

>> Catherine Harrington-McBride: Good afternoon, everyone, and welcome back from lunch. For those of you in the building, I'm glad to see you back and in your seats. And for everyone on the webcast, welcome, as well. My name is Cathy Harrington-McBride. I'm a staff attorney with the FTC, and together with my colleague, Michelle Rosenthal, we will be moderating this afternoon's panel exploring the treatment of sensitive information. Just a quick reminder, we will be accepting audience questions. If you're live in the room and would like to raise your hand with one of the question cards, one of our folks will come around and collect that and provide it to us. If you are out in webcast land, feel free to send an e-mail to [privacyroundtable@FTC.gov](mailto:privacyroundtable@FTC.gov). In this morning's panel on health privacy issues, the question of sensitivity of health data, however that term might ultimately be defined, was at issue. This afternoon, we'll take an even broader look at what constitutes sensitive information for privacy purposes. We'll examine the core characteristics that make data sensitive. We'll look at some of the challenges to defining sensitive information. And we'll discuss whether such data should be subject to particular restrictions. For example, collection, use, sharing or disposal restrictions. I know that the first panel after lunch is often a difficult one. For those of you who may have carb loaded, as some of us did in the green room. And so for context clues, let me let you know that we're going to split this into, basically, two halves. The first half of the discussion will focus on definitional issues and challenges, and the second half, we'll look at potential remedies for some of the problems we may be able to suss out. We feel compelled, Michelle and I, to let you know that our sartorial sameness was not intentional, and we also both apologize for not wearing Kelly green, and we thank those in the audience who are wearing green today. I'm delighted to welcome our excellent panelists, who will help us sort out these issues today. And I'll briefly introduce them before we begin. To my left, we have Parry Aftab, who heads WiredSafety and WiredTrust. Next is Anita Allen, a professor at the University of Pennsylvania. Next to Anita, Pam Dixon, Executive Director of the World Privacy Forum. Next, Jim Harper, Director of Information Policy Studies at The Cato Institute. Next to Jim, we have Kathryn Montgomery, a professor at the American University School of Communication. Next to Kathryn, we have Lee Peeler, President of the National Advertising Review Council, Council of Better Business Bureaus. And finally, last but not least, we have Lior Strahilevitz, from the University of Chicago School of Law. We are so grateful to each of you panelists for coming to talk about this difficult issue. It's not only difficult, but it is amorphous. And so, we have our work cut out for us. In our calls with our panelists, you all will recall -- and I'm clueing you all in, since

you weren't on the call. In our calls with many experts that we interviewed in preparation for this, and even in and research, we learned that achieving consensus about how one might go about categorizing data as sensitive, is maybe a tall order for a 90-minute panel. When you factor in the diversity of opinions about how you might bound a definition of each of these types of data -- well, you remember the challenge of doing that in just one context, health information, this morning. So our goal today is really to focus on the characteristics that make data sensitive. To talk about extracting the rule, about what is it, really, at its core, that makes something sensitive. To talk about those things, and in particular, in our conversations with panelists. What we've learned is that mostly, what it seems to come down to is, the propensity of certain information to cause particular harm. And so we wanted to focus the first part of our discussion today on some of those harms, and we thought we would start with the propensity of information to cause physical harm. So physical harm is a concrete and cognizable form of harm. We all know this. This is intuitive and obvious. If data, such as location information, could be used to subject a person to physical harm, should it be considered sensitive? And to start, why don't we go to Parry?

>> Parry Aftab: Thank you. If somebody can find you, they may find you in real life. So, as we start looking at these issues -- at Wired Safety, we deal with cyber stalking, cyber harassment and cyber bullying. So, if someone knows where you are, they may show up at your door. We've seen a lot of situations where kids have been targeting someone who is black onto a white supremacist website, harassing them, in the name of a black student, saying, "if you don't like it, this is where you can find me" -- name, address and telephone number. And people show up at their door. We're also seeing some cases of breaking and entering, where someone shows up at your house when you have Tweeted about this great vacation you're going on for three weeks. So where you are and how various devices, and where sharing that information can be used to hurt us, is something we're just starting to learn.

>> Catherine Harrington-McBride: Any other thoughts about that? Jim?

>> Jim Harper: Well, sure. I think personal security is an important privacy value, if you will. Something that may be, you know, may not be in your best definition of privacy, an aspect of privacy. But I don't think you can follow the train of logic, the information that could be used to

physically harm you, sensitive information. Think about how that explodes things if you just take some of the notable examples, like the murder of Rebecca Schaeffer, for example, which used address information. Are we going to make address information sensitive information, subject to special controls, when address information is constantly shared with all kinds of parties, for lots of good reasons? It would just sort of expose sensitivity go to in that direction. Obviously, personal security is an essential value. Harms to personal security are serious harms that need to be reckoned with. But it doesn't follow from that, that data that could be used to harm you is sensitive.

>> Catherine Harrington-McBride: Lior, the question about whether public information that is something like address that is widely publicized can be sensitive might be one that I would pose to you. Is that something that we should -- if we're going to look at this as a harm's-based model, can we go as broadcasting that is broadly as, um, you know, address, or are we going too far there?

>> Lior Strahilevitz: Well, with address I think it is somewhat complicated in that individuals can elect to have a listed or unlisted address. And so there may be a consent model that works reasonably even with the old-fashioned "White Pages." Which, I guess, nobody uses anymore. Although, there remain "White Page" analogs online that people are presumably using. On the broader question, though, I do think that in terms of figuring out what information is sensitive that - - Jim's right. That privacy may be a -- in 99% of all cases, a necessary aspect to the definition of sensitivity. In other words, it's very hard to come up with cases in which information is public, whatever the meaning of public is. Some people would like that meaning to be broad, some people like it to be narrow within privacy law. The meaning of what's private looks very different, in say the privacy act versus -- privacy provisions versus, say, New York tort law. But I think as a general rule, if we're trying to think of clear principles that might help us inform this debate, if it's truly private, then it may be sensitive. If it is public, it's very hard to construct a theory as to why it's sensitive. Very hard to construct a theory, I think, as to why it's harmful if disclosed. So, HIV status from the last panel we know is almost always extremely sensitive, it's extremely damaging if disclosed, but to disclose Magic Johnson's HIV status no longer is harmful to him. You might describe that information as no longer sensitive and indeed -- for some of the reasons I think Jim was alluding to, there'd of course be significant First Amendment constraints on any efforts to clamp down on discussions, of the HIV positive status of someone who was well known for being

HIV positive. John Edwards' extramarital affairs -- right, we can come up with a number of examples in which the information that's so widely known by the public, that even though the subject matter makes us think it's sensitive, the scope of the disclosure means that it no longer ought to be so, at least for these public figures.

>> Catherine Harrington-McBride: Jim?

>> Jim Harper: I would just add that even outside the realm of public figures, there are people, there are communities who broadcast their HIV status through tattoos and things like that. There are many, many subcultures in our society that treat information that could be highly personal, highly private to some as public to others. So, it's really subjective, that's the problem with broad definition.

>> Catherine Harrington-McBride: An excellent segue. Subjectivity is obviously an issue here. It comes down to the difficulty of figuring out when a particular individual might have a subjective desire to safeguard some information. Kathryn, could you speak a little about this in the context of your work, particularly with children?

>> Kathryn Montgomery: First of all, you know, this notion of defining sensitive information, only on the basis of harm, makes me a little uncomfortable. I think it sets up a certain high level of expectation there I think we may be able to talk about kinds of information that we all agree are sensitive without being able necessarily to identify harms. I think it also may have to do with what individuals choose to disclose as what you're saying. I think we may want to talk about that. I was involved in the 1990s with the FTC and Congress in passing the children's online privacy protection act. That law acknowledged that children are sensitive, what I would call sensitive users, and that is -- that law applies only to children under the age of 13 too, by the way. But that the information that they disclose, and the information that is collected on them, is, by definition, according to law, sensitive information. And I think that continues to be an issue. I've been looking recently at the role of adolescence in the new media environment. And I think particularly when you look at social networks and the kinds of information they voluntarily disclose as well as what is gathered on teens, at an age when many of them are not necessarily turning it at the age of 13 into

the wisest young people, depends on the kid, obviously, they can sometimes put themselves in harm in many ways and there certainly have been examples of that.

>> Catherine Harrington-McBride: Pam in the context of one particular group. Victims of Domestic Violence. How does this play out? I mean, obviously, there's a very real risk of physical harm in that case even from the release of information that might, by other people, be considered very public address information. But which victim of domestic violence might be striving very hard to safeguard. How would we have to treat something like that? That very particular instance?

>> Pam Dixon: Right. It's a good question. I think one of the things that's pointed out by the conversation so far is that the issue of sensitive information is an issue dealing with borders and borderlines and how incredibly difficult the borderlines are here. So, let's start with public information. So you have a victim of domestic violence who, prior to the relationship that was problematic, published their address information, and other locational information without fear of any consequence. And so, they, themselves made it public or allowed it to become public for whatever reason. And then after, you know, a difficult situation, then their situation changed. So now you have information that's in the public realm. And information that can in fact, potentially harm that person. Or, let's say they've gone to great lengths to then move or somehow change their status, so that now, the new location information or address information is now private. That information now is sensitive to them. So what you do in that case, you have public information for some people, and private for another. And this leads to what Katherine was saying about sensitive users. I think it's fair to cordon off some categories of individuals as sensitive users. I would also suggest that individuals who have various kinds of challenges that would, for example, diminish their ability to consent or to make meaningful decisions about what constitutes sensitive information. That would be a challenge, the very elderly individuals with mental challenges, et cetera. But something worth thinking about further here is the borderlines, and you can really see this in health information as well. So, an individual has a health condition for which they need to borrow money to pay. Let's say HIV aids status. Or even a cancer treatment, they need to borrow \$10,000 for treatment. They go to the bank and they get a loan for this medical treatment. So, here's the question. Is that medical data? Is that bank data? What laws apply here, and what protections would apply in terms of data sensitivity, because this is -- as soon as you try to save it,

for example, medical data, or, you know, victims of domestic violence data is sensitive. All of a sudden, you know, it gets very messy, because it all starts to spill over the borders. So then you come to -- you arrive at a position of, "Well, does the protection travel with the data." And then that helps you through the border issue, unless you have a Victims of Domestic Violence situation where your status could change. So this is -- what I am saying is this is a very complex, very messy issue, and I don't think there are any easy answers here. And I think that because of our sectoral system, we have quite a pickle in trying to solve it.

>> Catherine Harrington-McBride: I think, "Fair enough." And yet, we still have the good hour and 40 minutes left. So, we're going to keep at it. Don't anybody get up and go now. Please don't move your chairs. But Pam is right. We've been in deep on this now for six weeks, Michelle and I, talking with these panelists who have been extremely generous with their time and a variety of other experts, some of whom are in the room. And it really is. I mean, it's "Alice in Wonderland." You're down one rabbit hole and then you're into the next. I want to go back to the location issue. We moved very quickly from location to address. And of course, address is very public and widely known. In our second privacy round table at Berkeley last month, I guess now it's a month and a half ago. We talked about the issue of location tracking. And that's different than address. That's where I am now. This is not my address, but it happens to be where I am. I'll be some place else tonight. Hopefully all of you will be too, celebrating St. Patrick's Day. And that information is different, isn't it? And so, Anita, tell us a little bit about your thoughts about the sensitivity of that information, vis-à-vis, individuals who may or may not have any subjective issues with their privacy, but how does that play out, and not only their specific location but location tracking over time. What are the concerns there?

>> Anita Allen: Well, one striking thing about your question is that, I think if you ask the average person on the street, what are the major categories of sensitive information, they wouldn't say locational first. They'd say, "Oh, medical, financial, educational, sexual." They might even say sexual orientation information. And they might even say race and ethnicity information. But Locational information is sort of a new way to think about a kind of information which we might regard as sensitive. And one area in which locational information becomes very important is in the area of criminal justice/criminal procedure. Often times, we don't want people to know exactly

where we are, because we're doing something we shouldn't be doing. And public policy makers may want to fight public policies that make it harder for law enforcement, national security to get access to locations, precisely because it's the bad people who are gonna care the most about others not knowing where they are. And yet, all of us, no matter what we're doing, when we're baking cookies or making crack cocaine we don't necessarily want the world to know exactly where we are at a given moment. We might be having a secret rendezvous. Again, we might be just making cookies. So, I do think that there's something to the idea that we need to treat locational data as a category of sensitive information. Not perhaps as sensitive as a person's medical records, but pretty importantly protected.

>> Catherine Harrington-McBride: Lee, do you have any thoughts about the tracking of location data over time, not just where I am now, but the amalgamation of a pattern of movement for an individual. And whether that poses challenges or should be treated differently than individual points where a person might be at any given time?

>> Lee Peeler: Yes, I do. And also it seems like just, you know, the framework what we're trying to do here is talk about where information is more sensitive than ordinary information. And, you know, as you said, it's very contextually driven. And, you know, this type of discussion that the FTC is leading, I think is extremely valuable in looking at sort of evolving issues like location information. And trying to basically analyze to what we've done in the past. Katherine made a really good point that one of the first areas that we've looked at a while ago actually was kids information, and there were really two issues that drove that. One was risk of harm, which is what we're focusing on now, but the other important issue, in the kids' area was the feeling that young children just couldn't appreciate the trade-off that was involved or the risk that was involved in disclosing Personally Identifiable Information over the internet. So, you had those two factors coming together to establish a higher level of protection. And I think, if you're analyzing location information, you have to follow sort of that same approach, all information should be accorded fair information handling practices. There are lots of people out there that make their location information known, you know, widely. On Facebook, and people tweet where they are and where they're going and things like that. So establishing sort of a broad category that says all location information is sensitive, I think it's likely a step too far.

>> Catherine Harrington-McBride: I think you raised some really interesting points. I'm going to come back to you, Kathryn, really quickly here. But when you mention this sort of two-part analysis, that there's both a risk of harm and an inability on the part of the individual to meaningfully consent. Either they're under the age of consent deemed by law or there is some other factor that prevents them maybe from being a full participant in this transaction. Maybe we should go to the example of the prevalence of self provided data in location tracking. We all know that many people do it, Lee has enunciated this principle. And we all know it from our friends, we see where they are and where they've checked in and what they are the mayor of. That information though, that's self-provided. And so, by one argument, maybe Lior would say, "You know, this is-- you've made that public and you've told everybody where you are and that's your choice and you're broadcasting that." And one question that might come about is, "What about secondary uses?" So, many of you may have seen in the media recently, the pleaserobme.com website went up and it aggregated location information from Foursquare and Twitter and other places where people willingly provide their location. And the idea of the website was to say, "Well, these people are not at home, so if anybody would like to pop by and maybe grab a new TV. Now is the time." And so the question becomes, "What about secondary uses of this information?" Even where information is self-provided, is there a deep enough understanding on the part of the populous using tools like this, about the potential risks for either amalgamation of that data with something else or just repurposing of it? Kathryn, I wanted to get you too, but --

>> Kathryn Montgomery: One thing I wanted to comment on, because thinking back to COPPA is like thinking back to ancient history when I remember the research we did on kids and the fact that they were being asked questions, and filling out questionnaires and volunteering the information. And while a lot of that still happens in the digital media, a lot of what we're talking about here, and I'm glad you raised this broader issue, is more behavior targeting and behavior profiling and data collection, that's happening in a much more automated and passive way where we're not thinking, "I'm going to volunteer this information about where I am." So example, with Mobile Marketing. The whole growth of location based targeting is based on the fact that these technologies are capable of tracking where we are. So, we're not really thinking so much about every instance of what we're doing. Nor do most consumers, I would argue, fully understand the extent of data

collection in behavior targeting in today's contemporary digital marketing environment. The other thing is, talking about sensitive information in discreet terms, I think obscures the fact that another issue you raised that it's really the ability of these technologies and these applications, and the marketing practices, to amalgamate, to bring together, to converge all of this information, some of which you may have volunteered, consciously, much of which you didn't, and to -- packets of information about you in profiles on you, that you have really no idea has happened.

>> Catherine Harrington-McBride: Okay. Pam?

>> Pam Dixon: Thank you. I think it's a -- I'd like to kind of add on to, accrete onto what Katherine was saying. If you take, for example, the idea of a person who has their mobile phone on at a physician's office. That location information can easily be used in other ways. Something that certainly comes to mind is some of the digital signage issues. So, for example, just a few weeks ago, I ran into a digital signage vendor that has a digital concierge project that once you interact with it with your mobile phone, if Bluetooth is on, then they get your Mac address and then they target ads to you based on that information. This is all done with a kind of passive consent because you have Bluetooth on, right? So this information, taken by itself may not cause harm, but if you accrete this information over time and layer it with other bits of data, does this information become sensitive? If this information is, for example, tied to a physician visit, or something that could be construed as sensitive? So the whole idea of sensitive data in what context? And sensitive data -- or data -- little bits of data that become sensitive, when combined with others, I think is a very difficult and challenging concept, but one we really do need to grapple with because I think it's very tempting to look at data as individual units or pieces, but that's really not how most folks work with data anymore. Most people have really nice computers, and really nice systems that can crunch and munch a lot of data, and I think we need to think about that context as well.

>> Catherine Harrington-McBride: It's a Monet, and we need to stop looking at the brush strokes. Is that what you're telling us?

>> Pam Dixon: Absolutely.

>> Catherine Harrington-McBride: Parry?

>> Parry Aftab: I'll address your question.

>> Catherine Harrington-McBride: Thank you.

>> Parry Aftab: Whenever I'm asked about sensitive information, I break them into two pieces. One is kids, cash, and kidneys. Children, financial, and health. And in the United States, that's where we tend to regulate. Those are the things we care about, whereas in Europe, they care about trade unions, and a lot of things that in the United States, we don't consider sensitive. I also identify vulnerable groups, or vulnerable users. Those who are more likely to be targeted because of who they are, whether it's sexual preference or racial background or ethnicity or age or you're the victim of crime. Those kinds of things are more vulnerable. When one touches, once you get into a vulnerable group and it touches data that otherwise, might not otherwise be sensitive, like King Midas, it turns it to gold. So when you take location information, that might not be a problem, if it's in the white pages or yellow pages or some kind of thing that you can look up. But you're now dealing with a victim of violence. And she's trying to hide where she is or hide the kids. It now becomes sensitive. So, how do we, in secondary uses, know that information that we might not have considered sensitive, is now made sensitive because it involves a vulnerable group member. And that's part of the problem. I think as we start to look at this, we need to create higher burdens on the people who are going to use it for secondary use. And I think this is the FTC. I think commercial use is something we can do a lot more about than we can individuals or just saying a lot of hateful things that may be covered by the first amendment whereas commercial speech may not be. So I think that as we're looking at secondary uses and data miners and profiling and a lot of those things that are happening, and all you have to do is look at the front page of today's *New York Times* and see how little bits of information become a big mass of information. I think that we need to turn around and say to somebody, "For commercial uses, you need to know where it came from. And you have to be responsible for it." You can tie it -- tag it, using electronics, and I know we'll talk about this in the second half. But there are a lot of different things we can do. But I think we need to turn around and say, "If you want to use it for commercial purposes, and you're going to

start to combine it with something else, you have to know where it came from." So it has to have some type of authenticity. Some type of verification, otherwise it's hands off.

>> Catherine Harrington-McBride: Okay. Anita and Jim briefly. And then I think we're going to move on to our next type of harm.

>> Anita Allen: Yes, briefly, I totally agree with Parry and just wanted to add that you do have a -- this question of intersection, what happens when you intersect the vulnerable group with the information which is either inherently sensitive, or we might say it's inherently sensitive, and the information which is not really all that sensitive but when combined with a vulnerable group it becomes something we want to call sensitive. So I totally agree with that point. We have to think about the intersections of these bits of data. But I also want to emphasize that it's not just the question of what do individual people, who might be thieves, do with my locational data. And what do commercial actors do with my personal data. But I want to go back to government also. Because the government has access to our Amtrak travel records, and our airline travel records, all that locational data, all that data, which when aggregated, provides a portrait of our lives, it's in the hands of somebody not just commercial sector but also the government.

>> Catherine Harrington-McBride: Jim.

>> Jim Harper: Well, I think we run into problems defining sensitive data. There's more likely to be some traction in defining sensitive persons or groups but I'll throw some complexity into that. As a website operator myself, everybody should be one, I have comments on a site that I run called "Washington Watch.com" that run into hundreds per day, easily. One bill in particular has about 114,000 comments on it right now. And there's no way to manage that comment system other than trying to just automatically induce people to stop swearing so much, but I don't know in advance who a person is that's commenting on there. It is very open. It's a wide open system, anybody can comment with out identifying themselves. I don't know in advance who they are, what category they're in. I don't know whether they're telling the truth or not, when they say who they are or say things about themselves. I've seen, even today, someone say something about herself, about a domestic violence situation she's in, that'd be very stupid to say if you were in one, but I have not

way to adjudicate whether that's true or not. I have no way to adjudicate whether she's even a woman.

>> Catherine Harrington-McBride: And we're going to talk about some of those real challenged to businesses of implementation of any of the kinds of cures that we might propose, but to get back to the identification, maybe of the harms, we've talked about two other kinds on our calls, two primary types. One being financial harm that can accrue and I think that that one is a little more concrete and tangible than the other kinds and that is dignitary or social harms, the idea some data is sensitive because we simple don't want other people, or at least not broad swaths of people to know about it. And so, let's talk about those, maybe in contract to one another. Cognizable claims under law for both kinds of harms as we know, but when it gets to this data, may cause someone embarrassment or anxiety or social distress. Is there something that should be done about that? Should a system of regulation account for that somehow or is that simply too difficult to get your hands around in any sort of regulatory scheme. How would you deal with that, Lior?

>> Lior Jacob Strahilevitz: Well, so, I think one of the common misconceptions about the work that people who, legislator, regulator, hand down case law in information privacy cases is that the harms from disclosure are one-sided. And I actually think a sophisticated understanding of how privacy law works and what privacy law does, suggests that, with respect to financial harm, dignitary harms, there are often harms on both sides. So, let me provide one example to see if I can make that more concrete. All right, so, I think this fall under the stigmatization harm or the emotional distress harm. Let's think about criminal history information. There's been a huge move in nearly 50 states to publish information about crimes that individuals have committed. We know, because it's most prominent about the sex offense registries but California is now considering legislation with respect to animal rights abusers registries, arson registries are already on the books, burglary registries in some states,. All right, so what should the law do with respect to these sorts of issues? Well, there's obviously a harm to the ex-offender whose information is disclosed and who is trying to reintegrate themselves into society and that seems clear. What I think's less obvious, though, but equally important, and this is part of what makes these sorts of issues so difficult, is that not disclosing information harms other people, right? So, with respect to criminal history information, there's very disturbing, but actually extremely well done, technically, research that Harry Holzer,

who's here at Georgetown, has done, along with Michael Stoll and Steven Raphael. And they looked at the labor market consequences of criminal history disclosures and found that, in those jurisdictions where criminal history information is made most transparent, the employment outcomes of African American males in, let's say blue collar entry-level positions do better. In other words, in the absence of reliable criminal history information, employers for blue collar positions tend to assume that roughly all African-American males have criminal histories and then, as a result, refuse to hire them, regardless of whether they've got a criminal record or not. So, that's an interest in which, because of existing biases, because of discriminatory behavior, you're sort of caught between a rock and hard place, right? If you're interested in advancing the cause of racial justice, if you're interested in undermining this propensity of employers to punish African-American males, refuse to hire them, simply because African-American males, as a whole, have a higher propensity to have criminal convictions, then you might have a system of no privacy, or what people in this room might refer to as, "no privacy," which is complete transparency with respect to criminal history information. By the same token, though, if you focus on the marginalized population, the ex offenders themselves, and you look at the effects of the Megan's Law Registries, other registries, to try to create greater transparency for criminal history, you'll say, "well, there's an obvious harm to them, if this information is publicized." And so, I guess what I want to suggest by way of this, is that while it's very useful to talk about sensitivity, it's useful to talk about the propensity for harm and both financial harms and other dignitary and stigmatization harms, ultimately what the FTC is going to have to do and what lawmakers are going to have to do is confront these wrenching trade-offs. Right? These wrenching trade-offs because privacy law, inevitably creates some winners and some losers, and the government simply has to decide, in these cases, who the winners and who the losers should be.

>> Catherine Harrington-McBride: So that I don't take time away from the very important work that Michelle is going to do in just a few minutes, we're going to skip lightly over a couple of topics that we've actually spent a fair amount of time on, on the phone. And, I wanted to talk about one in particular. And this is somewhere along the lines of what Lior has been talking about, that there may be some value to publicizing data and we heard a little bit about this in the health information panel, robust databases can help provide meaningful research to be done in areas where we all may benefit. There may be progress in defeating disease if we have good information and yet, it does

come at a cost, there are real trade-offs. One issue that we haven't really talked a whole lot about is the risk that use of information in a way that individuals may find troubling will chill their conduct, will prevent them from reaching out, using these Web 2.0 tools because they fear that their information will be gathered and potentially used against them. Whether this is a real fear that would come to pass or not, this is the fact that their may be chilling. Would anyone like to speak to that issue? Jim?

>> Jim Harper: Well, it kind of should, shouldn't it? The idea that you should be able to put out information and not have consequences is probably mistaken. Individuals should be aware, that's the most important thing, understand what the consequences are. We don't know well enough, I think, with a lot of new technologies, a lot of new websites and protocols, but the important point is for people to be aware of consequences and act accordingly.

>> Catherine Harrington-McBride: Kathryn?

>> Kathryn Montgomery: Well I'd like to actually -- I know we already had a panel on health which, by the way, I thought was really, really interesting but, I'd like to talk about one area in health that didn't get much discussion and that's the way pharmaceutical companies are using the web and using digital technologies for direct to consumer advertising, some of which doesn't always look like advertising, and often it's in the form of, sort of unbranded sites that people might go to for information about symptoms and about illness and I know all of us have probably had experiences where we either come back from the doctor with the diagnosis that we have to first learn you how to spell and then learn more about and the doctor's given us information that's, you know, not totally clear or we have things we're worried about. And I think particularly, often with young people, sometimes these can be very sensitive areas. They could be sexual issues, for example, about sexual health, that they don't even feel comfortable talking to anybody about. And, the online environment is a terrific one. Internet is a great resource for information and I use it all of the time, and I'm sure we all do, but in many cases, you're not really aware of where you are and how that's being used and how that's collected and again, connected to other information. There's a whole infrastructure of companies engaged in this and people aren't aware of it. I agree with Jim. I think if they knew, then they should be very careful about it. But this isn't as if you're sort of

putting information out there, it's you're seeking information and your very process of seeking for information, then, is part of what's being collected on you.

>> Catherine Harrington-McBride: Anita.

>> Anita Allen: Well, I think it's often useful to go back to how we got the right to privacy in the first place and remember that when Warren and Brandeis, in the late 19th century, talked about privacy, they cited as the value behind it, the notion of inviolate personality, the notion of mankind having a spiritual nature. And, I think that in recent times, we've become reluctant to talk about those kinds of values in relation in to data protection and privacy but yet, I think it does help to -- help explain why people feel that, even when the data is out there in a public and accessible, that they expect their fellow citizens to have too much politeness and manners and discretion to actually use the data. I'm often surprised that my students will say, "Yes but just because I put it on Facebook doesn't mean that my employer has a right to use it." They assume there's kind of a social norm, which doesn't exist, actually. That people will just avert their eyes, as it were, to what they learn about you through readily available sources like Facebook. So, I'm just -- I'm personally quite challenged by trying to figure out, what do we do when, on the one hand, there is information out there, on the other hand, there are norms and shifting norms, which might say you're not allowed to use the information just because it's there. You're not allowed to use it just because you could get access to it. There may be sort of rules of demeanor and deference and politeness that keep us from exploiting information in the employment setting and other similar kinds of settings, that is there, just because it's there.

>> Catherine Harrington-McBride: This is Professor Helen Nissenbaum's Theory of Contextual Integrity, I think the idea that there need to be some boundaries around which people respect your decision to use information in one context but not hope that it's used in another, may be naive or aspirational, but, nonetheless, an interesting societal question. I have one other question for the panel and it's a toughie. We've talked a lot about the fact, throughout this roundtable process and even in this panel, about the fact that all kinds of information may be sensitive for some people and if that's the case, if the barriers and the distinctions between PII and non PII are blending and data can be reidentified, and there is this ability to take something that's seemingly innocuous to anyone,

maybe use it to access information that is not so innocuous about someone. Does this get us into a world where all data is, in fact, sensitive? Is it the Midas touch idea that Parry has touched on? Is that where we now are? Jim?

>> Jim Harper: Well, I think most efforts to define sensitive data probably do explode, that is, there's almost no barrier because of contextually and subjectivity. What it brings you to is an alternative way of addressing these problems, which is to focus on the harm that can be caused and then require whoever has data to be responsible in use of it, and so go to something like the public disclosure of embarrassing private facts tour, where you can get data, you can do anything you want with it, provided you don't cross this line where the law defines a harm. And so I think defining harms, and saying, "Do all you want to do without causing these harms," is a more productive way of looking at things. It's more likely to allow innovations to occur. We can't now predict what future uses of data might be. It's interesting to note, I think that, almost ten years ago. It was in May of 2000, the FTC came out with its report, asking for legislation around notice, choice, access and security. And reading that over, you realized that this is before Google, it was before Facebook and Twitter, Foursquare and everything else. If these rules had gone into place, knowing what we knew then, would we have gotten those things? It's easy, in retrospect, to say, "Oh, of course, Google would have figured it out." But Google looked like billionaire geniuses now and it's not a given they would've been able to do all this stuff. So, we are starting to learn what we don't know and I think a lot of the FTC work has been good at exploring that stuff and I think it's important to not try to define, clamp down, though, I think the definitions of "harms" is a productive area to go to.

>> Catherine Harrington-McBride: Okay, Lee?

>> Lee Peeler: You know, I think Jim's making some good points and just addressing the point that you were racing about, "Are we saying all information is sensitive?" I think another way of phrasing that is to say, you know, and particularly in the commercial contexts, that we're saying, "All information should be treated fairly." And I think one of the things the FTC has done a wonderful job in over the last several years is creating some real expectations and information will be handled securely, and that if you don't afford information the security -- that its type suggests it

should have, that you will be dealt with rather roughly by the FTC. There's a great program right now ongoing with the revisions of the privacy notices to make the privacy notices more accessible. The FTC's led an effort that's been embraced by the industry on online advertising to try to pull a disclosure outside of the traditional privacy notices to indicate the presence of online targeting, you know, an effort that the industries embrace. So I think if you're on the commercial side, there's a lot being done. The last thing though, that I think is really important in talking about sensitive information is the educational efforts that the FTC has pursued. I was thinking about this last night because my youngest daughter called me and said she's looking for a job this summer and a potential employer had said, "E-mail me Social Security number." I said, "E-mail him your address, but let's mail him your Social Security number." And we had this big debate about why that was appropriate or not appropriate. But clearly that suggests a need for continuing education on the sensitive data issues.

>> Catherine Harrington-McBride: We'll go to Lior and then Pam. If you could each take just about a minute, we are very close to overtime.

>> Lior Strahilevitz: So I'll try and be pithy and say in response to your question. If everything is sensitive, then nothing is sensitive. Hierarchies in law are extremely important. Not so much for automated processes. Automated processes don't get tired, but humans do. And if humans are forced treat everything as equally sensitive, then nothing's -- then the financial privacy, sexual privacy, private health information that we care about so much will get inadequate protection. And then just the quick point I'd make, maybe by way of support for that statement, is actually that we learn a lot by looking to the law of trade secrecy, which is essentially corporate privacy, and the judges there have figured this out. So firms that stamp "Proprietary Trade Secret" on everything don't get trade secret protection because the judges say, "You're overusing that label sensitivity and by abusing it, you're not really sending a signal to your employees, to outsiders, that this is to be taken really seriously." And so, I think what the FTC has to do, even though it's a tall order, is to figure out what the hierarchy should look like so that we make sure that people do take those crown jewels of private information, as seriously as they ought to be taken.

>> Catherine Harrington-McBride: Pam, last word.

>> Pam Dixon: My comment follows on that very much. I was going to say there is either-- it's really easy to decide. There's either all or nothing in this area. Everything is sensitive or none is sensitive, and I do think the solution is hierarchy and stratification and I think a good example of this, even though there was a health care panel, is to think about health information in a little more detail. So, for example, within health information exchanges being done digitally, one of the large conversations that's taking place at the state level in every state in this country right now is what data, within health information, is sensitive data? And so, for example, there's a broad consensus that reproductive data, genetic data, and domestic violence data, among some other types of medical data, are a little more sensitive in the hierarchy of medical data. So, I think it is possible to pullout categories of data within a hierarchical structure and at least begin there.

>> Catherine Harrington-McBride: All right, well, Michelle, we present you with a full plate of problems, so, up to you to solve them.

>> Michelle Rosenthal: You did such a great job, I'm thinking of leaving this all to you and--

>> Catherine Harrington-McBride: It's these guys.

>> Michelle Rosenthal: You all did such a great job. So, over the course of round table series, panelists have suggested a number of principles that might apply to the collection and use and sharing of data that would afford greater protection to consumers and I'd like to touch on some of those principles and discuss whether and how they should apply in the sensitive data context. So, I'm going to get to the fun one first. Some have suggested that some data is so sensitive that it's collection should be prohibited altogether. Katherine, is there any type of data or any type of user where the collection of data or the collection of that data should be completely prohibited?

>> Kathryn Montgomery: Well, I don't know if I'd exactly say "Just the collection of the data." In some ways I'm really talking more about behavioral profiling. And I think it has to be looked at within the marketing context. And a coalition of children's groups has called for no behavioral profiling for children under the age of 18 because of the special attributes of childhood and

adolescence. Saying that, I would not be talking about restricting access to information on the part of young people under the age of 18. And I think we really have to look at ways to balance the autonomy and the freedom of young people to use digital technologies, which I think are wonderful, with some -- I would say restrictions on particularly what marketers do with their information. And beyond that, I think, obviously, we need to ensure that young people understand what's happening on these various basis, particularly with media marketing, where they are provided with new tools to set limits to their privacy and choose who their friends are and who has access to this and that. But they don't understand the entire apparatus of data collection and profiling that's taking place sort of behind the scenes there. And so I think we need to look at it. I'm not prepared, necessarily, to say this definitely but I think it's an area that has to be looked at much more closely.

>> Michelle Rosenthal: Lee, did you have your --

>> Lee Peeler: So again, you know, we did work with Kathryn to come up with the existing COPPA format and regulations. And I think there's sort of two interesting learnings from that. The first is that when the issue of industry, self-regulation, of online behavioral advertising came up, one of the issues was what do you do about behavioral profiling of kids, young kids, kids under 12. And the response within the was, "That's a no brainer. We have a COPPA framework. You would apply the COPPA framework to this area. Even though the information doesn't meet the -- personally identifiable standards that currently exist in COPPA." So the self-regulatory guidelines say, "Don't profile children under 12, under the COPPA standards, unless you have parental consent." Not a prohibition, because if the parents say it's okay to do this on this website after disclosure, what's happening, that should be fine. But that's a good example, I think of how, you know, again going back to first principles, there's a risk of harm to the kids and they are too young to deal with it. It makes it fairly easy on a going forward basis. For kids, you know, 13 to 18, there's also some interesting history, though, you know, when we originally started the COPPA discussions, the proposal was to have COPPA extend to kids 17 and under. And that fell out of the debate. And it fell out of the debate largely because of concerns and uncertainty about what -- just what Katherine was talking about, "What's the impact of that type of approach by the government on other pretty fundamental issues that involve what teenagers and tweens do and what their rights

and what their status in society is. And you know -- I don't think Katherine is even suggesting that you would apply a COPPA model to young teens.

>> Kathryn Montgomery: I'm not. Can I actually respond? Because I meant to say that.

>> Michelle Rosenthal: Sure. Go ahead. Go ahead -- go ahead, no, go ahead.

>> Kathryn Montgomery: We dealt with this. Lee and I dealt with this and I was really troubled by it. It was really challenging, because the notion of getting parental permission, which itself, is a messy one. But I think the principle is what was important here, and it has really helped to guide the development of the Children's Online Marketplace. But with teenagers, what I argued for was a fair information practices, directly for teenagers, which I think is still important. Because COPPA only applied to under 13. 13 to 17 is absolutely fair game, with some of the most manipulative and unfair practices you've ever seen. Just exploding and really taking advantage of young people's need to develop identity, to explore identity, to explore friendships, to share and not really know, and even since then -- not know the consequences. Since then, there has been more science that has looked at brain development in teenagers. And we know, and this is actually reflected in public policy. Anybody who is a parent of a teenager who's getting a driver's license knows that you don't get them as easily and as quickly as you did in my day, when you turned 16. Because the brain doesn't develop fully until into the early 20s. And there is a tendency to be more impulsive, not necessarily to think about the consequences of what you do. There are also other things taking place in their social relationships. All those things have been built into the marketing apparatus and there really are no fair marketing principles in place now.

>> Michelle Rosenthal: Okay. So you're saying there should be a baseline of principles?

>> Kathryn Montgomery: I do, and I think we need to really look at that and develop some policies.

>> Michelle Rosenthal: Thanks Kathryn. So Jim, there's been a concern expressed, this sort of -- concern which is, you know, maybe in COPPA. COPPA is sort of, I believe, the magic words in COPPA are websites directed to children or with actual knowledge, that information about children

is being collected. But what about in other contexts? Do you always know that data is sensitive when at the point of collection? And how would this affect certain business models?

>> Jim Harper: You don't know. And that was going to be my answer to your prior question, was, "No, there's no data so sensitive that you could say it shouldn't be collected." In a lot of business models existing today and a lot of those to come, which we don't know about yet, you don't know as the operator of a website or a service how people are going to use it. What they're going to say on it, what they're going to publish on it, what they're going to hand over to you, and whether it's truthful or not. I think that's the dimension of this that maybe people haven't thought about as much as they should. Users are in a position, and I think they should be in a position, to mask their identities that they present to you, to mask the information that they present to you. They may say that they're something that they're not, and they're trying to achieve anonymity, pseudonymity, obscurity, along one dimension. That indicates to you that they're in a group that you have to deal with differently. So it's a real mess to try to administer systems based on categories of sensitive information or categories of sensitive users, though I agree that you have to look out for sensitive users. I think that COPPA is an example where the intent is certainly there to protect children. Whether it does or not, I think there's some talk about balance that should be done.

>> Michelle Rosenthal: Mhmm, thank you. Lee?

>> Lee Peeler: Just -- from regulatory which I used to do, and self-regulatory which I do now at standpoint, the point that you're making, which is whatever standards you have have to be sort of predictable up front is really important because a lot of the concerns that we've been talking about today are things that may subjectively affect individuals differently. So, you know, one of the things that's going on right now, in response to the FTC's call, is that the self-regulatory groups that develop the online behavioral principles have committed to continuing to look at the sensitive information categories to see if we can't come up with sort of objectively defined criteria in the health and financial information areas to sort of further refine our analysis there. That same work's being done by the Network Advertising Initiative and has been ongoing for some time. So there really is an effort, the industry really understands that there are certain areas of sensitive

information that require a higher level of protection, and it is working very hard to try to objectify that.

>> Michelle Rosenthal: Okay. So Pam, if it's difficult to prohibit collection, are there certain uses that should be prohibited? For example, and I'll use the behavioral advertising context since we're talking about it a little bit, the way that the information is transferred from your browser to various servers, it just automatically is collected in many contexts. The URL is automatically given my IP address. It automatically goes to the server. So the question is in that kind of context, should use be prohibited? So if I decide to go a sensitive website, a website about -- I'm not going to use myself here. If someone decides to go to a website about sexually transmitted diseases, should that information be able to be collected? Okay, it might be collected, right, because it's transmitted, but should it be able to be used to behaviorally target that person?

>> Pam Dixon: Okay. This is a good topic. There's a lot of meat here, so I'll try to be just as brief as I can. I really wanted to talk, just in this context, about self-regulation and prohibition on uses. One of the issues--I think, yes. I think that sometimes there is inadvertent collection and collection that is inescapable, for lack of a better way of putting it. In that case, yeah, you should have some data retention guidelines that are applicable. I think that is incredibly helpful. Also, data use guidelines that are very, very specific and concrete. Say, "Hey, look. If you have it, you don't get to use it because there are direct harms associated with this." So I think we can be very clear on that. I think something that also really needs to be mentioned here is the role of self-regulation in determining these guidelines. Currently, the self-regulatory process that has been in place for both the Network Advertising Initiative and the IAB guidelines, both of them, there's not been enough tension in that process. Industries got together and made a self-determination about what constitutes sensitive. The problem is that there has not been a mandatory addition of the consumer viewpoint. So therefore, the definitions of what constitutes sensitive, in both the NAI guidelines and the IAB guidelines, are really incredibly weak and I think improperly so. So, if we're going to have any kind of self-regulation in the sensitive area of space, there's got to be some kind of joint rule-making, or some kind of negotiated rule-making, something where there is some honest tension between what consumers want and what industry wants. Because if industry sets guidelines

for what constitutes sensitive information, we're going to have weak guidelines, just because we need more tension in the process.

>> Michelle Rosenthal: Okay, thanks, Pam. Jim, go ahead.

>> Jim Harper: So there's a venue where this kind of tension plays out, I think, regularly. That's the marketplace, where participants like Pam Dixon and many other advocates, point out that certain products and services are, plenty of people on this panel in fact, point out that certain products and services have negative implications if you share information with them. "Look at this bad actor, look at this bad actor. Do you know what they're doing?" That's a really important process and the important thing, I think, to me is that it's granular. It allows individuals to make decisions. Of course, they encounter error. They also make decisions for themselves about what risks they want to take, what services they want to enjoy, at what cost to privacy or consumption, personal information, that kind of thing. I think it's a far superior process, even though we're all great intellects, I'll include everybody in the room. We're all great intellects, but we don't have what it takes to figure out the optimal design of our privacy systems going forward. That's going to be in the marketplace.

>> Michelle Rosenthal: Okay. I think that's a good point. So there are consumers, obviously, that want to share information in certain ways. So that sort of gets to another principle, which is -- we've talked about restricting co-action or use. What about restricting sharing with third parties? An example I'll give is if you are on a social networking site and you decide that you want to play a game, let's say "Scrabulous". Does the provider of that game really need to know my religion and my political affiliation? Does all of that information need to be sent? Should there be certain restrictions that sort of prevent sensitive data from changing hands? I'll note that in the B2B context, many companies have these types of contractual restrictions. They say, "Okay, we're sharing this data with you for this purpose, but you can't then go and use it." So should this be a principle that we should apply to sensitive data? Kathryn.

>> Kathryn Montgomery: Yes. Great. It should be. I also wanted to respond to what Jim said, though. That is that, you know, having been an advocate for a number of years and spent a lot of

my energy and time doing research and working with the press and filing comments to expose bad actors and bad practices, it's a hell of a lot of work. It's not a very good system. It is a good system to be able to work as an advocate to try to influence policy. What we can do with policy is to create a level playing field, so that consumers have a set of expectations when they're operating online, and businesses have a set of rules. Now, that can be done through self-regulation as well, but there has to be accountability built into it. I think, again, the COPPA model of self-regulation and government oversight and government regulation has worked well. Whether the actual mechanisms are perfect, we can talk about. The idea of a framework of government regulation that then operates with some rules of the game that have resulted from some consumer input, so that we can have clear expectations. The other thing is who has seen a privacy policy lately and be able to decipher it? The other thing is it's not a question whether you're going to be able to negotiate with that website or with that service. You know, take it or leave it, essentially.

>> Michelle Rosenthal: Mhmm.

>> Kathryn Montgomery: A lot of these are services that we all need, and there aren't exactly alternatives. I don't think the marketplace has worked.

>> Michelle Rosenthal: Parry. I want to give Perry a chance to answer. She's had her -- yes.

>> Jim Harper: I don't want to diminish what Katheryn says. That's exactly what an advocate would say about the system. It's never satisfactory, neither is it satisfactory to people on the other side. I'm an advocate and I'm dissatisfied with the Obama administration's privacy practices, for example.

>> Michelle Rosenthal: Thank you, Jim.

>> Parry Aftab: I think as we start looking at this, I'll make one brief comment on the advocacy role. I think that a good appearance on the Today Show will change a lot of website practices pretty fast, and sometimes better than our sitting in a room and negotiating for months with different people who are not doing what they're supposed to do. That said, I think that if we start

looking at this third-party sharing, I think if it's an unexpected third-party sharing, that we should be regulating that. If it's the kind of thing that's not open, that's not on your Facebook profile and open to the world, 'cause you're not using the privacy settings and anybody could have seen it, I think that that can be done. When you look at the B2B environment, which you can turn around and say, "I'll share information with you, but you can't share it with others. It's only for our purposes or this limited purpose that we do," that comes under expectations everybody understands what it is. When it's something that's already available to everyone, it's hard to restrict it. So I think, as we start trying to see if that could work, we're going to have to be very granular. Is it information that's already covered and protected by privacy settings so that the person's locked it up? Is it the kind of thing the person has restricted? Have they provided an effect and expected consensual use by anybody who happens to see it? I think as we do that, we can come up with a solution that restricts the third-party use, as long as it's expected and defined and in the kind of thing that people would assume that it's not otherwise available just because, "I have the user access, a log-in and password because that's how they're going to get on my social game. I'm not going to be able to get in and see other things that they're posting, that they're keeping private."

>> Michelle Rosenthal: Right, okay. Anita.

>> Anita. Well, I don't think that average Jane or Joe consumer knows how their Toyota works, and they certainly don't know how the internet and the web work. I think that we really need to have a very strong, kind of consumer protection mentality when thinking about these issues of collection, use and sharing with third parties. And while, in some idealistic political world, maybe we would have a complete free market and let people just make their own contracts and their bargains and do their own thing, but I think there's so much complexity, so much technical complexity, so much hiding of information, and unavailability of information, and so much lack of freedom to truly bargain with website operators, for example, that we really need to have the government here playing a very strong role. I think the FTC needs to play a very, very strong role in regulating the ways in which information is made available or not available. and I don't think we should be too reluctant to use coercive and even paternalistic measures at this stage of life. The internet, the web, is too new for us to assume that people are capable of taking care of themselves when it comes to their online transactions. I personally welcome a bit of someone else kind of

helping me through my financial and market transactions on the web, and I think that the FTC has a very important role here.

>> Michelle Rosenthal: Thanks, Anita. What about -- there's the principle of sort of minimizing data collection. And so I'm going to borrow an example from Jules Cohen from Microsoft earlier today where he sort of talked about, you know, you go to a bar. And does the bar really -- you know, I show them my license, and all they really need to see is my date of birth. They don't need to see my address. they don't need to see my license plate number. So I should be able to give only the amount of information that I need to give, and that additional sensitive information or potentially sensitive information shouldn't be collected. So Lior, what kinds of harms would this type of principle protect? Is this is a good principle and would this protect against certain harms that we discussed in the first portion of the panel?

>> Lior Strahilevitz: You know, in a lot of the web-based applications, the consumer has a variety of self-help options which turn out to be fairly effective. So a colleague of mine on the faculty was in his office about two weeks ago, and he's searching for a condominium in Chicago. And I had turned him onto a really nice real estate website that helps people find condominiums in Chicago or houses, too, I suppose. In any event, he's searching for condos and gets a call on his phone. "Oh, I see you're looking for two bedroom condos in the blank blank neighborhood in Chicago." And he tells me this story, and I said, "You mean, you gave them your real name and your real phone number?" Part of what I think individuals do in these circumstances, and this is a falsifiable hypothesis, is they get around regulations they don't like by providing incorrect information, and I think firms that are doing work in this area tolerate very high levels of what we'll call consumer self help on pro-privacy perspectives. The other thing that happens I think through this sort of interaction is a consumer was very ticked off by what he viewed as an intrusive search into his own internet usage patterns and decided that next time he looks for a condo, he'll use another website, which does suggest that these market forces can work, but only if the fact that there was a person who was scrutinizing what my colleague was searching for by way of real estate, only if that becomes transparent. So it's the stupid firm that says, "I see that you're looking for condos in this and this neighborhood." And the danger is when that monitoring can be both surreptitious and potentially threatening or harmful to the consumer in some ways. But having said that, I think the

popularity of self-help through allowing consumers to provide inaccurate information or only partially revealing information about themselves does suggest that there's a fix here, and one interesting legal question is, "How should we regard my decision to enter Donald Duck as my username?" Is that a breach of contract? Might well be under the terms of service. Or is it something that I ought to be empowered to do as a way of opting into a privacy arrangement that's more protective than the ones that the firm on the other end of the transaction seems to be offering me. If they tolerate me as Donald Duck, and nobody ever calls me on it, and I'm allowed to continue using the service, should we regard as me having amended the contract, and then having agreed to it, by continuing to provide me service. That actually strikes me as a very interesting legal question on which there's good thinking to be done.

>> Michelle Rosenthal: Thank you, Lior. So we have -- I'm mindful of the time. We have about 15 minutes, and I would not want to take up anybody's break time. So I'm going to try to quickly get to some of these very important principles. What about data -- I'm sorry, limiting data retention? Parry, would that -- what kind of harm would that prevent --

>> Parry Aftab: Well, I think limiting data retention is a little bit what you were talking about at the bar. And when we started looking at pornography, and whether or not you could require someone to prove that they were over the age of 18 to be able to see certain pornographic images, it was thrown out because we said you might have flash your driver's license to show that you're 18 so you can buy a magazine. But if you're flashing it online, somebody is collecting it. And once it's collected, it's being used. And I think they really come together. So I think that as we're looking at data retention -- it could be it expires after a certain time, after the right use. It could be that it's tagged and watermarked, in effect, so it can only be used for certain purposes as it moves. And it could be that it comes through authentication and smart card type of technology, that it contains the information. All they're doing is authenticating somebody's 18, somebody is 13 and capable of COPPA communication. Somebody can have this communication without the sites actually having the real information. They're just having the authenticated fact that somebody's met the threshold. so I think it works that way.

>> Michelle Rosenthal: Okay, and should it only apply to sensitive data, or should that be the type of principle that applies across the board?

>> Parry Aftab: You know, I really think that if we start applying it across the board on things that could be sensitive under certain circumstances, and if we can get enough people to adopt it, I think it works. I think it's finding trustworthy providers, so the companies that providing those smart cards or authenticated services, you know that they're not gonna have the data bleeds, and they're not gonna have -- you know, they're gonna have adequate security and the right rules in place to govern it. But I think if you do that, it might be an answer to a whole bunch of the harms that we've identified.

>> Michelle Rosenthal: Great, okay, thanks. So we talked a lot I think in this panel about subjectivity and what's sensitive to me may not be sensitive to Katy and vice versa. What about the principle of access? So you know, would access prevent sort of that -- that concern? Because it would allow consumers to -- and of course, we have to talk about what access would look like. And I know there are a lot of feasibility issues and operational issues and things that would need to be discussed. But you know, if I can access the type of data that a company has about me, and either edit it or suppress it if it's incorrect. Would that prevent against or at least mitigate certain harms, especially some of the harms that are less concrete, so you know, dignitary harm or reputational harm. Pam?

>> Pam Dixon: I think the access model. Especially if you look at the fair credit reporting act model, and how that works with the credit bureau reports. I think it's a very, very good model to look at. And I think it's a challenging model to scale to broad internet kind of site issue, but I don't think it's impossible. And I think certain principles could be extracted and applied, and I think it's a very helpful way of thinking about it. I think that something else along these lines that I think about, just to follow on our last conversation, identify management, I think, is going to be a real issue when it comes to sensitive data in certain categories. Financial and medical come to mind. Because you have to authenticate the person, and then you have this authenticated information laying around. And I think that we should not minimize how incredibly sensitive that information is in and of itself as a category. From this morning's panel, on identity management, I think we need

to look at identity management as a coming very significant issue, that's going to need a lot of thought and attention. Maybe itself considered its own category of sensitive information.

>> Michelle Rosenthal: Thanks, Pam. So is there a cost to access? What kind of cost is associated with access? And can we really expect small companies to engage in this type of practice?

>> Lee Peeler: I mean, that's exactly right. Unless you're set up to provide access, there could be very significant cost in providing access. Also, you could increase the privacy warnings. Much of the information the companies retain now is in machine readable form. And translating it in a format that a consumer could actually get it and understand it would entail making it more vulnerable to start with. And then anybody that's been through the credit bureau report disclosure process knows that just verifying that you are who you say you are in light of this very significant threats of identity theft requires you to disclose a significant amount of information in and of itself. And if you don't get that balance right, you could end up disclosing sensitive personal information to someone who's not entitled to it. I think you need to be sort of wary of these broad one-sized approaches.

>> Michelle Rosenthal: Thank you. Thanks, Lee. So I'm going to move on. And this next question is for Anita. The principle, I think the most commented is the sort of principle of transparency. It's one that we embraced in the behavioral advertising principles in the report. And sort of the idea of notice and consumer control, and sort of making sure that consumers really understand what's happening. But Pam, the question is, can notice truly control the convey the nuances of the various business models, and some of the long-term consequences? So maybe there's not a harm that's going to occur tomorrow, but maybe it'll happen over time. And specifically, some of the harms that may accrue as data's aggregated. Did I say Pam? I meant Anita, and I said Pam. Apologies. You're sitting right next to each other.

>> Anita Allen: Well, transparency is great for consumers, if they can then use the knowledge that they acquire through genuine transparency to affect change in their life and protect their interests. I mean, one problem is that transparency without some sort of entitlement or privilege or right to do something about what one discovers is not very helpful. Much in the same way that access without

the capacity to actually change is not very useful. I can recall once getting my credit report, and discovering that my name was not Anita, but Dania. And every bit of financial data was absolutely accurate, but my name was wrong. And even after I sent my passport and my driver's license, it took me a year to get my name changed from Danita to Anita. So access without the power to correct is not very good. Transparency without the power to then affect the institutions and practices and information to make things right is not going to be any good, either.

>> Michelle Rosenthal: Based often all of these principles that we're discussing, do we really need notice? Do we need to give all of this information to consumers? If we had sort of a baseline, sort of a level of protection in various principles that we think are actually protecting consumers, do we need to provide notice about every specific piece of data that's collected and used?

>> Male Speaker: Not if you phrase it that way.

>> Michelle Rosenthal: So we just need really good protection?

>> Lior Strahilevitz: Here's what I think we need to do. So with any consumer good, you're gonna see bundling of various services into categories. People don't buy cars a la cart. They purchase the premium package or the premium plus package, or the fat cat package or what have you. And I think this bundling, in terms of privacy law, can be very helpful to consumers. So if you think about what, let's say, what Microsoft does with respect to its software. You can opt for high security, medium security, low security. That's a useful way to think about meaningful choice to consumers. What I think the law needs to do, though, is make sure that high security really is meaningfully more protective than medium security. And that low security is meaningfully less protective than medium security. And I think sometimes because consumers latch onto labels and short descriptions much more than they're likely to latch onto details or have time to read the details, we can actually make a tremendous amount of progress with these short descriptions, and then the law's role is simply to make sure that the terms actually match the abbreviated descriptors for the substance of what consumers are buying when they're agreeing to a particular service.

>> Michelle Rosenthal: Thanks, thanks. What about the consent? Pam, the argument has been made that if you were to require something like an opt-in for sensitive data that "a," it would ruin certain business models. It would actually prevent them from doing business the way that they do it. But also that consumers are going to opt-in, that if you give them the right incentive, that they will opt-in without truly understanding what they are opting into.

>> Pam Dixon: Yeah, I think consent is a really challenging issue. Consent really isn't a 100% solution for sensitive data because it can be manipulated. It has to be done very, very carefully. So that would be my answer there. It can be done. It has to be done very carefully and cautiously. In terms of notice, I do think that notice is very important. We need a public dialogue about this data. And too often, consumers do not have enough information for the dialogue.

>> Michelle Rosenthal: Thanks, Pam. Jim?

>> Jim Harper: I would just -- on with these ideas of transparency and consent, they're both great ideals. I think transparency is essential. It's not essential for each individual user of a service to take advantage of the transparency immediately. We have an internet-y problem here, and it needs to be solved in an internet-y way.

>> Michelle Rosenthal: Did the court reporter get that?

>> Jim Harper: Internet-y. It's a new adjective, I didn't come up with it. But a broad, diverse, moving changing community will make decisions about what's appropriate to do, about what services are appropriate to use. It's a distributed process and consumers are very well positioned thanks to the internet which is a communications medium to learn about this stuff. Many don't. We're never going to be satisfied that everybody knows enough, especially those of us in the room. We're never going to be satisfied that people are intellectual enough about their privacy decisions. But collectively, overall, they'll do a better job of figuring stuff out with the help of their peers, their colleagues. I'm proud of the fact that my dad told me to use Amazon the first time. That was because he'd gotten advice from others that this was pretty cool, so I went ahead and used it. That's

why I used Amazon. Not because I read their privacy policy or investigated Amazon. The collective mind had investigated Amazon and gave it their stamp of approval.

>> Michelle Rosenthal: Thanks, Jim. So Parry, what about security? Commissioner Harbor mentioned this morning sort of using SSL for e-mail, and I think that sort of raises a good point, which is, we talk about -- I talked with Jim about the ex-anti concern, which is, you don't always know that it's sensitive before you collect it. But I guess -- I think we could probably all agree that your e-mail contains some sensitive information. And certainly, those of us who don't have Lee as our father, you know, might include information that might be deemed sensitive, perhaps, social security numbers or information about e-medical information and what have you. So would this address sensitive data? Should we expect -- should e-mail providers encrypt -- use this type of encryption just because they know -- the odds are there's sensitive data included in the e-mail?

>> Parry Aftab: No. I think that it's less about what you're sending by e-mail and more about what happens to it once the data arrives. And so you see a lot of issues with people who have access to it, and people have no idea who they are. No background checks if people have access to the data. They have no control over the computers. Maybe somebody's doing it remote. You've got moderation staff or a working remote, or other countries, and nobody knows who they are, and where the computers are, and who else they may be working for, and confusing it with. So I think it's a lot less about the channel of e-mail and what's being sent, and a heck of a lot more about training practices, processes, policies, good, old-fashioned data hygiene when it arrives.

>> Michelle Rosenthal: Thanks, Parry. So we have about two minutes left. So I'm going to get to the final question. During the first half of the panel, we discussed the considerable challenges associated with defining sensitive data and the concern, of course, that if we label everything sensitive, that nothing is truly sensitive. So recognizing that. We also discussed a number of principles that should be applied to the treatment of sensitive data. And some of you suggested that a number of these principles might apply to all data, despite whether it's considered sensitive. So let's get to Lee's point, which -- something that he mentioned earlier, which is, is there some baseline level of protection for all data that would obviate the need for special treatment? Should we just be applying these principles across the board, and feel that then sensitive data would be

okay? That we shouldn't be concerned about sensitive data because there are certain principles that would apply to all data. Pam? Sorry, Pam, and then Kathryn.

>> Pam Dixon: Yeah, I don't think we get to go there in the sectoral society that we have running here. I think that certainly one can look at Europe and say that the omnibus style of protection is a model that could be very seriously considered, but the reality in this country is, I don't know how we could institute that at this point in an easy fashion. And maybe it will happen some day, but it isn't here today. So let me just speak about today, and I think that today in our sectoral system, I do think that we need some kind of sensitive data protection. I think we're going to have to work very hard to create hierarchies that make sense, and I think it's going to be very difficult to find one single standard and say, "Okay, absolutely, everyone on the internet and the health care sector and the financial sector, you all meet the same standard for all data." I just don't think it'll happen.

>> Michelle Rosenthal: Thanks. Kathryn?

>> Kathryn Montgomery: I think we've got a very challenging situation as I look here at the principles of data minimization and rules about data retention and access and transparency. I think we have the opposite system that's emerged in the digital marketing infrastructure. It is all about data maximization. It is not at all transparent. There are many, many, many forces at work that are going in that direction, and at the same time, I think we should think about the goal of a broad set of rules that will mitigate some of these very strong forces. But I don't think it's either/or. I think we should seek that, push for that, but I think we also should be developing -- and it's probably going to be a little bit more manageable, even though it's going to be complex, and we haven't resolved it all -- some ways of addressing these sensitive issues and sensitive information. I think that can be done. We're not going to solve it all today, but I would urge the commission to pursue that.

>> Michelle Rosenthal: Thanks, Kathryn. And Jim, you get the last word.

>> Jim Harper: Thank you very much, and I'll be brief. If there's a baseline --

>> Michelle Rosenthal: Second to the last word.

>> Jim Harper: Second to the last word? This is a real zinger.

>> Michelle Rosenthal: I know.

>> Jim Harper: If there's a baseline rule that should apply to all collectors and holders of data, it is that they should be subject to the rule of law. And I speak especially of the United States government which essentially steals data. And it has not seen any sanction as of yet. See, I told you.

>> Michelle Rosenthal: Wow, that's a zinger. So Anita, you gotta top that.

>> Anita Allen: I am so glad we're not stopping there. Sensitive data is not a platonic essence, but I think we need to keep using the concept. It's a rule of thumb. It's a heuristic device for helping us to remember that there are important social values that we have to incorporate in our data practices.

>> Michelle Rosenthal: Thank you, Anita. We have to end.

>> Parry Aftab: Just one comment.

>> Michelle Rosenthal: Yes.

>> Parry Aftab: I think that -- two things. "A," Privacy and respecting users is good for business. We need to remember that. But the most important thing is, the two of you have done a remarkable job.

>> Michelle Rosenthal: I'm glad I let you go, Parry.

>> Parry Aftab: But throughout this entire process, how you worked with all of us, how you pulled us together, it's like herding cats. You made sense of this. You basically kept to time, but I think that you two are amazing people. You have really brought this whole thing forward today, so thank you.

>> Female Speaker: Just for the general counsel folks who may be in the office. I just want you to know that this is not a paid endorsement. We don't want any sort of concerns rising.

>> Michelle Rosenthal: Thank you, you all have been wonderful. We really appreciate all of your work. Thanks.

>> Female Speaker: Back in 15 minutes.