing, then -- well, let's focus, why is the sharing a problem in that particular context? Where the information is going to be shared lots of places along the way of doing things that we all think ought to happen, like the transaction actually ought to get processed.

>> Jessica Rich: Howard, can I ask you, in the harm-based model, who decides? Does the harm based model provide clarity to companies as to what their duties and obligations are? Is it the regulator that decides after harm has occurred? What is the guidance that you put out to companies trying to protect privacy?

>> Howard Beales: Well, it seems to me that the fundamental guidance that you put out is don't use information in ways that are going to be damaging to your customers or damaging to the people that are the subject of that information. I mean, I don't think it's that hard a principle to follow. It's not substantially harder than don't write deceptive advertising. Yeah, it lacks a certain specificity. It doesn't tell you what's the type size for a particular disclosure, but I think it's pretty clear what people are supposed to be doing. Don't use information in ways that's going to be damaging to your customers.

>> Jessica Rich: And if as in Eli Lilly, they didn't have a deceptive statement. I mean, that was a deception case. Would that -- in the absence of new laws to make clear what's harmful, would the FTC have brought an unfairness case to say that was illegal?

>> Howard Beales: Well, as you know -- you know, my great regret was you didn't find the unfairness case on information security until I was out the door.

>> Jessica Rich: We found it, it was just hard -- we were investigating it.

>> Howard Beales: Yeah, I think you can bring that case as unfairness. If, you know, if there's really something going on there, but you need to be, you need consumer behavior in the marketplace, choices consumers really made or tried to make and not survey data that say some people care at best.

>> Jessica Rich: Marc, you're knitting your brow. So I think you need to say something.

>> Marc Rotenberg: Boy, Howard, I miss you. So let's just think about the problem with trying to approach, you know, tangible harm to privacy. If there is a tangible harm, you know, financial,

which is something that courts like, it's almost by definition not the privacy harm, in other words, when we're talking about privacy or the loss of privacy, the interception of a telephone conversation, the disclosure of someone's HIV status, I can't imagine how we begin to assign a dollar value in the abstract. We can say, "Oh the person lost the job." Well, then we sit down and sort of figure out what the value of the job was, but that's somehow apart from the harm that we think of as the privacy harm. And so the answer to this question, again, and I mean you have to go back a little bit, but it's there. Is that privacy laws have traditionally set out stipulated damages. And they've said, you know, we don't know what the exact amount is, for example, when someone receives, you know, an unwanted telephone solicitation after they've already told the company they don't want the unwanted telephone solicitation, but we'll just say \$500 and that's exactly what congress did in 1991, and it led to some enforcement action and eventually led to your do not call list. But that's a very concrete way of trying to understand how we create effective mechanisms for enforcement. So I mean and I appreciate it. It's not always been quite so literal and certainly in the Prozac case, it wasn't. But I want to put one other issue on the table, because if we don't get to it today, I think that would be unfortunate. The construction of privacy law in the United States is not just about isolated harm to individuals, we tend to talk about it that way. We tend to talk about a person's personal interest in their own data and the discussion gets very kind of, you know, individualistic. But the origins of U.S. Privacy law actually start in a very different place. The big concern in the United States in the mid 1960s was the creation of a large centralized database. People said they did not want the government to have a big database on everything that they were doing. Right, tax records and pension accounts and everything else. So what eventually emerged was a structure of privacy law for the government that tried to compartmentalize all of these different activities to avoid a centralized system of profiling and tracking of individuals. Now I think it's pretty reasonable to begin the discussion at this point as we think about the role of privacy law in addition to the impact on individuals. How do we feel about very large corporations that are creating exactly the same type of databases that break down these compartments in our private lives that build these detailed profiles, that are almost exactly the reason that we develop privacy laws, you know, 40 years ago? I would actually be interested in your view, because I suspect with respect to the government activities, you would agree that we try to keep these partitions in place.

>> Howard Beales: Well, and that it seems to me is exactly the distinction that was made in those laws is between government databases and private ones. I mean there was, you know, it's not like there wasn't data matching going on at the time on a pretty extensive basis on offline data with, you know, with catalog data exchanges and you know, whole host of other things. It wasn't -- this isn't a new problem. It isn't, you know, this isn't something that's just emerged with the internet. It's something that's gotten new attention, but it's the same beast and that was the decision that was made. We want to treat the government differently. I do think that makes a whole lot of sense to treat the government differently. And some of the things like notice that are really important when it's the government because you want somebody to be able to find out that the government is doing this with the information and be able to say that that's a problem, are much less valuable when you think about an individual consumer finding out about how the data is going to be used. It's not the same value that's being advanced by the provision of notice in those two cases.

>> Jessica Rich: Can I just ask, let's see, Fred, to comment on perhaps, to expand on this notion of uses of data that may not be covered by the harm-based model? Because I don't think we've given out specific examples of that, and I know you've written on this, Fred.

>> Fred Cate: Well, thank you. I want to start by echoing Howard's point, which probably makes Howard now incredibly nervous. But, once you say harms don't have to be limited to tangible economic or physical harms, you then have a much broader approach under this harms or, Howard, I think as you used the term consequences-based approach. So that you can identify, there are certain consequences, there are certain results which we are going to say would trigger regulation. And just to tie this back to the earlier discussion, you would in those areas potentially say choice is not an option. There's some harms which are simply so harmful, we don't give you the choice about them. So think about most consumer protection law. You walk in to buy a television, you can't consent to be defrauded in the store. The FTC doesn't offer you that option that you can consent to receive fraudulent advertising or false or deceptive advertising. So in some areas, not across the board -- I wouldn't suggest that for a moment. But in some areas, we could undoubtedly say there are just certain activities that really should be off the table or certain obligations that should attach irrespective of consent. I think security obligations would be a good example. There are also activities, which frankly, consent just doesn't seem relevant to. Not because the activities

should be expressly permitted or expressly prohibited, but consent just doesn't seem like a useful model. The example Barb gave, which I thought it was a terrific one, about backup of data, you know, currently under our approach to privacy policies, we would expect the company to describe this to the consumer. You know, we use a third party to backup our data. They may store the data some place else, here's how they do it, and then we would ask the consumer to consent or engage in the transaction knowing this. I don't think there's a person on Earth, other than maybe Marc who would actually care about the details of the backup data. What we want to know is that the backing up of the data is done pursuant to certain substantive obligations, and if you don't meet those, there's enforcement of those. Not a description of the, you know, type of backup tape you use and then do you consent to that or not? If it's cobal that's okay, but if it's not, you want something else.

>> Marc Rotenberg: Fred, if it's cobal, you don't want to consent, trust me.

>> Fred Cate: Yes, exactly. Thank you. I rely on Marc for all my my purchasing decisions in the technology world. And again, if I can just make one last point and then I will shut up, which is -- to my mind, it's the structure and the process that matters, frankly, more than the specifics. In other words, we might disagree on what goes in what bucket and there would be a lot of room for disagreement, but if you have a rule-making procedure or some process by which you would debate that. You could do something just like this, but in a more focused way -- the point that matters is that there is agreement that there needs to be some area that's outside of consent and that there is a process by which to identify that and frankly to keep updating it, to keep reviewing it, so that you don't lock in something in, you know, one law that's there forever.

>> Jessica Rich: Well, that's right and that's one of the things that -- I guess the harm-based model still leaves you with that who decides, because it's going to be the FTC enforcing the FTC act unless you have some structure in place, especially if you broaden the concept of harm and it becomes everything. But let me, before we --

>> Howard Beales: It doesn't become everything.

>> Jessica Rich: Okay, we're putting words in Howard's mouth. Now it's everything out there. Before we get to sort of, I think Fred has forecast that, you know, there's some new possibilities for a model we can talk about where we take certain things off the table, as was said in the prior panel. But before we get there, I think we want to talk a little bit about self-regulation because there's been a lot of discussion today about that self-regulation hasn't worked. It's been ten years, et cetera. We do have a lot of experience with self-regulation, we've got two people here -- Ira and Chuck who have -- will be able to tell us a lot about self-regulation. I want to ask Ira, just overall, I know you just wrote a big article about it. How effective have self-regulatory approaches been in the current environment, and does self-regulation need to be backed up to be meaningful, does it need to be backed up by government regulation, and otherwise how do you deal with people who don't join?

>> Ira Rubinstein: Thanks, Jessica. Let me make three points about self-regulation, the first is it's that been widely criticized not only today but over the years for weak standards, for ineffective enforcement and in adequate remedies. But at the same time, I think it's probably a permanent aspect of the U.S. Regulatory framework and there are a couple of reasons for that. One is that U.S. Internet policy has always been very friendly to ecommerce which tends to view regulation as costly, as inefficient, or it's harming innovation and I don't think that perspective has really changed. The second is that, I think we saw this today, too, that when there's uncertainty over what the best policy is or impact of regulation might be, for example in the online behavioral advertising area, self-regulation seems attractive because it allows experimentation and doesn't freeze laws once and for all. But that said, I think it's important to see that, and this is my second point, that self-regulation is not monolithic. We're most familiar with largely voluntary efforts at self-regulation such as from the DMA, the OPA and then more recently the NAI. But I think it's better understood on a continuum based on the degree of government intervention and there are other models available. So one is that the government sets substantive standards but leaves enforcement to industry and the model I have in mind for that is the EU-U.S. Safe Harbor Agreement which defines very clearly what the privacy principles are but relies on self-regulatory mechanisms for enforcement purposes. Another is the Statutory Safe Harbors under the Children's Online Privacy Act, COPA, where the government defines clearly not only the substantive standards but also how to handle oversight and enforcement. And I've done a case study of these three models and come to the conclusion that the Statutory Safe Harbor really responds best to the typical criticisms of self-

regulation but also does best against a variety of criteria, completeness of coverage of the substantive privacy standards, overcoming free rider problem which you eluded to how do we get outliers to join oversight and enforcement and transparency as well. So one recommendation I would have is that if congress enacts a new privacy legislation, it should continue to encourage self-regulation via a statutory safe harbor, but in doing so, it shouldn't just regulate the COPA experience because that had flaws too. And the main flaws were, first of all that very few companies signed up, there are under 100 companies who have taken advantage of the COPA's National Safe Harbor and I think this is largely because firms view the benefits as too limited and that's partly due to the fact that the requirements are simply too inflexible and to address that, I would suggest that the privacy community could learn a lot from the experience in the environmental field where they've been wrestling with similar regulatory issues for much, much longer than in privacy. And I'll just close these comments with two points I want to emphasize. The first is the idea of privacy covenants by which I mean covenanting approach where the government and industry sit down together and negotiate a regulatory agreement often under a threat of stronger harsher regulation if an agreement's not reached, and then typically with other stakeholders at the table. And Pam Dixon mentioned this earlier when she talk and the friction or tension that arises when you have multiple stakeholders and more meaningful compromises can emerge from that process. And this may sound a bit farfetched, for example, if FTC were to try to persuade NAI to include public advocacy groups at the table when they do a next round of codes of conduct, so privacy principles, but there is a model for it in the recent global network initiative where under both threat of regulation and very severely negative news coverage, Google, Microsoft, Yahoo! sat down with academics, with privacy and human rights groups to talk about global principles for addressing privacy and anti-censorship rules under the experience of cooperating with the Chinese government. So it's not unprecedented by any means and it's been tried quite a bit in the environmental areas as well. The final point I want to make is that it would also be interesting to experiment with regulations that differentiate between good and bad actors. So we've heard a lot of concern about whether there will be a one size fits all approach if regulation is followed. But I think the way to avoid that is to build in criteria that treat different performers differently. That of course raises the question of how to measure that, but we'll put that aside for now. And then to adjust the set of carrots and sticks that are used as incentives to motivate more firms to fall into the good performer category. And one way to do that might be to consider a

traditional use of safe harbors, which is an exemption of liability, so if legislation was to include a private right of action or liquidated damages, that might be -- firms that fall into this defined category of having either undertaken a covenanting approach and won approval from other advocates for their approach would be exempted from that liability and it would be limited to firms that don't participate in that well defined safe harbor or other measures for good performance could be devised.

>> Jessica Rich: Thanks. Now, Chuck, Ira just said that self-regulation works best, he recommends that it should be supported by regulation, are you going to take that?

>> Charles Curran: I'll take that for \$200. First off, to be clear, there's no unitary model of self-regulation for all online advertising. But I think it is important -- there's an idea in Ira's article that he talks about in the covenanting process of the advantages of flexibility of having performance objectives. What we've seen in the context of OVA specifically is I think the dialogue with advocates with the commission through town halls like this, helps us in effect formulate a performance objective. For example, transparency, it's been called out repeatedly that there's insufficient information about the nature and substance of the categories used for OPA. So the industry responds to this, objective has been with some degree of differentiation based upon the company specific technologies to serve up and you see it with Google's ad management platform, you see it with Yahoo!'s iteration on that same concept with even more bells and whistles and you see it even with smaller companies like BlueKai. So you have companies responding relative to their own technology but trying to satisfy the performance objective of transparency. Same thing for the persistence of opt out cookies. Critique was you're not providing a stable enough platform for the browser to remember these preferences. So here, too, some industry advances, some advocate, Chris Sygoian's here who's developed a pro bono code, and we at a NAI and in industry are now in effect bringing to market the same concept with our own in effect flavors to recognize what we think is the best way to address consumer needs. And finally, for enhanced notice, which is the big kahuna of -- issues that people want addressed in the context of OVA and there, too, we have a complex ecosystem involving advertiser, publishers, ad networks, we obviously need the consistency of a common iconography, common messaging for consumers to understand, but at the same time, we need some flexibility to implement the backhand so that companies participating in a

disclosure ecosystem can express that information in different ways whether they'd like to put it in interstitial or on webpage to transmit the information. So I think overall, the ability through the self-regulatory process to address general principles rather than any particular technological mandate I think is really the core virtue of the system that we are trying to encourage.

>> Jessica Rich: But in the absence of any regulatory scheme, what do you do about people not joining? You know, consumer thinks it goes to NAI and the consumer opts out and then there's all these people not -- who aren't members.

>> Charles Curran: So I think here there are two different problems, one is the free rider problem and the other is the edge rider problem. If you move to a system, certainly the NAI has been in existence for some time, but in the past year, with the in effect active participation of thousands of companies through their DMA, The IAB, we have much more of a platform of common ownership of the responsibilities of self-regulation and enforcement. And in that, I think that speaks to the issue of the free rider problem, the ability for companies to avoid the obligations in the work that they have to do to be part of the virtuous ecosystem. The edge rider problem I think becomes more front and center when you achieve that ecosystem-wide self-regulation and there as is typical with other problems online that the FTC has addressed, it's not as if there aren't -- there are remedies that address aggressive practices, material omissions, deception, existing tort law. There are often remedies, but it is also true and I think that the DMA and the IAB certainly bring the experience to this that once you have a generally ecosystem wide adoption of self-regulation, you do, in fact, have a system in place where the desire of the participating companies who are making the effort to name and shame and to identify and to in effect to create processes that relate to nonparticipating members and to call them out for their conduct and to investigate them and to refer them to you, so that's, I think, where we get to the solution for the edge rider.

>> Jessica Rich: I want to get to some of the new models that are been proposed so I'll get to you, Barb, in a minute but Evan, do you have a very brief comment on this issue of self-regulation.

>> Evan Hendricks: Yeah, I think there's another model that's out there that hasn't, we don't talk about much here because it's the Dutch Model. The Dutch Model was that you did, I think your

questions go out to fact if you don't have standards in place, what are the standards for whatever self-regulatory model is? In the Dutch Model, European country, they had the fair information practices in law and what they did to implement it, is they told the different, this is several years ago, they told the different sectors of the economy to come up with their own industry wide set of practices, how they were going to comply and they opened up a process so it wasn't just them talking to each, the public was involved. And so then, then they had to submit that to, in their case, the privacy or data protection commissioner and then ultimately it was hashed out and became a stamp of approval but the principles were set and the standard, the industry working with anybody else who was interested including advocacy groups worked out the code of practices and then it became enforceable code of practices, so I think that is something that has a lot of legs with what we need to do have real standards, we need to have enforceability and we also need to have flexibility given the environments we're talking about.

>> Jessica Rich: That's a very good point. Barb, do you want to talk us now about, I know that --

>> Barbara Lawler: Business forum for consumer privacy.

>> Jessica Rich: The business forum has come up with a use based model that it's proposing and it would be great if you could briefly describe that so we have a chance to talk about it.

>> Barbara Lawler: Yeah, sure. What I actually wanted to comment on before I get into the use and obligation centered model is I wanted to build on something that Ira mentioned a moment ago to make sure we're accurately capturing the self-regulatory environment, until one of the areas we haven't talked much about are privacy seal programs. When we think about fair information practices, the traditional fair information practices, and programs like trustee programs, online when they existed, those self-regulatory programs in many ways did a better job of applying and do a better job of applying fair information practices than perhaps some actual regulations do today. And I wanted to capture that before moving into the use and obligations model. The purpose of the use and obligations model is really a culmination of a lot of thinking and effort over a number of businesses and organizations over the last three or four years to really look at how do fair information principles, fair information practices work in the 21st century with the digital economy

so what the model really does is it focuses on the idea that use rather than collection driven by notice and choice that use is the driver for the other fair information practices. Let me talk about what that means. As we think about traditional privacy models today, we spend a lot of time talking about that. We've talked a lot about the fail you, the limitations of notice and choice and the excessive focus on notice and choice. In a notice and choice collection based model, you have to know where that information began, where it started, to understand what obligations might go with it. In a use centered approach, it's different because it says through the lifecycle of the information from the point it's collected through the different organizations that have some responsibility and accountability to handle that, obligations carry throughout that and that's driven by use. The use and obligations model if you read through the paper and we have some nice graphics that talk about different types of major use categories, focused on fulfillment, on internal operations around risk management, we talked about risk management actually in the data broker context, fraud prevention and also security and legal obligations. And what we do in the model is actually outline how notice, choice, access and correction as well as enforcement and oversight concepts fit in but are driven based on the different categories of use. So let me stop there.

>> Jessica Rich: Okay. And if you focus on use and of course the collection use debate has been in play for a long time, but what do you do about the -- we talked earlier, two of our examples, I think in the first panel where with the AOL breach and Google Subpoena, how did use affect data sitting there and then ultimately landing in the wrong hands?

>> Barbara Lawler: One of the benefits for organizations in applying a use and obligations model, what it actually does is, if handled right, forces the organization to sit down and talk about, think about what information they are collecting, how they are using it and to frankly have a data strategy and information management plan. So that ideally, a situation like AOL and the release of research information, there might have been a different set of criteria, a different set of framework that might be driven that. When we look at enforcement, a couple of things that we think are important in the use and obligations model is the current environment that we have around fair information practices really places a lot of burden on the consumer to police the market. And we think that organizations, responsible organizations have an accountability and responsibility to be more responsible and to actually relieve consumers of the burden while at the same time providing

transparency so that individuals can have more informed decisions, more nuanced decisions but that organizations frankly are being more sophisticated, more thoughtful, more comprehensive in their approach, because consumers should expect a safe marketplace. They shouldn't be the ones to police the marketplace.

>> Jessica Rich: One of the things that is intriguing about the use based approach is that it does attempt to identify categories of uses that perhaps should be subject to lesser restrictions and are consistent with consumer expectations such as fulfillment, security, I think you have different names for it but you know, maintenance of the website, et cetera. Is, we talked in an earlier panel about simplifying things for -- we talked in every panel about simplifying things for consumers and we'll keep talking about that, but is it possible to and this is for anyone because I think this goes to potentially new different models we might think of, is it possible to identify, to get things off the table for consumers by identifying uses that we think are entirely consistent with consumer expectations and don't need to be a privacy policy and don't need to be susceptible to choice. By the same token, uses that are -- could we agree on uses that are so harmful that everyone agrees they should be prohibited and thereby boiled down to a much smaller category of -- Fred was talking about this, a much smaller category of uses or collections, things that consumers have choice about so that it's manageable? Would that be -- could we work with something like that? Marc?

>> Marc Rotenberg: I'll answer the question but I want to first say that I absolutely agree with what Barb just said, that consumers should not be expected to police the marketplace, I think that's one of the best criticisms of self-regulation, that there has to be some independent entity, let's -- you know maybe like the federal trade commission that would have the responsibility of policing the marketplace. Now with respect to the use approach, yes, it's one of the elements. In fact if you read a privacy law it will typically have an exception to a limitation on disclosure that says that a disclosure that's necessary or incident to the provision of the service is fine. If I want to you ship something to me, you're going to ask me for my shipping address and you're going to disclose it to the shipper so I can get from you what I wanted. I mean --

>> Jessica Rich: So long as the shipper doesn't use it for any other purpose.

>> Marc Rotenberg: Yes, but in fact a lot of these privacy norms reflect common sense understandings about how people interact with businesses. I think a lot of Joe's work is fascinating because what it tends to reveal is that in fact that most people have expectation of privacy and most assume that those expectations are respected. The actual story, of course, is very different. But to also make this very important point, Michael's chart which lists all these different international privacy frameworks still settle around eight to ten main fair information practices. They actually don't vary that much, which is a remarkable fact about the modern information economy and that is that if you look at how different countries that are participating in this information economy have understood privacy protection, whether on a country basis or regional basis, they've come to surprisingly similar conclusions, which I think is a very important insight for the FTC. The last brief comment I want to make is to the extent governments are not engaging in some of the most pressing privacy issues that we have today, I actually think civil society at the recent meeting of the privacy commissioners in Spain issued a very important document. This is called the Madrid Privacy Declaration, which really identifies the current challenges to privacy protection where some of the gaps are and what governments need to do, so I think if you take Michael's chart with those eight to ten fair information practices that are fairly well known and you put next to it civil society's critique of what else needs to be done, you'll cover a surprising amount. So yes, it's part of it, but I think if you stop there, you know, we're back to having kind of a notice and choice approach to privacy protection.

>> Jessica Rich: But it seems clear --

>> Barbara Lawler: we're not stopping it.

>> Jessica Rich: It seems clear that there's certain consumer benefits like access and transparency and I know benefits is the wrong term, that do require an interface with the consumer. So apart from the things we can agree on, I think there's a lot of discussion about not collecting data you don't need and some of these other principles. Let's say those are all enacted, in terms of the interface with consumers what can we do to simplify that? So you know, I'm wondering if you take some of the categories and use base model, I think marketing is controversial, so they put that in the use base model, but Barb, the other ones are fulfillment, fraud prevention, subpoenas.

>> Barbara Lawler: Security and legal requirements.

>> Jessica Rich: Yeah, if you took those which I think are less controversial than the marketing and then what else is there? What are the uses --

>> Marc Rotenberg: But Jessica, this is not necessarily the right approach. And what I'm trying to suggest, and you know, an engineer I thought had a good insight in talking about privacy, he said you actually want less on the dashboard and more under the hood. And what he was saying is that you don't want to confuse consumers with a lot of complicated privacy choices and decisions, you want them to engage in whatever transaction the merchant is holding out which is good for the consumers and the merchant, right, with the privacy safeguards built in. And you see the problem with this approach.

>> Jessica Rich: Marc, I'm with you, I'm saying that assuming you have substantive protections, there's still going to be certain things, perhaps, that you can't agree on. Maybe we can agree on things that are okay maybe can agree on things that aren't okay, but there may be that middle ground, for example, marketing where there might be consumer choices and the question is can we narrow, can we narrow the areas where there will be consumer choices by perhaps having substantive rules about everything else and thereby not put so much burden on the consumer? Evan?

>> Evan Hendricks: I think Barb had mentioned fulfillment and what was the other one? Marketing? And then Pam Dixon talked earlier there about fraud prevention there's a dangerous loophole. But yeah, things like fulfillment, and even Marc mentioned that in his comments, the data is basically being used to complete a transaction, that's very consistent. And I think on the other side, we've talked about sensitive information that has been identified in different realms as things like your religion, your political affiliation, your health condition, financial condition, minority group, ethnicity, sexual preference, those are some of the categories that you look about taking off the table, which are not these days. But on the other hand, I think the answer is no. Ultimately for a national policy, I agree that the supreme court said that in 1988 and the reporters

committee case, which was the freedom of information act case that the meaning of privacy begins with the ability of the individual to maintain reasonable control over their personal information and in terms of the proper policy there is no substitute for a reasonable in standard. You have to have, if you go to a website because you want to see about a sports score and then you get floated in an ad about sports, is that such an unreasonable? I don't think it is. I don't think it's that big a deal. But if your elderly parent has a condition or you have a friend that has aids or something you go to an aids site but you're identified as someone who has aids and that's sold to an insurance company, I think most of us agree, that's unreasonable. And so for the larger picture, the answer is no. There has to be a reasonableness standard, there has to be that kind of flexibility in there. And I think that ultimately, too early, there has to be a mechanism that the individual can initiate enforcement of his own rights.

>> Jessica Rich: Okay, so we've talked about a bunch of different types of models that we could consider, assuming we're developing a new model. We've obviously we've talked about the notice and choice model. We talked about harm based, we've talked about the use based model. We've talked about the Dutch Model, which was based on self-regulation, we've obviously talked about more comprehensiveness FIPs of the sort that had been enacted in many places in the world and we talked about, Fred and I at least have talked about perhaps taking certain things off the table with substantive rules but perhaps leaving choice for other things. Any other models that we should just throw out there for exploration?

>> Marc Rotenberg: Yes. I mean the idea that you can have anonymous online transactions, right, which is actually a very powerful concept but the reality for most consumers, and I used to track these numbers, they're issued by the Department of Treasury. Up to about four or five years ago, the majority of transactions that consumers engaged in the United States were cash based. Right? If you got into a cab to come to this meeting, if you went across the street to buy lunch, if you went to get a newspaper, all of those transactions allowed you to purchase a product, someone to get paid and there was no disclosure of personal information. That was the majority default for most transactions. I think it's worth spending at least a little bit of time thinking about how we could recapture anonymous techniques. In some areas of our society, it turns out to be vital. For example, voting online and maintaining the secret ballot. You have to solve the problem of

protecting privacy to make the secret ballot work. So I think for the FTC to spend some time as a lot of other privacy agencies have around the world, on how to make provable anonymous transactions work, would be a very good model to pursue.

>> Jessica Rich: Is that a regulatory model or is it a technology-driven model?

>> Marc Rotenberg: It's both, actually. I mean it's an excellent question. And my view is that you get better technologies from a background of privacy regulation. In other words if you make it difficult for companies to collect and use personal data, they will come up with innovative solutions that are less dependent on the collection of personal data. And if you say we're really enthusiastic about companies that can make anonymous transactions work, I think the market will respond but it will take in leadership and the thing that will surprise people in this room is that a lot of privacy advocates are actually very strong supporters of technological innovation, we just want to see innovation that promotes privacy, right? Commerce is great, but let's also promote privacy.

>> Jessica Rich: And I guess we shouldn't forget other privacy enhancing technologies that could either be done in either a self-regulatory way or through incentives through regulation. Does everyone want to take 30 -- whoever's got their card up now, 30 seconds quickly so we can end semi on time. Oh, Howard put it down. Okay, Howard. Everyone quick.

>> J. Howard Beales, III: I just wanted to say about the taking some uses off the table thing, some uses don't have to have notice and choice about or consent about that that makes perfect sense. To me, the way to think about it though is not expectations. I mean I think consumers want most of the products they use, they want it to work. They don't have expectations about what goes on under the hood, if you will. And they shouldn't have to have expectations about what goes on under the hood. I mean we got to protect them from bad consequences but that really ought to be the focus.

>> Fred Cate: Jessica, just on the model point, I don't think you implied anything, but it seems like we should be clear, these models don't have to be mutually exclusive and so while I think notice and choice is to some extent exclusive of others of these models, it's really sort of overlaying them in a way that makes the most efficient, effective, appropriate protection. The other comment is you

used the word simplify and you scared me to death when you e-mailed that question you were going to ask about simplification. Because first of all I think, it's absolutely right it should be the goal to simplify the role of the consumer, the role of the individual on privacy protection. Privacy at its heart's remarkably complicated because information is so complicated. And therefore, I think we need to at least need to keep some sense that there are going to be a lot of different approaches in different sectors, different types we've already talked about the difference between public and private sectors distinguishing between good actors and bad actors, I think we are overall unlikely to simplify the role of the consumer makes great sense.

>> Jessica Rich: We'll have to leave simplification for the next roundtable, I didn't get there. Evan.

>> Evan Hendricks: I'm going to take 30 seconds please tell me when there's ten seconds left. I'm talking about a dynamic that's always happens and the FTC has considered this. In the 1990's they were afraid, there were two differentials to the internet business and therefore they didn't go with the strong privacy regime. If you look at who came to the workshop then, a lot of them don't exist anymore. And they got their way and had nothing to do with privacy.

>> Jessica Rich: But you came.

>> Evan Hendricks: Yes, that's right. They came with the IRS-G principles, there was a lot of difference to that sector of the economy, they went with the self-regulatory thing. Most of those people are not there anymore either, and it's happened over and over. So I think this time, I think history shows, we we've heard a lot of testimony earlier about how concerned the ad industry was that their ad rates are going down. Yes, it's a sector that's in huge transformation right now as is the industries that depend on it. But I don't think we should be bending over backwards or going the other way with our privacy policy and sacrificing protection for personal information based on these transformations going on in industry.

>> Jessica Rich: Okay, Barb.

>> Barbara Lawler: So to finalize the discussion on the use and obligations model, I want to encourage folks to actually download the paper, grab a copy and read it. The question was have we captured all the uses? We think we've captured all or virtually all of them but we actually encourage, welcome feedback, there's more work to do on the model. And I wanted to make sure I leave folks with the idea this is a use and obligation centered model built around all of the fair information practices, it's not the use only model.

>> Jessica Rich: Ira, last word. Quickly.

>> Ira Rubenstein: I just wanted to echo Fred's point that the models are not usually exclusive and also point out that with the statutory safe harbor approach you are forced to define what the FIPs are, but then as in the Dutch model the approved codes of conduct is where you experiment. So the use and obligations model might be such an experiment subject to FTC approval.

>> Jessica Rich: That's interesting. Okay! Well this has been a great panel. Thanks very much. We have some closing remarks by David Vladeck, our bureau director.

>> David Vladeck: Thank you, and I will get you out on time. You'll all be out of here by 6:00 because we're now down to the hard core. This has been a remarkable, exhilarating and in some respects exhausting day. It's the beginning of what we hope is an important dialogue on consumer privacy and we thank you all for coming. I want to begin, however, by thanking the FTC staff that made today possible. This is truly an all-star team, you've seen many of my colleagues up at the podium today with enormous amount of work went into organizing this conference. Please join me in thanking them. [applause] I also want to thank all of today's participants. We had very high expectations for this conference. But the dialogue today exceeded even our loftiest goals. I think all of us learned a great deal today, I certainly did. Who knew privacy had its own vocabulary, we learned about issues like boxing, script, ecosystems, edge riders and daisy chains, all very interesting concepts. But last but certainly not least, I want to thank each of you for coming today. We have very hard questions to answer here. The last panel, I think, as the predecessors exemplified just how difficult the questions we have to confront are. We will need your help in finding the right answers. We urge you all to help us as we move this process along, we look

forward to your comments, we look forward to your thoughts. So, let me just make some overarching conclusions about what we gained today and what questions face us in the future. We began today by discussing a wide variety of ways in which these important but powerful tracking tools bring benefits to consumers. But we also discussed the risk of possible misuse of information. Panelist pointed out that the benefits including free content, better search results and more relevant advertising. These are all consumer benefits but the panelists also mentioned real risks including the disclosure of information consumers believe is private. And the chilling effect that people -- on people who might modify their online behavior for fear of being tracked. These are real risks as well, we need to confront them. We also heard that the traditional distinction that has been drawn in privacy law between personal identifiable information and anonymous information may be a thing of the past. These observations raise questions about how to build in transparency, consumer control and accountability into the process without sacrificing the benefits. Our task is made even more urgent by the researchers who talked today that confirm our intuition that consumers do not really understand the data collection process. One panelist pointed to some misperceptions about the phrase privacy policy. According to this panelist, many consumers believe that if a company has a privacy policy it means the company does not share data with third parties, we know better, but consumers do not. There is also general agreement that consumer disclosure as we know it simply does not work. But as today's panelists pointed out and I think a lot of discussion we just heard confirms this, just because it's broken, doesn't mean that we should scrap it or discharge it. Transparency is challenging but we need to think more creatively and innovatively about how to deliver important information for consumers when they need it and in clear and in simple terms. We heard about new efforts to make effective and meaningful disclosures. On the positive side, we heard that companies like Google and Yahoo! are creating pages that consumers can click to see what data these companies have about them. That is to the good. But there is work to do and consumers are not clicking through to this data in large numbers. The economists also pointed out the limits of disclosure. They noted that consumers engage in bounded rationality where they tend to discount long-term negative effects of giving up their privacy. I also have a questions about timing, is notice at the time of collection adequate or should we think about notice at the time of use? These are questions we have to confront. Online behavioral advertising remains a highly visible issue. Since the FTC released its report in February, the industry has responded with a number of initiatives, including efforts to improve consumer notice about these ads and to provide

more effective choice to consumers. We welcome these efforts. There are, however, concerns, particularly about how some in the industry frustrate consumer choice by using technologies other than cookies to gather information online and by collecting and using sensitive data for behavioral advertising. There was a lot of discussion about what is sensitive. As with beauty we learned that beyond certain categories, sensitivity may be in the eye of the beholder. Indeed one speaker mentioned the example of Rogaine. Now I might not care if others know that I use it but I would add parenthetically that if I do, if apparently doesn't work. But someone else might care. The data broker industry is largely unknown and invisible to the consumers. Yet there's a lot of diversity in the types of information, uses of information and even the rules that apply to how such information and in some cases highly sensitive information is managed. This is an issue that may warrant our attention. Finally, we heard discussions about various approaches to managing the privacy and security of consumer information. The self-regulatory approach as has occurred in the advertising space, fair information principles including notice, choice, access, security and enforcement. And the experience of other national regimes and the importance of harmonizing standards so as to not impede international commerce. These are all questions that we will be confronting. In short, we had a robust debate with interesting arguments on all sides, just the kind of debate we hoped for. We welcome, we invite this kind of dialogue and those planned for our second round table to be held on January 28 in Berkeley, California. Again, I want to thank everyone who contributed to the success of this important conversation and we look forward to seeing you next month, next year in Berkeley. Thank you very much for your patience. [applause]