

>> Maneesha Mithal: Okay, well, thanks everybody. We are now in the home stretch, the final panel in the final round table that the FTC has been hosting over the last several months. And those of you who have stuck it out will not be disappointed. We have a very distinguished group of panelists with us. And let me just introduce them down the line. We have Paula Bruening from the Center for Information Policy Leadership. We have Fred Cate, from Indiana University School of Law. We have David Hoffman from Intel. Chris Hoofnagel from Berkley. Richard Purcell with the Corporate Privacy Group. We have -- sorry, Jennifer Stoddart, the Canadian Privacy Commissioner. And we also have John Verdi. John is filling in for Mark Rotenberg, who was called to testify before Congress. So John is a last minute replacement, and I'm sure he'll do a great job. So before we get started with the steps into the panel, I thought I would just start with some opening notes. First, the title of this panel is "Lessons Learned and the Way Forward." So the way we'll do this is, we'll be picking out nuggets of things that we've learned at the prior roundtables, and we'll be exploring them and talk not about challenges, but mostly about the way forward and the ways we can address the challenges that have been raised. So, I urge the panelists to kind of look forward and talk about the future a little bit. Second, we have a lot to cover in this hour an a half. So I'd ask the panelists to keep their remarks brief and to the point. And finally, since we have a lot to cover, I just want to be clear that the issue of government collection and use of data is a really broad one and that's something that we won't be covering today. So, if you keep your comments restricted to commercial collection use of data, I think we'll be able to get through the material that we have. With that, let me start with the first question. We've heard a lot today, and in prior days, about the distinction between Personally Identifiable Information and non-PII, how it's been increasingly blurred. And I want to throw the first question out to Richard Purcell and ask him, is this PII distinction still viable? Is this something we should continue to use in our vocabulary as we talk about data collection practices?

>> Richard Purcell: Thank you. Personal data has become ubiquitous in all of our society. I was speaking with Dana Boyd, a Microsoft researcher who was referred to earlier, as well. She had a really interesting comment. Her observation is that decades ago, not that many decades ago, what was easy was being private, and what was difficult was being public. In today's world, that's reverse. It's overly easy now to be public and very difficult to be private. One of the things we've discovered is that all data has personal implications. If it can be linked to a person, not only can it

be, it will be with some inevitability. I believe that any bit of data about an individual deserves the kinds of protections that we currently reserve for personally identifiable data, largely because, inexorably -- maybe not today. You know, I'm sure somebody could make a big argument that would say, "No, no, no. We can actually have non-PII." It's going away. That distinction will no longer be relevant in our future. And since that is a case that I think we can all commonly agree on, that at least in the near term, sometime in the short-term future, all personal data will ultimately become identifiable or attached to an individual, that all data about people needs to have protections, needs to have consideration, needs to be protected in some way or other. It would be -- it's a little bit like confidential data at a business. If it's about the business, there is a chance that it is -- needs some kind of discretion, exercised around it, period -- end of story. If it's about intellectual property, if it's about processes, any of that, what we call maybe trade secrets, then it needs to have protection and discretion has to be applied. If it's about a person, at the very least, we have to be discreet about how we use it. And so, for the future I think, yeah, there is no such thing as non-PII. It just should not be treated differentially. It's all roped together.

>> Maneesha Mithal: Commissioner Stoddart.

>> Jennifer Stoddart: Thanks. Yes, amazingly enough, in Canada we never made that distinction. We just talked about personal information, and some of our American colleagues started talking about PI and PII. And we just say, "Well, what is that?" And kind of, you know, try and munch that one over. But what we do in Canada -- first of all, I think the work of people like Latanya Sweeney was carefully studied and the lessons were -- have made a big impact on Canada, even about ten years ago. So we avoided going to a very tight distinction between the two. And then generally, in Canada, we use concepts like proportionality, context, how the laws applied, what the outcomes are to be, to modify whatever the principle is. And so I just like to tell you what the -- our own federal Courts said recently, almost paraphrasing Richard, in a case where we proposed this test and it was adopted. "Information will be about an identifiable individual, whether as a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information." The information that was in -- that was being contested in that case, it was about drug trials and government-held information on drug trials. The particular piece of information that was withheld was the province. The province is not Personally

Identifiable Information, in itself, probably, but combined with everybody else, would've let the media learn about who had died in a drug trial. And so, in that case, it was adopted. So that's how we approach thinking, everything is potentially Personally Identifiable Information.

>> Maneesha Mithal: Well, let me ask a follow-up question, and then I'll get to David and Fred. So, suppose a company says to consumers, "We collect your information and share it with third parties on anonymous or aggregate basis." Given what you all have just said, does that create a false sense of security for consumers? So, I'll call on David and Fred, and if anybody wants to answer that question, or address something that's been said before.

>> David Hoffman: I think the answer to that is, "It depends." I think there are ways to anonymize data or de-identify data. But depending how that data is then going to be used, and whether it's combined with other data, could potentially have it relate to an identifiable individual in the future. I think the debate over, "Is it personal data or non-personal data? Is it PII or is it non-PII?" is something that we have spent a tremendous amount of time as a privacy community debating for maybe the past five years, especially, and I think it's largely been an unproductive debate. I think most of the place where the debate has happened has been in Europe, on the definition of, "What's personal data in Europe?" particularly with respect to IP addresses. And IP addresses, I find to be interesting, particularly for the company that I work for, because what an IP address really is, it is an identifier and most often a unique identifier at least for a period of time that's stored in hardware or software. There's actually a great number of instances of similar identifiers. So I think the question -- you know, under the implementing legislation of the 9546 directive, what's interesting in Europe is the definition of "What's personal data?" Something that can relate to an identifiable individual, and things that could likely, reasonably relate to an identifiable individual when combined with other data in the future. I think it's fairly easy to see that many of these identifiers that could occur in hardware and software could potentially fit into that category. So the question is then, "So what?" I think -- and this is where, what I think is really important to learn from that debate, which is, that the reason why so many organizations and entities needed to come forward and to try to fight that was because the restrictions that would be imposed upon them then, if a certain category was filed under the definition of personal data. Under some of the Nation State Implementing Legislation of that directive was deemed to be very burdensome, and I'm not saying

whether I think it was or not, I'm saying that, it clearly was by others. So, for example, people make the argument that under the U.K. law, the existing U.K. law, that if something falls under the definition of personal data, then an individual has a right to get absolute access to all of the processing of that. If you think about that in the terms of a unique identifier in hardware or software, it may actually be extremely difficult, if not impossible to actually even be able to provide that to an individual. And, even whether, if it is possible, you'd have to ask the question, "Well, does it really make sense for them to know all of the logs everywhere, where every IP address is that could relate to them, and how are we going to authenticate that individual to come back to see if it really does apply to them?" So, once again, I think what this really comes back to is, these definitions make a lot of sense, if we have flexible normative standards that are applied on top of them that really makes sense for the degree of protection that's necessary for that type of data, which I think is something that Richard and Jennifer were both talking about and I wholeheartedly agree with.

>> Maneesha Mithal: Okay. Fred, I'm going to give you the last word on this, and then we'll move on to the next topic.

>> Fred Cate: Thank you very much. I would certainly echo the point on proportionality, and just say, I think we might add to that the notion of contextuality, because you would have to say PII for what reason? So, for example, our Freedom of Information Act exempts certain data that might be thought to threaten privacy. Well if we said all data concerned was personally identifiable, we might exclude all data from that, or access the examples already been given, if we apply access to all data that we think could be used to identify you, we would then make access meaningless. So, instead I think this notion of proportionality applied in context, and I think maybe the best example there, and it's one in an area already been touched on today, is in the area of health information. So for example, for years, companies that do health research dealt with we would call "anonymized data." Meaning, they knew exactly who they were dealing with, but they were required by the FDA to screen that identity behind a number, and that number could not be applied to de-identify the data under threat of federal penalty, except in certain circumstances. So, most of us would refer to that as de-identified data. Yet of course, technically, Latanya Sweeney would tell us that is fully identifiable data. The point is irrelevant. In other words, it's a question that I suspect has no

meaning any longer, rather we come back to this question of, "What is the broader context and what is the proportional response to whatever we come up with out of that?"

>> Maneesha Mithal: Okay. Thank you, Fred. I'd now like to move on to transparency. We've talked a lot about notice and choice at these workshops. And actually, they've probably been fairly vilified, the idea of long privacy notices that consumers can't understand, that they don't read. And if they read them, they can't understand them. But I'd like to direct this question to Fred. So, is there a continued role for notice, and if so, how can we make notice meaningful?

>> Fred Cate: This is -- this is so hard. Let's face it -- I mean, notice and choice have not only been vilified. Somehow, they've managed to continue to survive. You know, I was going back looking at the record -- every chair of the Federal Trade Commission since Chairman Muris has expressed dissatisfaction with notice. Yet, they seem to hang on. Like, what do you have to do to kill something around here? [Laughter] They keep coming back. And you know, at the beginning of the last of these three round tables, David Vladeck began by saying, you know, there's still an important role for notice and choice. And I find myself scratching my head saying, "What is that role?" So, I guess there is some role left for notice. "But what is that role?" is, I think, a very hard -- a very hard question. So, I would say, one of the things that many advocates point to notice for is, it tells the rest of us -- just the few of us in this room, nobody else outside could care less about what we're talking about -- but those of us who do, it tells us what companies and government agencies are up to. So in that sense, if we just mean transparency or regulatory filing, like you have to tell the FTC, what's your privacy policy -- yes, I think that's a continuing valid role for notice. Another area where notice, I think, has clearer continuing validity is where there is a meaningful choice for an individual data subject to make. So if you're actually going to ask me, "Do you want your data used, and will it point this way or that way?" You got to tell me. You got to give me the notice, or else that is a completely pointless illusion of a choice. So in that one instance, individual notice might make sense. And then, a third rule for notice, although I would never use the word "notice" for this, ever -- but just because somebody else might, and I don't want to feel like I've left something critical out. I think there's an educational role for notice. So again, I would not call this notice. But again, let's face it -- most people are not interested about being educated about how their computer collects data about them, or how business collects data about them, and the

environment. But for those people who are or in those settings where we really think it's important that there be education, notice of some form probably plays some role in that education. Those would be my three suggestions for notice to remain valid.

>> Maneesha Mithal: Okay, reactions -- John and then Chris?

>> John Verdi: Sure, yeah. I would agree with the widespread derision regarding notice, and the notice and choice model. I mean, I think that what we really have at this stage is an understanding that control, and access, and meaningful and effective privacy safeguards are what consumers expect. They are what good businesses provide, and they are something that needs to be required. And I'll just tell a brief story about one of the more recent failures of notice -- you know, and notice and choice. There's a company out there, called Echometrix, which publishes a piece of software that parents can purchase and download, and limit the access of their children, when their children surf the web. It's safe surfing software, right? And this company also has a sideline in selling all of the data about the children that it's "protecting" to marketers, so it can profile them without telling the parents. But here's the issue. We ran in to this issue, and the issue was brought to the attention of the Department of Defense. And it was brought to the attention of Department of Defense, because the D.O.D. had agreed to sell the software to military families at a discount. So you could get your spyware cheaper. And what we found out was, once the D.O.D. became aware of the situation, they began making inquiries with the company. And they said to the company, "Why are you doing this? This is inconsistent with our principles. This is inconsistent with fair information practices, et cetera, et cetera, et cetera." And the company said, "Well, there is this check box, and you can check this check box. It's buried a little bit, but it's in there somewhere. And you can opt out of all of this data collection." Right? And the D.O.D. responded by saying, "We only permit personal information to be collected in order to improve the quality of the service. You've purchased product, we're going to collect personal information to improve the quality of the service." Fine, fair enough. Everybody can get on board for that. Just by giving someone notice and the choice not to check the box, that isn't good enough, right? So I think that that's sort of a common sense principle that we see in real life. You know, you drop your car off at the gas station for service, and they drive it around if they need to, to figure out where rattle is. And they replace some parts, and they take some things apart. And hopefully, they put it back together, and all that

fun stuff. But if they decide they're going to take it to Florida, and then they're going to drive it back, you know -- I mean, they explicitly didn't prohibit that when you entered into that agreement. But there's sort of a common sense understand. They're going to do what needs to be done to provide the service. And I think data collectors need to be doing that, as well. Notice and choice doesn't allow you to collect data, and use data, and transmit data, and share data and disclose data in ways that are wholly unrelated to the service and not beneficial to the consumer.

>> Maneesha Mithal: Chris.

>> Chris Hoofnagle: I would agree with everything Fred said, and go on to say that we need to, if we're going to pursue notice as a solution, I think we need to change the incentive structure in the notice format. I just noted that every time that I go online to pay my telephone bill it interrupts the payment process to ask me if I want to go paperless, every single time. And that is so important to them that, they are willing to interrupt the payment process -- I'm about to give them money. [Laughter] They said, "Oh, before you give us money, we'd like you to go paperless." The other kind of example that I would bring up comes from Chase Bank. They wrote a notice concerning overdraft fees, if you want to opt in to overdraft fees. And the notice that they wrote reads, "If you do not contact us, your every day credit/debit card transactions that overdraw your account will not be authorized after August 15th, 2010, even in an emergency." This is written in red and underlined. We don't see privacy notices that say anything that clearly or that urgently. And I'd argue that it's a problem of the underlying incentive structure.

>> Maneesha Mithal: Okay, I see Paula, you raised your tent. And I'd like to actually direct a specific question to you. Fred raised earlier the idea that maybe notice is useful when there's an opportunity for a consumer to make a meaningful choice. So, just broadening that a little bit -- are there things that we can take off the table in notice, so that a notice might be more readable to the consumer?

>> Paula Bruening: Well, I think that, you know, one way to think about notice is that there may be two kinds of notice that we might be able to offer. And I'd just like to preface that by saying, I agree with Fred's analysis, that notice remains important for all of the reasons that he stated. But I

think, you know, there are two ways you can think about this. Indeed, notice is at its most useful when there is something meaningful going on, where you can truly consent where there is really a choice that the consumer has. And -- but that doesn't happen all of the time. And so, it would seem that to maintain the transparency, you want to have some kind of an available notice, where you can -- where we can all, wherever we sit, whether it's in government, or it's policymakers in this room, or it's the average person sitting behind their computer screen -- they can find out what's going on within a company, in terms of their data collection practices and their privacy protections. I would say that there's also an opportunity for notice where there's actually going to be a real choice that a consumer can make. And that's what I would refer to as something we'd call "just in time notice." And at that point, you can offer to the consumer the information they really need in order to make a meaningful, well-considered choice. Now, what those particular pieces of information are that they need, that probably remains to be worked out. But I think there is work to be done to figure out, what does the consumer want to know? What really underscores a good decision? And then, figure out ways that you can make that available in real time when the data collection is actually going on, and when there's is a real decision to be made.

>> Maneesha Mithal: And if I can just follow up on that. We've heard about this concept of "just in time notice" before. But I want to kind of bring it back to Chris' point, which is every time he makes a payment he's inundated with that request of whether he wants to go paperless. And so, is there a concern about consumers being provided too many notices, being inundated with notices, at the "just in time" point? I can ask -- Paula, you could answer that, or David, or Jennifer?

>> Paula Bruening: Well, just as a quick response, we probably doesn't have as much choice as we like to think that we do. So if you really put the notices in front of people, when they actually have the choices, it may not be as many notices as we might think. The important thing though is that, behind that "just in time notice" is something more robust, that's more comprehensive, so you can really get the entire picture, if you want. And I would argue that probably, most people aren't that interested in it. But it does provide the transparency. And that broader notice is also available in cases where there really isn't choice. But you just want to know more about what's going on, as does the FTC and other people who are -- and the advocacy community.

>> Maneesha Mithal: Okay. David.

>> David Hoffman: I was just going to try to answer the question and state specifically some things that I don't think serve a lot of purpose in notices anymore. For example, I think there's been some fantastic work that's been -- recently done on a used-based model around privacy. And a lot of that work has been to delineate certain uses of data that are largely implicit in engaging in a transaction, and shouldn't require any sort of additional choice, or I think particularly even an additional notice. So if you're ordering a book, for example, should you have to be provided with notice that that book company is likely going to provide your address information to a separate company so that that book can be delivered? I don't think you necessarily need to be given that notice. I think that's implicit in ordering the book. There are different categories of those. I'm not sure that that information, when it's provided, really helps any individual make a better choice in those instances. I just think it makes the notice a lot longer and read more like a large legal document. Another one that I would state would be in the area of security. I'd be interested in -- maybe in a show of hands. Is there anybody in the room who has read a privacy policy and read specifically the security section that said, "Now that I've read that, I really don't want to provide the information to this"? So we go -- and we've got a couple people, I'm surprised, because everything that I read says we provide reasonable and robust security. And I say, all right, I've been a lawyer for an I.T. organization for a long time. And I'm not sure I know what that means. But c'est la vie. I think there's a bunch of categories we can take out of the notice.

>> Maneesha Mithal: Okay. Commissioner Stoddart and then Fred.

>> Jennifer Stoddart: Yeah, just to remind us that there may be light at the end of the notice and choice tunnel -- because about 450 million consumers in the EU and 36 million in Canada have never used that model. We used informed consent. There doesn't seem to be the debate about notice and choice, I guess because I think it forces us to be more simpler, because the test is, does the citizen or consumer really understand what they are getting into and really happening with the data? So I think, rather than being viewed as a kind of notice of legal liability and what you will and will not do, it's "does the consumer understand?" And I think it forces level of simplification. But I'm just presuming that. I think it would be interesting to see what global companies that sell

the same products in the United States, and then in consent environments -- how do you change that particular part of linking up with the consumer, and does that provide any ideas for innovative ways forward that are global?

>> Maneesha Mithal: Fred?

>> Fred Cate: I was just afraid we were feeling too positively in here about notices by finding any proper uses for them. Although, I think that the two last comments have helped. To clarify that, I just think we should be frank. I mean, on the whole, notices have been unmitigated disaster.

[Laughter] And that is --

>> Maneesha Mithal: How do you really feel? [Laughter]

>> Fred Cate: Look, I've toned that down for a public audience. [Laughter] And in many ways, I mean not just because many people can't read them, or don't read them, or all of those things. Partly for reasons already touched on -- because they have become contracts. And therefore, any hope we have that they would communicate something intelligible, the FTC took away when it said, "We're going enforce these as promises that you will be held liable for." So immediately, we started adding the words "reasonable" and "where appropriate" and "as best possible." And we took what could have been a meaningful notice, and turned it into something that we would be able to fight about in court. But in addition, notices so often now become an excuse for not doing something else. You know, we know we've got a problem. We were going to solve it. But you know, let's just send you a notice instead. Maybe breach notices being the classic example of that. So that we've lived through, now, seven years of millions of breach notices being mailed before, finally, a state got around to saying, "You know, let's try to maybe stop these breaches. That would be an interesting idea, rather than wait until they occur and send a notice, and make ourselves feel better." And I think, in fairness -- and I don't in any way want to get arrested before I get out of here or anything. But we don't just do this in privacy. I mean, there are many other examples of places -- you know, anyone who has ever applied for a home mortgage and gets all of those federally required notices -- which again, nobody has ever read, and nobody will ever read -- or an informed consent notice in the hospital. It's something we use a lot in ways that are, frankly,

inappropriate and becoming increasingly inappropriate. So while there may be -- while there are still some places notices can be used, I think we should be clear, at least, that notices should not be the de facto position, and that when used in their other roles, for transparency, for education and the like, we're going to have to move away from treating them the way we have treated them, if we have any hope of them ever conveying information that the public will care about or be able to internalize.

>> Maneesha Mithal: Fred, if I could just stick with you for a minute. You talked at our first roundtable about the illusion of choice. And I think somebody here -- we started down the road of informed consent. But could you talk a little bit about what you meant by the illusion of choice, and segue into a discussion of how we can actually make choice meaningful?

>> Fred Cate: Yes, I can, I hope. Let me just say here, too, because I don't want to do anything that makes it sound like I think choice is a good thing either, because I think too often, and again this is well illustrated on this panel and earlier today, we slough off good protection by saying, "Well, they checked the box." And so, we should be very careful about not sort of celebrating choice in a way that's inappropriate. But I think the illusion of choice is, for example, where we provided choice where there is nothing to choose from. So accept or decline, when decline shuts down the program, that's not meaningful choice in my world. I don't think providing choice, where the choices are, if you will, minuscule in comparison with the things people really worry about. I often feel this way in the Gramm-Leach-Bliley environment where, you know, the types of things people really worry about with their financial information are not captured by the one choice that Gramm-Leech-Bliley gives us. You can opt out of certain marketing, sharing of information with third parties for marketing certain non-financially related products and services. It just missed the whole game. I mean, it's like -- it's like arguing over the color of team uniforms or something, instead of the playing of the actual game and how it comes out. I think the illusion of choice is there when people either don't get the notice. So we say, "Well, I had a privacy notice. Of course, we know nobody has ever read it. That page has never been clicked on. But it was notice." And therefore any choices based on that notice, particularly the default, where nobody changed the default because notice told them they have to. That would seem like an illusory choice. So my basic principle would be, any time where there is a choice that either is not real, here's nothing for them

to choose from, or it's not about the types of concerns that would really face most consumers -- that is an example. I mean, we saw one -- quite recently, like just the day before yesterday, I was flying in here, and I saw a notice I had never seen before, which I'm just embarrassed about. But it said, "You do not have to provide this information to the TSA, but you will be denied boarding if you don't." [Laughter] Well, I'm sure somebody over there is celebrating that choice opportunity, but I would not call that meaningful choice.

>> Maneesha Mithal: But just to follow up, is there -- I think you acknowledged at the outset that there's a role for notice when there's an opportunity for meaningful choice. So where there are situations there is an opportunity for meaningful choice, how can be implement that?

>> Fred Cate: Yes. And let me be clear -- I do think there are places where there are meaningful choices. And particularly -- I mean, just to take one example, where you're going to make a use of data that is unexpected and not related to the transaction. And to say at that point, "I'd like your permission before I do this." And in that instance, I tend to think that just in time, notice related to the choice, almost always is the best way, because will people forget about what it is they're choosing if you gave them notice 30 seconds earlier or three days earlier, or you know, heaven forbid three months earlier. This, of course, makes a particular challenge for electronic devices that have to pose choices where they can't deliver the notice. So you've got, you know, a hand-held device that may have a screen or no screen at all, or the computer in your car or what have you, where you had to make that choice in an earlier environment. You know, obviously, a very difficult situation. So I think giving notice as contemporaneously as possible with the choice will help to make the choice more meaningful. Similarly, I think making the choice -- the notice as simple as possible and related to the choice. So again, not notice about things which nobody would care or would expect otherwise. So, for example, we have lengthy notices today about "your information may be shared with service providers who will provide" -- you know, the example of -- you know, "to mail your package to you, we're going to have to share it with the Post Office, who may in fact share it with somebody else," but instead to focus the choices, and therefore the notice on where you really have a meaningful choice to make. And then, I don't think it hurts to make that -- maybe you have some other longer notice available someplace else, but the actual notice at the point of choice, to be really bold and clear and basic, and I always described these like cigarette

pack warnings. If you can't fit it in, you know, a little box, in 12-point type, it's probably too detailed, for most people.

>> Maneesha Mithal: Chris.

>> Chris Hoofnagel: I think the illusion of choice goes much deeper than just the notice problem. In particular, if you look at things like opting out of behavioral advertising, or targeted advertising, you download an opt-out cookie. I think most consumers believe that that opt-out cookie means that they are not tracked, when in fact it means that they are not getting targeted advertisements. To me that's the worst of all privacy worlds. You are still being tracked, and you get -- you do not get the benefit of the tracking. And we're now in a place where there are companies that are very powerful and are staffed by very smart people, they keep reminding us. That, you know, privacy is about the fact that you can tell them not to market to you about golf or tennis. But privacy apparently is not about the fact that they have trackers on 70% or 80% of the websites on the internet. So your choice is, I think, completely illusory and counter productive in a lot of contexts.

>> Maneesha Mithal: Okay. Actually, that's a really good segue into a discussion on access. Chris, you mentioned the fact that companies may have data about you that they may not necessarily use. And I'm wondering if access is a way to address that issue, so that a consumer might be able to see -- see what information a company has about it. So maybe Paula, would you like to talk a little bit about access and the potential benefits of access, as well as some of the costs?

>> Paula Bruening: Sure. You know, I think -- access, I think, has a very important role when it comes to transparency. It informs individuals about what kind of data organizations have about them. It can promote accuracy of the data if there's a correction right, particularly if that data is really critical to some kind of decision making, and it promotes the suitability of that data for whatever purpose that it might be put to. And I think more over, it really enhances the trust relationship in good situations between the individual and an organization who is maintaining data about them. I think though, you know, when we talk about access, I think we have to be careful about how we think about that, because if you think about access as an unmitigated right across all situations, I think you start running into problems pretty quickly. One is the cost issue. You know,

there are legacy systems that have to be dealt with when you're talking about data. Data has to be collated from a variety of different places. Some of them are quite far flung. So making decisions about, you know -- what kind of access to offer in different situations I think is part of this puzzle. I think in situations where that data is really critical to decisions that are going to be made about me, I want to see the data itself, and wherever possible, I want to correct that data when it's wrong. It's better for me, it's better for the company. It allows for, you know, a cleaner transaction. But when you're talking about large amounts of data that may be something like marketing data it may be that, to keep the cost down, but to maintain the transparency, we can provide a more generalized kind of access that says, this is the kind of data that we maintain about you. And now, you have a right, then, to suppress that data, to have us not act on it. There's another right that goes with that. But we're not in a position where we're going to gather every single bit of data about you from every place we might store it, because that would be too burdensome. It's one way to approach it.

>> Maneesha Mithal: Reactions, Richard?

>> Richard Purcell: I have a concern about the response that some companies make, that say that it's just too hard to get to the data to give you access to it, because to me, that indicates that they don't know what they have, that they're not -- they don't have access to it themselves. And to me, my next question would be, are you over-collecting data? Because if you can't get to it, then why do you have it? How are you using it? Are you using it? And what is your retention policy? Because it may be that this -- the fact that I can't get to it, or it's too expensive to bring it together means it's not got the value that you've promised me that it provided when you collected it under your disclosure. It really does bug me. I have a feeling that the access discussion can easily reveal very poor information management practices, including particularly over-collection and over-retention of the data itself.

>> Maneesha Mithal: John?

>> John Verdi: Just to echo what Richard said, there are also accuracy issues with that data, because if the company is collecting data, using data and disclosing data that they've associated with an individual, and then says to the individual, "Well, it's too hard for me to give you access to

the data, or to authenticate that you are who you say you are, so I can give the right person access to that data," perhaps they ought not be disclosing the data to third parties and making the representation it's about this particular person. I mean, some of the basis for these -- this data collection, these data disclosures is the company making the link between the individual and the data. Well, if they aren't terribly confident in that link and that comes out in access and authentication process, that's sort of your answer right there.

>> Maneesha Mithal: David?

>> David Hoffman: So I have a long history of bugging Richard, so I'll continue to do that when he said that this really bothers him. I would want to come back to the first thing that we talked about, about the breadth and the scope of what personal data could be, or personal identifiable information is. The broader you go in scope, the more difficult it's going to be to determine who you should actually give access to. How are you going to authenticate and identify? This same data may, in the future, relate to a specific individual, but are you actually forcing me now to do that comparison and relate it to an individual to figure out if it should go to that particular individual? These are not, I think, just excuses that companies may not give access. Sometimes they are, I would agree. But not always -- it's not always reasons that their retention limitations are unreasonable. For example, I've talked to companies that do -- make software that does security screening, for example. They have to collect IP addresses to do the kinds of security screening. The retention period for those might actually be very small. But it's continuous. When you get an access request in, what's the universe? When do you stop deleting? What do you -- these are really difficult situations, which is I think the only thing I can take away on access is, I think it is a fantastic aspirational goal. And I think people need to be able to try to give as much access as they get. I think in many situations, it's very difficult. In other situations, it could actually be harmful in a number of places to actually provide more access.

>> Maneesha Mithal: If I could just follow up on that, is there some low-hanging fruit on access? So for example, you know, it might be one thing to get access to data that, you know, Amazon has about you, about your prior, you know, product purchases and that sort of thing. But how do you get access to data that a third party might have on you that's not consumer facing? So I wonder if

anybody wants to comment on that distinction. Well, actually let me go with Paula first, since she had her tent up.

>> Paula Bruening: I was -- actually wanted to respond to a couple of the comments made about prior -- and I definitely agree, that it should be getting easier to provide access rather than harder. I think our systems are such that we should be able to gather it more quickly. And I think the data that's available in the ordinary -- of course, with business we should be able to make that available to the consumer. But I think, you know, the sort of distinction that I'm talking about in terms of access has to do with the use to which the data is being used. As I said, you know, if the data has to do with my tax return, if it has to do with whether or not I get a loan, if it has to do with whether or not I can either buy or operate a car, I better have access to that data, so that I know what's going on. If there's a problem I want to clear it up. I do think there are different kinds of data, and they may -- they may warrant different levels of access. But it really has to do with how that's being used and what the impact is going to be on the individual.

>> Maneesha Mithal: Fred?

>> Fred Cate: Yeah, I mean, I think there are loads of examples of low-hanging fruit, where access could be provided. And I think one useful place to look -- I'm not suggesting you adopt this model, but simply a place to look is the experience we have with other laws, for example the Privacy Act of 1974 and FERPA, both of which talk about systems of records. So that you say, effectively, I'm not merely oversimplifying, but also being incredibly inaccurate. But Chris, we'll clear this up in a second. But effectively, if you maintain records in such a way that you identify them or you locate, or you pull data out of them on a person-by-person basis, providing access ought to be pretty simple, because you got it there. That's how you use them. That's quite different from saying you have to search every PC in your business to see if anyone has an e-mail that has this person's e-mail address in it. And so, it seems like we could start with some of those. In fact, there's very good work done on the privacy act since the privacy act. The GAO did a report. There are certainly other reports done by privacy advocacy groups about ways of modernizing that definition, but still keeping it focused on some notion of a system of records, or record where you have information that is stored in some appropriate way. I would also say, I don't want us to trivialize the security

issue here, because I think it's actually quite significant. And it gets more significant, the more important, or relevant, or sensitive, or whatever we want to say the information are. So when the Federal Trade Commission's own panel on online access and security effectively couldn't reach a conclusion on access, I think it was as much the security concern, as it was the difficulty issue that drove that. And so, although we've certainly come farther, we can do things now that we couldn't have done eight years ago when that panel met. I don't think that those concerns have been resolved yet.

>> Maneesha Mithal: Okay. I want to go back to something that Paula mentioned in terms of access, and correction, and suppression. I think, and correct me if I am wrong, Paula, I don't want to put words in your mouth. But I think you suggested that for marketing data, there might be categories of information, and there could be a suppression right, whereas for other categories of data, might be a correction right. I just want to see if there's any reactions to that. Are there areas where we would want to give consumers a correction right, and how do we draw the line there? Richard?

>> Richard Purcell: Well, it's vitally important that you give people correction rights in a variety of scenarios. But at the most fundamental, if there is a denial of service, or a removal of a service, or for some reason, you know, some lessening of the relationship based on information, the individual has to have an access to the decision points that were made, upon which that decision was made, in order to review them and correct any flaws in them. And you know, this goes directly to the idea of saying, you know, you present your credit card, and it's denied. Why? You've got to give access to somebody by saying, you know, "We're not providing you service based on this data." The individual has to have access to the data in a reasonable way. And you know, "reasonable" means timely, prompt and effective in terms of being able to challenge or correct it. In order to make sure that the service is being denied based on a fair reason, and not some unfair reason. So, I mean, this is the concept of redress. We have to keep in mind that although there's been a lot of discussion over this day, and prior to roundtables, that people are discussing each of the elements of the fair information practices principles, as if they stand alone, they do not ever stand alone. Remedy or redress -- access or redress are related. They're related to the notice. They are related to the choices. They are related to the accountability of the organization. None of these are first among

equals. They are equal concepts that all have to proportionately build a regime of respect for personal information.

>> Maneesha Mithal: Okay. Commissioner Stoddart?

>> Jennifer Stoddart: Yeah, I just was reflecting, why are we talking about access so much now? You know, I'm the fish out of water here, right? I'm really not in my element. And I wonder -- it sounds to me, if I may say so, that we're talking about access so much, because the consumer is nervous, or ill at ease and concerned about his or her information, how it is being handled. If I reflect on our own organization that regulates personal information, the law that's based on fair information principles, is developed by the Canadian business community based on the OECD guidelines, the same guidelines on which you based your fair information principles. And so, there's a whole series, as Richard has just reminded us, of principles. And I think if there were more emphasis on proportionality limiting collection, the use principle, not collecting information for which you do not really have a use, that there wouldn't perhaps be so much anxiety about access. I mean, I look at our complaints -- 60% of our complaints are about collection use and disclosure of personal information. I don't remember that access is way up there, but I don't have the annual report in front of me. I don't know why Canadian consumers aren't, you know, so concerned about access. That being said, access are some of our most difficult cases and we're prepared to go to federal court on an access case, but in a real kind of live human situation access case. So I just wanted to put that on the table, that if you have a whole framework that is applied, principle by principle, it seems to me that that would lower the demand for access.

>> Maneesha Mithal: Okay, I want to follow up on a point that commissioner Stoddart just mentioned, which is the point of collection limitation. I think we've talked at this roundtable and prior roundtables about the benefits of having a collection limitation. And I wonder if any of the panelists want to comment specifically on that. In fact, Chris, why don't I call on you? I know this is an issue of interest to you.

>> Chris Hoofnagel: Sure. I'm happy to talk about it. You know, in looking back at three roundtables, one of the most salient arguments I think we heard was the idea of having a regulatory

system that only looked at use of information and did not put limits on collection. There were a number of organizations that said, "Let us collect what we want and just create rules around use." And I was interested in why none of the advocates kind of jumped on that. It seemed to me that if you didn't have collection limitations, it could open the door to all sorts of pretty bad practices -- spyware would be legal under such an approach. You could collect information that self-regulatory groups have said that they will not collect, such as sensitive, personally identifiable health information. And just as Richard just explained, that fair information practices are related to each other, I think collection limitation ends up being closely aligned with use limitations and implementation. In looking at the privacy act, you know, if you have a situation where an entity is allowed to approve uses of personal information, they are going to run wild with that authority. I think the FTC has 16 routine uses of personal information under its Privacy Act implementation. So it seems to me that, you know, you're opening your door to a lot of problems down the road with different uses, unless you have collection limitations on the front end. The other issue, you've seen in the Privacy Act is when data matching arose. You know, once you have a lot of data, it becomes kind of impossible for decision makers not to use that data for new matching purposes that probably would not be approved of at collection. So I do think we do need to talk about both the procedure and substance of collection limitation, and thinking through these issues, because on the back end, you're going to see a lot of uses that are nefarious or objectionable if you don't place some kind of limit on the front end.

>> Maneesha Mithal: John.

>> John Verdi: You know, I think that that's particularly true, given how quickly the technology evolves, and how iterative a lot of these products have become. And I mean, you don't need to single out particular products. But you can see how, you know, a single technology product like Facebook, right, looked like something two years ago, and it looks very different to its users now, in terms of how it uses data and how it does things like that. You can see how Gmail started out as an e-mail service, and then integrated chat, and then became really social with Buzz and did a lot of other things, and used consumers' data in very different ways. And in a lot of circumstances these uses weren't just not implemented at the time of collection -- they didn't really even exist, or weren't even contemplated at the time of collection. So I agree with Chris, that the only real way to head

that off is collection limitation, and not use limitation, because you fall into serious problems down the road when you encounter uses that consumers and companies never contemplated to begin with.

>> Maneesha Mithal: Paula?

>> Paula Bruening: I'd just like to comment on both of these comments. I think when you're talking about the use model that I believe that Chris is referring to, it does not take collection limitation off the table entirely. What it -- I mean, to my mind, as somebody who worked in the advocacy community for quite a while, it was to our great consternation that purpose limitation and collection limitation and use specification sort of got written out of the rules. And I think that in some ways, that use model brings them back into play. But it becomes the company's responsibility to be answerable for the amount of data that it's collecting, and the kinds of protections it's putting in place around that data. It also, I think, implicates the decisions that are being made about how that data is being processed and used, when it comes to new business models and new technologies. So it's not a free and clear -- you know, we collect all of this information, and then you know, there's no responsibility about it. There's an answerability that comes with that use and obligations model that says, you know, I have to be willing to say what I'm doing and have good processes and practices around what I'm doing, with respect to the data that I collect. So I think it's a little unfair to just sort of say that it doesn't factor in at all.

>> Maneesha Mithal: Actually, if I can follow up on the last couple of comments. So let's say a company has implemented this collection limitation principle and only collects the amount of data necessary to effectuate the transaction. I think John's point is that there still could be unanticipated uses of that data. And so, I guess my question for the panel is -- I hesitate to use the term "notice and choice" -- but how can we get informed consent of consumers when the data is used in an unanticipated way down the line? Okay, David and Richard.

>> David Hoffman: Yeah, let's me take a stab at that. You know, I keep coming back to Richard's comment, which I thought was very insightful, that it's very difficult to take any one of these individual fair information practices and drill down on it, without relation to the other. When I think about this topic, I think about it under a header of data minimization. And for me, that tends

to mean the categories of collection limitation, a use limitation and a retention limitation, because your question talked about, "What about subsequent uses?" I think that we also -- you can think about retention limitation as the -- one of the best ways to prevent additional issues that come from security breaches. If you have gotten rid of the data, then it's not subject to being breached in the future. And the same -- that's also true for the collection limitation. I think, you know, going backwards, the original concept that people were thinking 30 years ago about how this would handle was not a concept of necessarily what they would call "notice." But there was a concept of purpose specification. There was a purpose for which the data was provided by the individual. And that that was obvious, not just from some sort of notice that was provided, but from the context in which that that was provided. This is why I think, once again, that this is incredibly powerful, this use-based model that's been developed, which is to come back to that to concept and say, "It's the context which the data is being provided that creates what that sort of purpose specification should be." And if you're going to then do something, there are a number of uses and potentially transfers that are implicit within that purpose that you are providing the data. And then, if you're going to have a subsequent use for that data, I think it's quite good -- there should have to be a very effective means for exercising choice on that. I think we've run, though, in to two additional difficulties, which I will point out, and I don't have very good recommendations on how to solve them. I think one is the data not provided by the individual. So how do you manage -- purpose specification if it's actually -- let's say there's a social network that's created, which I think very well might be created soon enough, that people who hate David Hoffman and want to discriminate against him. You know, that might be -- a lot of people are going to join that and share information within that. I might be very concerned about some of the uses of that data. I think the separate category is organizations that are created where the actual purpose is, we might determine to be malicious, or the purpose itself will say, "Our purpose is to collect data and sell it to whoever would like to buy it." What kind of rules do you apply there? And I think then, that creates a situation where we probably do need some normative rules laid on top of these fair information practices to say, where are some -- there are some pieces of behavior that we just believe are malicious and should not be allowed.

>> Maneesha Mithal: Richard?

>> Richard Purcell: I think it's great to kind of hearken back a little bit. Some of these first principles that we talked about -- Jennifer mentioned the OECD guidelines -- really do encapsulate this. And we've been splitting hairs ever since. And we kind of are splitting these things into finer and finer points, until they become less and less and less meaningful in some ways. The original access and redress concept was wrapped up in something called "individual participation." And in fact, consent was part of that, too. And it was a great high-level concept. The individual must be involved and participate in this process -- first of all, by being able to make an informed decision. We got notice out of that. And notice turned into a corporate liability, "cover my ass" kind of situation. And it didn't actually do a lot to allow the individual to make an informed decision. The choice mechanism was every time you want to use data in a certain way, and it's an unanticipated or previously unexplained use, the idea of individual participation is what Paula was talking about earlier -- you pop a question to the person, and say, "Hey, we just had an idea. You gave us this, this, you know, some time ago. We could do this with it. What do you think?" That's not so hard to do. But it definitely falls outside of our current conversation about what consent and choice means. It's a -- it really does let the person participate. Participation also includes, "What do you have on me? What do you know about me? And how can I make sure that what you know is accurate in some way or another?" So this idea that these principles, you know, have been teased apart to the point where they become a bit more difficult to manage -- could be if not resolved, at least we could start the conversation at a higher level and say these ideas of individual participation and of organizational accountability, which pretty well take up a lot of these principles, could be perhaps elevated to a difficult level of discussion, instead of these practices, and these command and control kinds of things. We could start talking about what outcomes are we looking for here, from both sides?

>> Maneesha Mithal: Okay, I'd like to read a question that we got from the audience. "The panel seems to be focusing on information collected directly from the individual. What about a company that minimizes the data it collects from the individual, but appends third party data, which is not necessarily relevant to the original transaction?"

>> Jennifer Stoddart: Well, was the individual whose minimal data was collected told that this would -- that this would be done, that this was the purpose, or one of the purposes of the data collection?

>> Maneesha Mithal: Assume it was.

>> Jennifer Stoddart: Well then, if the individual had an informed consent, they knew that their information was going to be used for that purpose, I think that's -- yep, that's fine.

>> Maneesha Mithal: And if it wasn't?

>> Female Speaker: If it wasn't, well there's a huge problem. I mean, our country, it would be illegal. And I think we had a recent example in one of our investigations, where individuals were not aware of the amount of information that was being shared with third parties. I'm talking about our Facebook investigation this summer. And this is clearly in violation of Canadian law. They have to know, they have to -- well, there were a couple of issues. There was no data minimization. There was access to a whole suite of data, just to run an application. And individuals weren't clearly aware of that.

>> Maneesha Mithal: Chris?

>> Chris Hoofnagel: I've been talking about the privacy problems of enhancement for some time -- the idea that you can go to another company and buy information about your customers independently of their interaction -- I think is problematic. I'd say look at a case called Pineda vs. Williams-Sonoma. This is a situation where a customer goes to a store, and at checkout, swipes her credit card, and then is asked "What is your zip code?" And I think a lot of us have -- we might have different conceptions about what that meant. Some people, if you ask them, they say, "Well, the store is doing demographic analysis to determine where they should place their next Williams-Sonoma." Other people might say, "Well, they need that zip code in order to do some type of fraud, anti-fraud practices like you do at the pay-at-the-pump." But what the store was doing was using the credit card swipe plus the zip code to use a reverse directory in order to get the

consumer's home address. So enhancement is squarely in one of those -- in the area where it's about getting personal information from a consumer without telling them, and personal information that they probably would not provide if you asked. And it's, I think, an area ripe for FTC intervention.

>> Maneesha Mithal: Okay. Fred?

>> Fred Cate: I think this brings us back to Commissioner Stoddart's reference to proportionality. And, once again, it's not an area where black and white, clear lines help us, or are terribly useful. So, for example, if information is going to be repurposed, or it's going to be combined with other information in a way that can constitute a clear, demonstrable harm, however we want to define that, or in a way that puts the individual at risk in some way. I think you would want one level of oversight of that, if you will. So whether that's explicit opt in, notice in choice, or whether that's regulatory approval, or whatever. In the example Chris gave, I guess I would go back to, sort of, the Fair Credit Reporting Act model. You know, as long as the first mailing to that address says you can opt out of receiving these mailings, I'm not sure that it would really make a lot of sense to first send the mailing to the address to ask for permission to send the second mailing to the address to make the offer, then the consumer can opt out of. So it would just take a little bit of common sense, a little bit of measuring or quantifying risk of harm or injury to the individual that might suggest the type of response to the repurposing of data.

>> Maneesha Mithal: Let me follow up on that, and also a point that David made about the need for, in some circumstances, informed consent when data is repurposed. So does this kind of consent or choice, would that include, "well, we collected your information for this purpose, now we're going to use it for this purpose, and if you don't like it, you can't use our site, or you can't use our service anymore." How would people view that?

>> Jennifer Stoddart: Well, I mean, again, in Canada, I think that's not allowed by the law. You have to -- you can only collect information that a reasonable person would think is appropriate in the circumstances. These are not weird Canadian laws. These are based on, you know, the principles that we all -- your country and mine signed on to. And you have to get informed

consent, you have to give access. And you can't refuse to supply the service or the product on the basis that the person will not give you the information, unless the information is appropriate to your line of business and to your service, in that context. So there's kind of an in-built protection. You can't trade a good or service against information, per se.

>> Maneesha Mithal: And again, once again to follow up on Fred's point about scaling the type of consent to the risk of harm -- does it make a difference whether the repurposing or unanticipated use is sharing with a third party versus an unanticipated internal use? Is that a useful distinction?

>> Jennifer Stoddart: Well, you know, in practice, people don't know about these things, usually. I mean, it takes a very sophisticated regulator going on an audit or, you know. How do we know what the companies are doing with information inside, you know? So, there's just -- you know, I think in the debate, people have talked about time being wasted on debates that aren't fruitful. I think it's useful if we, you know, spend time on things that can reasonably happen. And this whole issue of unanticipated reuse, or different use, brings up the question, well, how long are you keeping this information that you didn't anticipate? A week, two weeks, a month before? I mean, is it hanging around for years? And we look at now, it seems to me, that most businesses have a continuous feed of information from the consumers, so that, you know, seems to me that this is not really a use of information that's very credible to a regulator.

>> Maneesha Mithal: Other reactions?

>> Chris Jay Hoofnagle: It seems to me the first third party distinction doesn't make sense anymore. I think it can contribute to integration, and I say that look at companies that have 1,000, 2,000 affiliates, especially in the financial services world, doesn't make a lot of sense. We're seeing, you know, information collection on the internet is done by an increasingly smaller number of companies. And we benefit them by saying, well, if you share data with third parties, you're gonna experience these privacy regulations. So I think it might favor hegemonic actors and it is something we should probably reexamine.

>> Maneesha Mithal: Let me just use an example. So let's say data is collected from an individual to buy books, and then later, the company develops a model where they say "okay, we can suggest books for you." So there's no kind of sharing with any third parties there. Should we be treating that repurposing differently from, I guess, other types of repurposing?

>> Chris Jay Hoofnagle: If that's directed to me, I would suggest that, generally, first party reuses have to be looked at more carefully than they are today, because of how large these entities have become. And it's not just repurposing. I think the conversation cannot end around "is this an appropriate use?" You have to also look at retention, what choice in the matter individuals have about this. Civil -- Civil Service access and law enforcement access, I think, also plays into the equation.

>> Maneesha Mithal: Okay. David?

>> David Hoffman: Yeah, I would want to agree with Chris on that and I'll just add something. I think unanticipated use is extremely important for us to get a handle on whether it's first party or another party. I'm sorry. I think unanticipated use is something that's very important for us to get our arms around, whether it's first or third party. I think there is an additional issue with transferring to other parties, but it's not necessarily around the unanticipated use. It's around the anticipated use, actually, and I think that's around what are the structures that are being put in place to make sure that the commitments that the first party has made are actually being realized by the other party. I think this gets to all of the work that's now being done on accountability, and how to drive that from just within an organization to make sure that all the vendors and all the other parties are making real on those commitments.

>> Maneesha Mithal: Paula?

>> Paula Bruening: Yeah, I would just add that a part of it this analysis really just has to be an analysis of the risk of exposure to the -- excuse me -- the risk to the individual's exposure to some kind of harm. The risk -- and that can be, not just financial or physical, but also -- we're starting to talk about a societal harm, risk to reputation. So that should be part of the analysis. As well as,

you know, what are the expectations of the individual? And making some judicious choices about that, the expectations of the individual, but also the societal expectations. Because I think we've seen instances where a company will step beyond some envelope -- to mix a metaphor -- and there is a backlash. There's a public backlash. And so we generally will figure out as we go, when we've gone, sort of, beyond the boundaries of where -- of what people will accept, and it's that risk analysis, part of the risk analysis is figuring that out as the company goes along. Because I think that bright line of internal versus external doesn't really work. You can have data practices internally and you can do analytics internally that can be just as harmful as anything that might be going on outside of the company.

>> Maneesha Mithal: All right. Why don't we now turn to accountability, which David just mentioned? So let's say a company has policies in place, it's got collection limitation, it's got data retention, it's got just in time notice and choice. And let's say that, you know, an opt-out doesn't work. It has all of this inaccurate information about consumers. Oops, they retained data accidentally. What are internal mechanisms that companies can use to ensure accountability of these policies? Are there technical protocols that could underlie a system? Could technology help here? What are some other internal accountability ideas? Paula?

>> Paula Bruening: Sure. Well, I think this morning, we started to hear about some of those, you know, I think what underpins accountability is the fact that a company made the commitment to be accountable, and that it's got these internal processes and procedures to ensure that it's going to meet its obligations with respect to data. And key to that is making sure that everybody understands what those obligations are. So there was a discussion this morning about data tagging, so that you can get clarity around what obligations matched to what data. But I think that's only part of the equation when you're talking about -- you know, the protections within a company. I think that Drummond Reed talked about the fact that you can tag the data, but it doesn't necessarily mean that the policies that go with that data are necessarily going to be followed. So it's important to also have an educated workforce, some protocols that help you make good decisions about that data, some oversight within the company to make sure that whatever decisions that are being made are actually giving you good privacy outcomes. But I think what's also important to remember, is that an accountable organization is accountable even when the data is being processed by a third-

party agent or vendor, when it's being shared with a business partner. There's got to be due diligence on the part of the company that those obligations that go with the data, that they're understood, and that also, the recipient of the data is in a position they can actually meet those obligations. So, you know, this is really -- and also, there's got to be some opening of the curtain, this isn't an interior monologue. You've got to have -- these processes and procedures got to match up to some external criteria. So it's an internal process, but there's got to be an openness to the outside for oversight and enforcement.

>> Maneesha Mithal: Richard?

>> Richard Purcell: Well, certainly, accountability has to be supported and implemented with administrative, operational and technical controls. If there's part of that formula missing, then you don't have -- you can't establish that accountability. One of the contrasts I want to draw here is that when we talk about the accountable organization, we begin to contrast this with an earlier discussion around user control, and there is again this sense that there are these monolithic or unilateral kinds of silver bullets that are available to solve this. And user control is oftentimes put forward as one of those. But although user control of personal information, your control over your own personal information, is important, it's not a reliable way to provide privacy protections. I don't know what user control would have helped the people who shopped at TJX stores when they lost all of their data to a hack. Nothing would have helped. No spyware detector or intrusion detection on a user's basis would have helped. So an accountable organization needs to be matched up to, as a control, to individual user controls over personal information, as well. That had to be collaborative, because this really comes down to having an information sharing agreement between an individual and an organization. And the organization, in taking on that responsibility, has to be serious about it, use administrative controls, operational controls, technical controls, in order to do so. As an example, we talked earlier about the need to encrypt e-mail that has personally identifiable information in it. Well, fine. But it's not done. It's not done on a user basis. It's not done on an organizational basis very often. Most data is sent in the clear using e-mails, even from corporations. Although it's generally a policy, or an aspirational policy, to prevent spread sheets to being attached and sent, you know, outside of the organization, and files to be carried around on laptops. But we all know that that's not how it works in the world. We have a long way to go, not

only to creating the accountable organization, but also to understanding what these controls really mean in a way that actually liberates the service delivery, in a way that gives us the promise that the information age is actually going to do us more good than harm.

>> Maneesha Mithal: David, last word on accountability?

>> David Hoffman: Yeah. I'm actually really excited about the potential that accountability has to deliver real privacy protections for individuals as we explore it more. Marty Abrams and Paula from the Centre for Information Policy Leadership, I think, have been true visionaries on this, of recognizing that there hasn't been a lot of detail and specifics about what does it mean to be an accountable organization? Even though accountability has been one of the Fair Information practices for over 30 years. And I think if you ask people from organizations, "do you work for an accountable organization?" They would say, "absolutely, I do." And then if you drill down and you ask, "okay, so you have a person who's clearly in charge, you have clear, delegated authorities, you have adequate staffing, you have a training and awareness program, you have documented issue management process, you have clear, individual participation processes. It's all documented and you can provide it to me and could I read it and understand it?" And very few of them, at this point, I think, would say yes. I mean, leading companies would -- a lot of companies would, in this room, probably would. I think the good news is that people are starting to drill down on this now and try to define it. Folks in industry, along with regulatory participation, are starting to explore it. I also think, you know, there's a lot of -- we have a lot of guides from other compliance operations that we can look to. You know, financial reporting, environmental compliance. There's a lot of other reasons we need to run accountable organizations. I want to say, one of the things I'm most intrigued by -- Accenture, I know, designed their entire processes around the seven standards of the Federal Sentencing Guidelines. And when I found out about that, I thought, "that's perfect." Because what we really ought to be doing is running an accountable operation so we can clearly communicate it to CEO and our and General Counsel, in line with other obligations we have to be an accountable organization. So I can't say enough about how important I think this work is. And to have regulatory participation in deciding that -- what the definition of an accountable organization really is.

>> Maneesha Mithal: Okay, I'd like to circle back to a concept we talked about a few minutes ago. There seems to be a fair amount of consensus on the panel that there's a role for informed consent here. And we talked a little bit about just in time notices. What I want to follow up on is ask, is there a role for standardization of this process? In other words, is there a way we could take the burden off the consumer to try to digest many different kinds of just in time notices? Is there a role for standardization? Commissioner?

>> Jennifer Stoddart: Sorry. Informed consent does not mean, in my jurisdiction, a whole series of complicated notices. You are not informed and you cannot consent if you cannot under a reasonable person, not necessarily with an university education, whatever, cannot understand what they are consenting to. So informed consent is inimical, then, with a whole series of explanations that, you know, most people will just glance over. We know school psychologists, for example, psychologists in Canada have shown that, you know, there's a natural tendency just to go on. You don't read this stuff. So you're not really consenting, and you haven't been informed about what you're doing. So at a minimum, it's about going back to plain language. What is really happening here? And who talked about something that could just be, you know on a cigarette package? It was Fred, yeah, you know. I saw it in the airport recently in France -- "cigarettes kill," it said. Never seen that before. I don't know if this is the French approach, or what? I haven't been looking at cigarette packages or something, but I thought, "oh, boy." You know, that is clear.

>> Maneesha Mithal: If I could just follow up. I think, though, isn't there a difference between "cigarettes kill" and privacy, which may vary from business model to business model, and, you know, consumer preference to consumer preference. Does that create a complication here? And how do we address that complication?

>> Richard Purcell: Well, it is complicated. I mean, technologies -- not the technologies themselves, so much -- but the models that technologies are used to support today can be extremely complex. And a simple explanation is not going to be usable, because it's going to hide more than it's going to reveal. At the same time, we talked earlier about the concept of little, middle, big. Okay. So one of the things that notices today are used for, of course, is to cover liability, as opposed to expose real decision making. It's entirely possible, if we help, kind of, lessen that

liability burden, it's entirely possible to say, "look, here's the best-case/worst-case scenario for this condition." And, you know, you can have the little condition. You give me your e-mail address, I'll give you these services through e-mail. The worst case is, I don't know, that I'll spam you or something like that. The middle case may be -- worst -- one of the things that people don't understand, and companies will not reveal, is what's the worst case condition of you giving me this information? And it would help people to make an informed decision if they understood better. What could be -- what could go wrong here? And, you know, frankly, we could lose your data. And that could be bad. Now, we prevent that by implementing these procedures. It gives a context for the ability for an individual, a reasonable person, to make a decision. And isn't that the reason we're supposed to be giving notices? To have informed decision making?

>> Maneesha Mithal: Fred?

>> Fred Cate: I rarely disagree with Richard, but I think he's out of his mind. This will be like drug labeling. You know? You'll lead the 65 complications you'll get from using this drug, and upon we all know that people still go right ahead and take the drug, anyway. So I think we need to be extraordinarily cautious here. Frankly, and again, overvaluing the role of consent here to start with. So one possibility, and -- this may be a lousy possibility -- but would be for the Commission to think about identifying a sort of default scenario. To say "look, if this is what you are doing, you owe no further disclosure and there's no need for further consent." So if you're only collecting data to complete the transaction, and you're only going to retain it as necessary for the completion of that transaction, you don't owe the consumer anything else and you're going to use appropriate security. And there's no consent there, there's no additional notice, there's no -- I know I'm filling out the form. I don't need a pop-up notice saying "you're filling out a form now." You might remember that disastrous road we went down of the first version of the HIPPA notice, where we were going to get consent to use information provided for treatment. Like I was going to go in and tell my doctor something, and then be shocked if my doctor actually relied on it in treating me. And cool, calmer heads prevailed and we finally got that taken out. But I think one thought would be to think about, are there default, maybe multiple defaults in different scenarios, where the Commission could identify through research or through rulemaking, or whatever, a process of saying "this is what consumers rationally expect here." Don't bother telling us about it if you're just

doing what you already expect. That might also increase the pressure, if you will -- that's a slightly stronger term than I would like here -- on data collectors to say "do I really want to do something else? Do I want to retain the data?" In which case, I now have to do something else. I can't just use the default.

>> Maneesha Mithal: Commissioner Stoddart, I'm going to give you the last word on this. Was your tent up?

>> Jennifer Stoddart: Well, it was. When Fred said we're relying placing over reliance on consent, he was partly right and partly wrong, if I can say, just to get something going, yeah. We do have different kinds of consent, and the example we're talking about is implied consent. So, you know, it's not an elaborate, formal, highly logical process every time. But the basic principle is, yes, I agree, but it can be implied from your actions at the time that you're giving information.

>> Maneesha Mithal: Okay. We have about five minutes left on the panel, and I would just like to wrap up with a question to all of the panelists. And if you could take a minute or less to answer this question. The question is now that we're at the end of our Round table Series, what should the Commission do next? So let me just go down the line and start with Paula.

>> Paula Bruening: I think that going forward, the commission should heed what it's probably been hearing for over the last three roundtables, and not use notice and choice as the starting point for the discussion. I think it's just becoming increasingly clear. That's not to say you look at Fair Information practices, because, obviously, you do. But I think going forward, the exercise needs to be how do you make Fair Information Practices work in the world that we've just described today? How do you make them work in a really dynamic environment where there's massive change, incredible amounts of data, less and less ability for the individual to exercise the kind of control that might be envisioned in the 1970s? But I think the frustration is always that the conversation keeps starting back at notice and choice, when that isn't really the starting point anymore.

>> Maneesha Mithal: Fred?

>> Fred Cate: Thank you. Commissioner Stoddard described that in good data protection as a whole framework. And I think that is a very important concept and one we might keep in mind when thinking about ways of moving forward. So if I had to identify an objective here, it is to have organizations or individuals who collect and use data to feel appropriately the burden of what they're doing, so that we don't regard it as a costless activity of the organization, but it may impose very significant costs on individuals. There are a lot of ways to do that. Law is, I think part of that for helping the organization feel the cause. But I think the way not to do it is to shift all of the cost back to the individual by saying, "let's just ask you for consent". If you go along with it, we can do anything damn thing we please.

>> Maneesha Mithal: David.

>> David Hoffman: I agree with just about everything Paula and Fred said, except when earlier he said Richard is completely out of his mind, which he may or may not be. I think what I would recommend is, I do like this idea of going back and looking at what are these sets of fair information practices and not going down the road that others have gone on, down to as saying, let's have really detailed regulations that we're going to write specifically about how to manage and impose things. But instead creating some ability for some interpretation and flexibility on the enforcement of those practices as we move forward. I think your question about standards was a good one earlier. Because I think then, standards is an interesting question. -- phrase, because the technology community you say standards, and we take international standards organization, technical standards sitting around tables for about three years, before we agree on something that we can all agree to, and that has great interoperability, increased functionality. I think if what we mean by standards is more best practices that we bring people together and define some recommendations about what the interpretation of those fair information practices should be that could inform really robust enforcement action. And that that practice when you include academics and industry and advocacy groups and regulators, that then makes a lot of sense to me.

>> Maneesha Mithal: Chris.

>> Chris Jay Hoofnagle: So I keep on saying look back at 1996 report, where Beth Givens said the FTC no matter what it does should create metric for outcomes, for its approaches. So if it's self-regulation creates a metric so you can review the outcomes. If it's legislation create metric. One area where you have metric is adoption of privacy policies. The Federal Trade Commission created an atmosphere that caused companies to very quickly adopt privacy policies in the 1990s. We went from 20% to almost 100% probably today. Now, the harder question is, how do you build substance into those policies? It seems to me that the market really isn't functioning to create substance, because competitors are not rewarded for privacy by design or for privacy enhancing technologies. In fact there's a lot of free riders that claim they do things like anonymize their search logs. And they really don't. And their competitors are investing serious research, and money into true anonymization. And they are not awarded for that. And it seems to me that the Federal Trade Commission could do a good thing for consumers and for competition by beginning to police the free riders who are claiming to do things that are really laughable upon deeper analysis.

>> Maneesha Mithal: Richard.

>> Richard Purcell: For me without any disagreements from the prior comments, there's a balancing here that I think is important. And deferring to the fact that our hosts here are the Consumer Protection Bureau, this is not necessarily or unilaterally a consumer-based society. We're also citizens. We have a certain amount of shared human dignity that is important to respect and try and figure out. It's not all about consumers or users or any of these euphemisms we have to describe people who are carbon based life forms. The other part of it is, I believe that that should lead us to a little more cross cultural sensitivity about what the whole world is like. Not just the idiosyncratic American approach is, that we have to begin to think a little more carefully not to go down the prideful kind of data as personal property consumer protection exclusively path of privacy protection but expand that and accept the fact that the world has different concepts of that and different approaches and at least let those influence the inputs and our thinking on this.

>> Maneesha Mithal: Commissioner.

>> Jennifer Stoddart: I don't think it's up to me to tell you what to do next, but just from the outside looking in. The FTC is a world widely respected organization. And there are a lot of hopes put in the FTC's initiative in the area of data protect. Outside of the United States, we're all affected now by products and technologies that wash over us. Sometimes independent what our individual laws are. That's a huge challenge. So we're looking for some action within the United States, I'll just refer you to Pamela Jones Harbour's comments. Those would be places to begin.

>> Maneesha Mithal: John.

>> John Verdi: I think we're at a point in 2010 where the FTC does confront hard cases sometimes, in the consumer protection context. But the commission also on occasion confronts very straightforward cases. Cases with straightforward violations, straightforward bad actors and I would encourage effective enforcement on those cases. What effective enforcement means to me, in this context is a prompt response to consumer complaints about a business practice. Decisive action on the part of the commission, and penalties that are proportional to the violations. And I think that that would go along way moving forward in the straightforward cases, help consumers.

>> Maneesha Mithal: Okay. Thank you very much. Thanks for the panel and thank you to Katy Rattay and Katy Harrington-McBride. And if you could stay in your seats for a little while longer we have Jessica Rich, who is the Deputy Director of the Bureau of Consumer Protection, and she's been a leader at this agency on privacy issues for the past ten years and Jessica will deliver some closing remarks.

>> Jessica Rich: Am I shutting off the whole system? I hope not. Before I make some brief closing remarks, I just want to thank everyone who made this event happen. First, the excellent FTC staff that put it together this event so quickly after a second round table. In particular, Loretta Garrison, Katy Harrington McBride, Naomi Lefkowitz, Manos Moapatra. Where's Manos, is he still here? There he is. Katy Rattay, Michelle Rosenthal, Randy Fixman, Chris Olsen. So thank you. And I want to thank all of the panelists here, panelists and audience for staying interested, staying here. Look you're all still here. And helping insure such a comprehensive, relevant and focused event in all three roundtables. In closing, I'd like to just talk briefly about the next steps in

this process, and the issues that we're going to consider as we move forward. It's sort of hard to talk to all of you. As you know, we've had three remarkable round tables full of ideas and observations. Some old, many new. Our panelists have included many of the nation's privacy leaders. Many other nations too. I can't see Jennifer from here but I know she's there. We have many thoughtful comments to read, and I want to remind everyone that the comment period stays open until April 14th. So if you have some good points, especially after this great discussion, please send in your comments. We have some really, really -- despite all these excellent suggestions for what we're going to do next, we have some really really difficult issues to grapple with, as I think you know. We get just how hard they are. I thought I would just count the ways. I mention a few of the challenges and tensions we're dealing with as we work through these issues. So we want consumers to have greater control. Recognizing that they really don't want to spend time reviewing privacy policies, even short ones. We want to distinguish between data uses that raise privacy concerns, truly raise privacy concerns and those that don't that are benign uses recognizing that privacy preferences may -- are likely to differ across different individuals and that hard lines they may be very difficult to draw. We want to protect privacy without stifling innovation, in a marketplace that clearly has been using data, personal consumer data to create products that many consumers like, products and services. We want to accommodate the incredibly diverse business models and privacy concerns that exist today and that may be developed tomorrow. Online retailing. data brokering, mobile devices, social networking, cloud computing, behavioral advertising, online radical information, identity management, location services to name a few. We talked about more today than that. And we want a relatively simple framework so that everyone can understand the norms and the expectations. And we want to improve on the current privacy models while building on and not undermining the progress that has been made under those models, and supporting and not stopping the valuable privacy work that's under way right now. We've been encouraged, for example, by the steps that industry has taken into -- in response to our call for greater transparency and consumer control and behavioral advertising. I should add it's not done and you keep working on it. We need to see how it turns out, but we want that work to continue. And we have ongoing projects, and commitments with international partners to coordinate enforcement and policy development, for example, in APEC, which commissioner Harbour, who spoke to us this morning as led. These efforts can be a delicate process. We don't want to preserve them and pull out of them. Despite the cleared short comings of privacy policies

as a consumer tool they've been instrumental in promoting accountability among businesses. Many of us remember it wasn't long ago when there were no privacy policies and no commitments made about how information would be used so we want to preserve, somehow harness that accountability while figuring out a better way to communicate with consumers about the kinds of uses and choices they have. So clearly, none of this is easy at all. And -- but, we think it's worth it. Discussion at these round tables and especially the last comments that were just made told us loud and clear that the dominant models, really haven't kept pace with the wide range of business models, and data practices that are in today's marketplace, which is evolving, you know, every day. So we had a lot of work to do. In terms of how we get that work done, we intend to continue the collaborative process that we've launched with these round tables. Given the challenges that involved it, we aren't about to just pop out a new framework tomorrow. We have these round tables and let's propose this new framework, fully formed and ready for implementation. Instead we're going to take some time to think about what we've learned here, we are going to be reviewing the comments and then, you know, we're going to get our thinking together and likely, as we've done in prior processes, we're going to put some thoughts out for public comment and get more input once we focus the issues a little more. In the meantime, we may reach out to some of you in particular to ask you to elaborate on some of the comments you've made here or some points that have come out. We really continue to appreciate your help with this immensely challenging but extremely important project and we look forward to continuing work together. So thanks again for coming and we'll keep talking.

[Applause]