FEDERAL TRADE COMMISSION

ADVISORY COMMITTEE ON

ONLINE ACCESS AND SECURITY

9:00 A.M.

FEBRUARY 25, 2000

VOLUME 2

FEDERAL TRADE COMMISSION

600 PENNSYLVANIA AVENUE, N.W.

ROOM 432

WASHINGTON, D.C.

REPORTED BY: SUSANNE Q. TATE, RMR

DEBRA L. MAHEUX

A T T E N D E E S

FEDERAL TRADE COMMISSION:

David Medine

Jessica Rich

Hannah Stires

Allison Brown

COMMITTEE MEMBERS:

James C. Allen, eCustomers.com

Stewart A. Baker, Steptoe & Johnson LLP

Richard Bates, The Walt Disney Company

Paula J. Bruening, TRUSTe

Steven C. Casey, RSA Security, Inc.

Fred H. Cate, Indiana University School of Law

Jerry Cerasale, Direct Marketing Association, Inc.

Lorrie Faith Cranor, AT&T Laboratories

Mary J. Culnan, Georgetown University

E. David Ellington, NetNoir, Inc.

Tatiana Gau, America Online, Inc.

23 Alexander Gavis, Fidelity Investments

24 Daniel E. Geer, @Stake, Inc.

25 Rob Goldman, Dash.com, Inc.

COMMITTEE MEMBERS:

David Hoffman, Intel Corporation

Lance J. Hoffman, George Washington University

Josh Isay, DoubleClick, Inc.

Daniel Jaye, Engage Technologies, Inc.

John Kamp, American Association of Advertising Agencies

Rick Lane, U.S. Chamber of Commerce

Gary Laden, Council of Better Business Bureaus

James W. Maxson, Paul, Hastings, Janofsky & Walker

Gregory Miller, MedicaLogic, Inc.

Deirdre Mulligan, Center for Democracy and Technology

Deborah Pierce, Electronic Frontier Foundation

Ronald L. Plesser, Piper, Marbury, Rudnick & Wolfe

Lawrence A. Ponemon, PricewaterhouseCoopers, LLP

Richard Purcell, Microsoft Corporation

Peter Reid, NCR Corporation

Daniel Schutzer, Citigroup

Andrew Shen, Electronic Privacy Information Center

Richard M. Smith, Internet Security Consultant

Jonathan M. Smith, University of Pennsylvania

Jane Swift, Commonwealth of Massachusetts

James E. Tierney, Former Attorney General, Maine

COMMITTEE MEMBERS:

Frank C. Torres, III, Consumers Union

Thomas Wadlow, Pilot Network Services, Inc.

Ted Wham, Excite@Home Network

Rebecca Whitener, IBM Corporation

P R O C E E D I N G S

- - - - -

MR. MEDINE: Okay, if you could take your seats and we'll get started, please.

Good morning. Welcome back to the Federal Trade Commission for the second meeting of the Advisory Committee on Online Access and Security. Before we get started in some of our procedural work and some of our substantive work, I just want to commend all of the members of this group for the fine work product that they have developed to date. The outlines that each of the subgroups created are thoughtful, in-depth analyses of the issues and I think far exceeded our expectations about work product. So, I think we're off to a tremendous start.

Let's keep our eye on the goal, which, of course, is preparing a report to the Commission, but I think we have really done a -- you have done a great job in fleshing out these issues.

Now, returning to some of the formalities, I will call the role of the committee.

James Allen? Please signify by saying "here"

or "yes."

MR. ALLEN: Here.

MR. MEDINE: Stewart Baker? Not present.

Richard Bates? No response.

Paula Bruening?

MS. BRUENING: Here.

MR. MEDINE: Steve Casey?

MR. CASEY: Here.

MR. MEDINE: Fred Cate?

MR. CATE: Here.

MR. MEDINE: Jerry Cerasale? He's here. Jerry Cerasale?

MR. CERASALE: Here.

MR. MEDINE: Very dramatic.

Steve Cole? Gary Laden substituting by written permission for Steve Cole.

MR. LADEN: Here.

MR. MEDINE: Lorrie Cranor?

DR. CRANOR: Here.

MR. MEDINE: Mary Culnan?

DR. CULNAN: Here.

MR. MEDINE: David Ellington?

MR. ELLINGTON: Here.

MR. MEDINE: Tatiana Gau?

MS. GAU: Here.

MR. MEDINE: Alexander Gavis?

MR. GAVIS: Here.

MR. MEDINE: Daniel Geer?

MR. GEER: Yeah, hi.

MR. MEDINE: Rob Goldman?

MR. GOLDMAN: Here.

MR. MEDINE: David Hoffman?

MR. DAVID HOFFMAN: Here.

MR. MEDINE: Lance Hoffman?

DR. LANCE HOFFMAN: Here.

MR. MEDINE: Josh Isay? No response.

Daniel Jaye?

MR. JAYE: Here.

MR. MEDINE: John Kamp?

MR. KAMP: Here.

MR. MEDINE: Rick Lane?

MR. LANE: Here.

MR. MEDINE: James Maxson?

MR. MAXSON: James Maxson? Oh, that would be me.

MR. MEDINE: He's here.

Greg Miller?

MR. MILLER: Here.

MR. MEDINE: Deirdre Mulligan?

MS. MULLIGAN: Here.

MR. MEDINE: Deborah Pierce?

MS. PIERCE: Here.

MR. MEDINE: Ron Plesser?

MR. PLESSER: Here.

MR. MEDINE: Larry Ponemon?

MR. PONEMON: Here.

MR. MEDINE: Richard Purcell?

MR. PURCELL: Here.

MR. MEDINE: Peter Reid?

MR. REID: Here.

MR. MEDINE: Art Sackler? No response.

Dan Schutzer?

MR. SCHUTZER: Here.

MR. MEDINE: Andrew Shen?

MR. SHEN: Here.

MR. MEDINE: Richard Smith?

MR. RICHARD SMITH: Here.

MR. MEDINE: Jonathan Smith?

DR. JONATHAN SMITH: Here.

MR. MEDINE: Jane Swift?

MS. SWIFT: Here.

MR. MEDINE: Jim Tierney? No response.

Frank --

UNIDENTIFIED SPEAKER: I think he's here.

MR. MEDINE: We will grab him as he walks in

the door.

Frank Torres?

MR. TORRES: Here.

MR. MEDINE: Tom Wadlow?

MR. WADLOW: Here.

MR. MEDINE: Ted Wham?

MR. WHAM: Here.

MR. MEDINE: Rebecca Whitener?

MS. WHITENER: Here.

MR. MEDINE: Thank you, we certainly have a quorum.

Let me remind everybody we do have a court reporter taking down the transcript of these proceedings. So, to help the court reporter, could we again be sure to identify ourselves by name each time that we speak, speak into the microphone for the benefit of both the court reporter and for the overflow room, and if one person could speak at a time, again, to keep the transcript -- and we will add Richard Bates.

MR. BATES: Here.

MR. MEDINE: Jim Tierney?

MR. TIERNEY: Here.

MR. MEDINE: I just wanted to also remind members of the committee that we have been posting

important and relevant documents relating to the committee's work on the committee's web page at ftc.gov and we have been sending e-mail updates to individual

committee members. If anyone is having e-mail problems, let me refer you to Hannah Stires, who along with Allison Brown and Jessica Rich are responsible for putting much of today together.

If anyone -- has anyone had any problems -- like I say, feel free to talk to Hannah afterwards in terms of downloading documents or getting access to committee information.

As we mentioned at the first meeting, we are accepting public comments on the work of the committee and encourage committee members to consider those comments as they move forward in their work. To date we have received one public comment, which we have posted and alerted the committee members about via e-mail, and again, we would encourage you to check the website occasionally to see if additional comments have been submitted, and we will also try to alert you to those, as well, but we want to both have this committee's views but also incorporate the views of the public to the extent they are communicated to the committee.

One business matter that I guess I'd just put

to the committee is we know that many of you are traveling from distant places and distant time zones, and we have heard some concern about the ability to

make West Coast flights if the sessions end at 5:00 or 5:30. Is there any interest in the group in starting earlier at our next meeting so that we can adjourn earlier?

(Show of hands.)

MR. MEDINE: I see a substantial show of hands, okay. Does anyone want to be brave and propose a specific starting time?

MS. MULLIGAN: 8:00.

DR. JONATHAN SMITH: I can't make that.

MR. MEDINE: You can't make 8:00 a.m.?

DR. JONATHAN SMITH: I take a Metroliner down, and the earliest -- unless I come the night before, which I don't really want to do.

MR. WHAM: We probably have half the room coming the night before.

DR. JONATHAN SMITH: Excuse me?

MR. WHAM: Half the room is probably coming the night before now.

MR. MEDINE: Well --

MR. ALLEN: Starting one hour earlier would allow everybody from the West Coast to be here one

night instead of two nights.

MR. MEDINE: Okay. Should we accommodate our West Coast visitors? I'm getting a lot of nods. Okay.

8:00 a.m., okay. It's not the chair's favorite time either, but in the interest of serving the committee, as your designated federal officer, we will appear at the appropriate hour, but again, we would be happy to try to adjust this committee's work in any way that meets the committee members' needs.

MR. TORRES: As long as you provide coffee.

MR. MEDINE: Well, under federal appropriations rules, we are not appropriated funds, but we may want to discuss if there are members of the group who would like to contribute to the group's sustenance at the next session.

UNIDENTIFIED SPEAKER: Can we nationalize Starbucks?

MR. MEDINE: Or people can just stop on the way in to the sessions, but we'll certainly entertain offers for the next couple of meetings.

MR. LANE: The Chamber would be happy to sponsor the next coffee.

MR. MEDINE: Okay, we accept your offer. Thank you very much.

In terms of our work today, what I propose

today is to go through the work of each of the subgroups in order, that is, starting with access one and working through security three. What I would like

us to keep in mind is having the goal of the final work product of this committee, namely, a report to the Federal Trade Commission by May 15, in which, of course, we'll be discussing views about access and security online.

We've stated previously that the report should reflect options for implementation of access and security, pros and cons, costs and benefits for both consumers and businesses. So, what I guess I would like to try to aim for by the end of the day is a full discussion of the issues and a breakout of a different set of subgroups to work on developing options with regard to a variety of issues so that -- and have those options submitted for the website as the outlines were for this meeting with the options sent by March 24th so that members of the committee will have a week before the next meeting, which is March 31st, to consider the series of options that are developed by each of the groups.

What I think has been done to date is a tremendous fleshing out of the issues, and I think we can spend some more time today fleshing those out even

further and getting input from people who have views on certain matters that may not have been on particular subcommittees, but I hope for the next meeting, if our

working group people are agreeable to that, would be to essentially now build up from this vast array of information and ideas into a set of options for how the commission can view these issues and how firms can think about these issues in terms of implementing those.

I guess I would entertain a discussion about whether people are comfortable with that as a basic procedure.

MS. SWIFT: So, are we going to --

MR. MEDINE: If we could start identifying ourselves I think for the record.

MS. SWIFT: This is Jane Swift.

Are we going to split up into the same subcommittees with the same members or some other membership?

MR. MEDINE: I guess, unless the group disagrees, is we will redivide not only the membership but to redivide to some extent the subject lines of the subcommittees to focus on options. Some of the subcommittees were extremely useful in fleshing out ideas, but we might want to redevise things at the end

of the day that gear us more toward the set of options.

MS. SWIFT: I think that there seems to be a lot of overlap, so the degree to which we can try to

define now without as much overlap might be the best way to accomplish what we need to by the next meeting.

MR. MEDINE: Okay, point well taken.

MR. ISAY: Just for the role, I'm here.

MR. MEDINE: Josh Isay is here for the record.

Any other comments on that as a method of proceeding?

Therefore, what I -- following up on that, I again propose to work through each of the proposals. We'll start in with access one and sort of aim to take a break around 10:30.

The first subcommittee on access one focused on the scope and categories of information and suggested that the sensitivity of the information might be a variable used in determining the extent of access. One thing I guess I would propose to the group is at least from the website, we were unable to print out a chart that actually showed all the Xs and Os and question marks that related to the intersection of various types of information.

Deirdre Mulligan?

MS. MULLIGAN: Deirdre Mulligan.

The group decided -- we had taken an initial cut, and people had -- we were trying to be very comprehensive, and we got a little ahead of ourselves,

and we decided that what would be more appropriate was to actually provide the framing document and to have that discussion either with the whole group or at the next date when we're actually trying to define what it is, but the hope was that the sensitivity issue applies both to access and security, but in the chart, really to provide a framework for looking at the issues, what are the kinds of data we're talking about?

MR. MEDINE: Okay. Let me -- as we move forward in this discussion, I would encourage, again, members of the subcommittee to sort of -- to discuss why they came to the conclusions they did and those who were not on the group to raise issues that they think may not have been raised by that -- by the first group or just to comment on the first group's work.

Yes?

DR. SCHUTZER: Dan Schutzer.

It might be worthwhile to go through some of the other sections that we visited, because some of the other sections had some different slices and additional kinds of categories of data.

MR. MEDINE: Some of the other subgroups or

within this -- within this subgroup?

DR. SCHUTZER: No, some of the other subgroups.

MR. MEDINE: Okay.

DR. SCHUTZER: All the subgroups tended to address to some degree categorization. They all sliced it differently. So, it might be worthwhile to take this one, comment upon it, look at some other slices and then revisit them at the end.

MR. MEDINE: Well, again, I think as part of the moving forward process, one of the issues we want to consider is how do we frame options and do they -- will some of the options turn on the sensitivity of the information or not.

Did anyone want to comment on -- again, either from the subgroup or otherwise on whether the sensitivity of information is the appropriate sort of measure of appropriate access, any members not on the subgroup?

Andrew?

MR. SHEN: Hi, Andrew Shen, EPIC.

I was on the access one subcommittee, but I just want to highlight something that I think another subcommittee had on access, authentication, that in some ways it's very difficult to figure out what is sensitive information. A lot of it depends on context,

depends on the point of view.

MR. MEDINE: Is your microphone on? Just a little closer maybe.

MR. SHEN: So, I think that's something that the committee should take into account, that it is very difficult to figure out what is sensitive information.

MR. MEDINE: I guess then that I would -- then turning that around, is in your view sensitivity of the information the appropriate sort of benchmark as to how much access people should get, or should there be some other standard by which we judge when access is appropriate?

MR. SHEN: Well, I think you -- Andrew Shen again.

I think you should judge access by, you know, whether it's personal information or whether it's not personal information and leave the sensitivity topic up to the data subject, let them decide.

MR. MEDINE: Deirdre?

MS. MULLIGAN: Deirdre Mulligan.

Just to add onto that, the principles that we pulled out here represent views of various people in the subgroup. I think that particularly in looking at the security piece, we thought that sensitivity would be particularly important. The sensitivity of logged

data might be very different if it's stuff that you think could be very compromising, from a company perspective it might be very important, but if you

compare that to the sensitivity of something like credit card information where the security of that, if it's breached, could have serious consequences to the individual, I think on the access issue, Andrew is, you know, absolutely right, that I think there was a broad range of views about whether or not that's a definitive point.

I think we all think it's a point of consideration. I don't think it's the line at which you determine yes or no, and I think that sensitivity is something that is best viewed from the individual's perspective.

DR. SCHUTZER: Dan Schutzer.

I would agree sensitivity's important, and that doesn't mean that it shouldn't be determined by the individual. And just as an aside, financial information is very sensitive, but sometimes even more sensitive than that is seemingly innocuous information such as birth dates and so forth, perhaps even Social Security numbers, things that would give you access to that kind of information, it might be even more sensitive.

Usage is another important category you mentioned. I think one that you didn't mention might be the nature by which the information is certified.

It might be self-certified or it might be provided by an independent third party that's doing the certification, and that might impact the -- who's entitled to updates and modification, depending upon how it's certified.

MR. MEDINE: Do other people have views on this issue of should sensitivity be the benchmark for access? We can obviously raise that later in the security discussion as to whether it's appropriate there.

DR. GEER: Dan Geer. It's been widely quoted by Bob Metcalf how in a network, the value of the network is proportional to the square of the number of nodes on network. I think the risk that sensitivity represents is proportional to in some sense the square of the number of the pieces of information in mind that are in play. I would tell you -- I would answer to you any question you could ask me, I would probably answer one of them for this audience, but I wouldn't do 20, and that's -- it's not linear is my point. The sensitivity issue is not linear. It's something bigger than linear and the number of items in play.

MR. MEDINE: Again, turning that around into sort of an operational or implementation point of view, if you're setting standards, how do you set in a

standard for access when a company might have a little bit of information on some people and a lot of information on other people?

DR. GEER: The hardest thing we're going to face is the question of data fusion, and some of it's inadvertent, such as when two firms, both of which know something about you, merge. That's the hardest thing I think we have to deal with, and I don't have an answer for you.

MR. MEDINE: Okay.

Richard?

MR. PURCELL: Richard Purcell, Microsoft.

I think we have to be careful when we discuss the issue of individual consumers nominating or specifying which parts of their data is sensitive, although I think that that's something that is worthy of discussion. We have to also be cognizant of the fact that we're in a technology environment here, and to have data attributes that specify -- that are variable to the degree that the same data attribute can have a range of sensitivity that's nominated by the user itself would create a database architecture

nightmare and would be very difficult to implement in an accurate sense.

MR. MEDINE: James?

MR. ALLEN: James Allen.

I agree with what Richard says partially. First of all, I wanted to make a point that I think sensitivity of data is critical to a lot of the things we're discussing, but it's not critical to whether or not you give a consumer access to the data about themselves. I think consumers should have access to the data about themselves in any case, but rather, that the sensitivity of the data should dictate the means of authentication, for example, used and so forth, and the more sensitive the data is, the more you should do to protect that data from inappropriate or unauthorized access.

As far as -- back to the point Richard was making, I absolutely agree that from a technology standpoint, and I am a technologist, that it would be very difficult to implement a system that allowed consumers to, as Richard put it, nominate the sensitivity for each individual data element. I think that's why it's -- one of the many reasons why it's critical to come up with some system of categorizing data that puts it into relatively large grain

23 categories of a relatively small number so that you

24 can, one, have a default treatment for data, and two,

25 have large categories that consumers can say, well, for

this information, I consider it more sensitive than the default, and I want it to be treated as such.

And if those categories are large enough and therefore small enough in number, it is possible to implement a technology solution for dealing with that.

MR. MEDINE: And do you have a sense of which -- how would you -- which of the large categories you might use in making that cut?

MR. ALLEN: Well, no, I punt it to somebody else.

MR. MEDINE: Okay, Frank Torres?

MR. TORRES: Well, I am not going to answer that question.

MR. MEDINE: Again, if you could identify yourself.

MR. TORRES: Frank Torres.

At the git-go, are we assuming a level of notification to the particular consumer, customer, person about the information being collected, because to me it's -- the sensitivity question might come into play, because while my name and address and birth date might be considered to be sensitive information for

some people, simply knowing that somebody has that, I may not need access to that information. I mean, they don't have to show me where on their computer system

they have it.

Whereas if they have a bunch of other information about me, say, you know, my account balances and things like that, it might be important that those numbers be accurately reflective of what my creditworthiness truly is, then that's on a little bit different level. Maybe we're -- you know, there's -- the sensitivity definition, but then you move on to what -- then what does that mean as far as access goes for that information and the value of access to a consumer?

MR. MEDINE: So, just -- are you saying that the more consumers know about what's being collected about them -- well, that would affect the degree to which access was important to them?

MR. TORRES: I think that's a factor, yes.

MR. MEDINE: Okay.

MR. TORRES: And David, this is Frank Torres again, you made the comment should sensitivity be the benchmark. I don't think there's any one -- you know, what became clear working in -- within these subgroups is I don't think there's any one element. I think

there's so many interrelationships going on here, it's not just sensitivity. It is usage. And I'm glad that the certification question or the certification issue

came up, as well, because that's going to be an important one down the road.

MR. MEDINE: Jane, did you want to just respond to that?

MS. SWIFT: Jane Swift.

I just want to say I think it is important that notice not be separated from access when we're talking about the sensitivity of information, but I would just add that it becomes more important depending on the usage of that information and its distribution to people that we may not know it was given to. So, just because you gave notice in the first instance, I think access and sensitivity of information takes on a different meaning -- I understand that's complicated, but as it sort of goes into its third and fourth and fifth generation of places that you don't know, people, you don't know who they are or which information they have.

So, just addressing notice in the first instance doesn't solve the entire piece of access, because you need to then know what you don't know, which is where it went.

MR. MEDINE: Unless, of course, notice does provide you not only how it's being collected but how it's being used and to whom it's being given, and even

though the focus of this group is obviously not notice, I think it would be important in your report if you want to address how you view the notice principle as interacting with the access principle.

Ron? State your name for the record.

MR. PLESSER: Ron Plesser, Piper, Marbury, Rudnick & Wolfe.

I just ask the question of the subcommittee, I think some of these category areas were good, but I think there's one that's missing that I -- I think subparts are covered, but in the industry we generally talk about transactional information as information that ends up being generated from the transaction, and I know that some of the elements may be covered here, certainly online, offline contact information is important, but if we're talking about access in terms of what transactions you have had with the website as against, you know, some of the other inferred data and stuff, it would be helpful.

So, I think as we go into options, a category of transaction information would be extremely helpful, and I just have a question as to why it's not on this

list.

MS. MULLIGAN: May I just respond? Deirdre Mulligan.

It's covered in interactive data, actually, because on the web there are things other than what people consider to be transactions, as in purchases, that generate transactional data.

MR. PLESSER: I continue to -- I don't see them as totally together. I think that it would be -- I think it would be -- I think that presupposes a lot of other things, like clickstream and other stuff, so I think it would be --

MS. MULLIGAN: No, that's actually in a different category.

MR. PLESSER: That's not the way it reads. That's not the way I read it. I think there would be value to have transactional information there. If you want to read -- if it's the same thing, then call it transactional information, but I think that we're also looking and I think concerned about how this impacts, you know, the non-web world, and I just think some sense of identifying this stuff as the elements of a transaction are important.

MR. MEDINE: Just -- maybe Ron, just to clarify what -- are you just dividing information into

transactional information, perhaps clickstream or other information related to the transaction and then add on information that may not have even come from the

consumer? Are those three categories?

MR. PLESSER: No, I'm talking primarily about the interactions with the consumer. So -- but it would also, you know, it may reflect credit report information or other things that's gathered, but it's really information related to making that transaction.

MR. MEDINE: Okay, Dan?

MR. SCHUTZER: Dan Schutzer.

Two other things about sensitivity of information. One is I think we all have agreed sensitivity of information affects how you would store it and how you would protect the access, whether it's encrypted or not, and if you couple that with the cumulative effect you talked about, I think that really spooks people a lot. Sometimes you see things that are seemingly innocuous in the public, for other people to access, you're not controlling the access, and when you combine these, you say, oh, my God, now they have got my name and address with a map of how to get to my home, you know, and that sort of spooks people a lot.

So, I would say a category might be for those things that we think are seemingly innocuous, and we,

consumers, and the people providing the database,

somehow we have to come to grips with what is out there

in the total cumulative sense of public and what can be

done with it to both educate the public and ourselves, so if they find that sensitive.

The other aspect of sensitive is just a different kind of a way of looking at it. There is some data sometimes that I would call sensitive which is, let's say, if we're doing some kind of criminal investigation, but it's not sure, it's alleged, you know, we're just trying to collect this information, or if the government suspects money laundering or something like that, that's perhaps sensitive to not want to have anyone to have access to. It's only tentative. It's only investigating things, because we're asked to investigate or we're suspicious and we don't really have a firm case on it, and it would be premature or wrong to provide that information, perhaps.

MR. MEDINE: So, are you suggesting that there be an exemption where there is --

DR. SCHUTZER: Yeah.

MR. MEDINE: -- illegal activity involved where you --

DR. SCHUTZER: I think, so sensitive in that

sense, sensitive to not disclose the information.

MR. MEDINE: Okay, Lance?

DR. LANCE HOFFMAN: Lance Hoffman.

I think we want to keep in mind here, we're talking about the report of access of subgroup one, but, in fact, we were working on access in subgroup four, which dealt with a lot of these same issues it turns out, and if a picture is worth a thousand words, I would direct you to our picture, which Jamie Allen was in large part responsible for, which talks about a number of the same things, but it sort of sets up a framework where you can see all this and see how it might happen and where the data is going and that sort of thing.

Three quick points I want to make on that. One is we do handle I think the information Ron is concerned about, we call it metadata, and it's all the data about transactions or events or everything else, without getting more specific at this time, okay? So, there's both consumer data itself and then everything about what's going on with the consumer data, and that's handled in there, along with -- the other thing in terms of sensitivity is we provide there a sensitivity, you know, levels and so forth as a first cut, but I think someone said here a minute ago, which

was very important, which is these can be considered or

if you consider sensitivity, I think you have to

consider it as a default sensitivity.

I'm sensitive to Richard's concerns about the kind of databases that handle all this. On the other hand, as we say in the report of access four, the problem is that one size does not fit all cases, and people have different attitudes, and it's something we may have to address more, but I think it can all fit in this framework, in working it down. So, not to jump ahead, but we were covering some of the same material.

MR. MEDINE: I appreciate that, and again, I would encourage this group, if you think one size doesn't fit all, how do you translate that into an operational standard will be a challenge.

James?

MR. MAXSON: Jim Maxson.

I guess I've gotten a little confused about what we're talking about in terms of access here. If we're talking access simply in the sense do they have the ability to get to it, I don't think it makes any sense at all to link sensitivity and access. I mean, following up on Richard and Jamie's comments, if you are -- if you have a series of subjective determinations of what is sensitive to the individual

23 determined by that individual, then it would be

24 literally impossible to implement. So, I think that

25 sensitivity really is an authentication issue, a

security issue, and not so much an access issue.

MR. MEDINE: Well, let me just turn that around just to clarify it for the group, because some would say that you should not be entitled or provided access to every possible bit of information about you and the degree to which you should be provided access should depend in part on the sensitivity. That -- obviously I've just heard that from the group, but are you saying that that's not the appropriate cut on the basic question of who gets access to the information?

MR. MAXSON: No, I think probably a cut that makes more sense to me would be the feasibility of providing the information. I mean, one of the things that we're tasked at looking at is the cost of the, you know, proposals that could be implemented, and if there's essentially no cost to provide all information or very little cost, why not?

MR. MEDINE: Regardless of sensitivity?

MR. MAXSON: Regardless of sensitivity.

MR. MEDINE: And how would you assess cost on an operational basis or say for -- in terms of setting fair information practices or implementing those, how

would you -- would you do it on a company-by-company basis?

MR. MAXSON: Yeah, I think you would have to --

well, I think you could probably come up with a series of guidelines. Again, this is not one size fits all, but depending on the type of, you know, architecture that the individual company uses, the hardware/software that they have, I would say that certain types of information -- and I guess maybe I'm going to argue against myself here, but probably certain types of information absolutely you would get access to, and I guess that would be a sensitivity call, and then you would have whole other categories of information that just depends on how much it would cost to get to, you know, the ease of access.

MR. MEDINE: Okay.

Mary?

DR. CULNAN: I want to return to the transaction point that Ron Plesser made earlier -- I'm Mary Culnan -- and argue that, in fact, I think it is important to include transaction data, which involves a sale or whatever with a consumer, as a specific type of category, because in these cases, for example, the consumer has actually probably seen the data and has a record of the transaction if they care to keep it.

People obviously want their transactions to be correct, but they may put that data in a somewhat different category than data that is collected and

maintained behind the scenes, even though it's interactive data, but it's cookies or clickstream or stuff that the consumer has not seen and is presented with a record of after the transaction.

MR. MEDINE: Would you make a cut -- something that was alluded to earlier -- between personally identifiable information and nonpersonally identifiable information?

DR. CULNAN: Oh, yeah, yeah.

MR. MEDINE: And what would your cut be in terms of providing access to nonpersonally identifiable information?

DR. CULNAN: I don't see how you would do that, quite frankly.

MR. MEDINE: For instance, what if you had a cookie and you say give me access to that cookie transaction, even though it's not necessarily identifiable to me?

DR. CULNAN: I wouldn't define that as a transaction. I would define the transaction as an exchange where you make a purchase, and other things may be a transaction in another sense of the word, but

they're not a sales transaction or an economic transaction, and where you actually get a receipt or some kind of a record that itemizes what took place,

how much money was spent, and you get a printout of basically the information that was collected about that transaction.

MR. MEDINE: Okay.

Dan?

MR. JAYE: Dan Jaye.

On that first committee, when we looked at the different categories, we were trying to address -- use the categories as a way to help us think about the different levels of access, and then we -- the reason why it's a matrix is we ended up comparing the categories against the types of keys or identifiers by which you would actually get to data, and that allowed us to, for example, to distinguish between sort of the ease of identification and ease of access.

I think sensitivity is extremely important for the security aspects. I'm actually not necessarily in agreement that sensitivity drives what the categories are. I think the categories are driven specifically by the access requirements and that to some extent sensitivity may be a useful convenience as a way of helping us think about the different categories, but we

shouldn't get stuck on sensitivity as being the reason why things are in different categories. There are lots of other good reasons to break something into two

categories other than varying sensitivity.

And the final point in terms of sensitivity being a consumer centric issue, I very much agree with that. I do think that it may be useful to think about data source or data controller as a way of thinking about how things are categorized or set -- or how sensitivity or access requirements are determined.

In other words, it may be that the data source or the data controller has some degree of expressing what the expected future access requirements are. So, once again, data that's generated cooperatively or generated sort of on, you know -- like, for example, derived data is generated by a service. Once again, I would say that the service probably has some degree of influence over the access requirements to that data, but at the same time, if it's highly sensitive and is being used for making -- for decision-making activities, then that might then bring on additional access requirements for the consumer side.

MR. MEDINE: Just -- you would -- you raised one point about sort of accessibility to the information or keys to the information. Is that --

would you view that as another cut in terms of when access is provided in terms of how essentially easy it is or capable the firm is in terms of aggregating the

information to provide to the consumer?

MR. JAYE: Yes, I -- one of the late cuts of the matrix that we put together, I'm not sure if it was -- was that -- was the idea of trying to matrix the categories against the types of identifiers, whether they were personally identifiable information, like name and address, sort of online contact information, offline contact information, globally unique identifiers, locally unique identifiers, that there would be different implications depending on each of those, because implications of the data were different in each of those situations.

MR. MEDINE: Okay, Alex?

MR. GAVIS: Alex Gavis, Fidelity.

I think to some extent, in terms of setting up access, we can probably fairly easily sit down and come up with sort of categories of data that we think would be important to provide customers access to. I think what's a more difficult decision here is at what point does the data actually sort of escape the consumers' hands and become derived data? And what I mean by that is when essentially a company collects data about an

individual, if an individual voluntarily provides

information to open up an account with a company, for

example, the company has to then do a certain amount of

scoring with that customer, as was mentioned earlier, or perhaps even checking for fraud purposes, et cetera, and then there are decisions made based on that data, and to what extent does the access then pierce through the company into its decision-making process?

And I think that's really where the debate has -- is going to be tough going as opposed to figuring out, well, can we say that this kind of information fits in this category or that category? I think we can do that, but I think where we really are going to struggle is figuring out how far do we pierce into the decision-making part of the entities that are collecting the data.

MR. MEDINE: So, one cut is to give consumers access to the raw data and not to the essentially manipulated, analyzed, scored data. I guess if people have views on that subject, that would be helpful.

Fred?

MR. CATE: Thank you, Fred Cate.

I think in response to your question is sensitivity the touchstone, the answer as a member of the subgroup is no, that it's one, but that to some

extent the whole list of categories on the second and third pages are relevant to saying what type of access, how much access, what have you.

I guess the point I really wanted to follow up on, though, was the one that James Maxson made first and that others have also followed up, this idea of the interplay between cost, feasibility, and he was talking about sensitivity, that maybe for more sensitivity, we'd be willing to see a higher cost incurred to have to provide access. I would guess that interplay would extend, though, to other criteria, as well, including some really we didn't identify, for example, the purposefulness of the data collection.

Is it just incidental? Is it just data that -- you know, you're an ISP, you happen to have this data because it flows through you, but you don't have access, you never make use of it, it's stored on a backup tape. I think that would be treated differently than a database you used routinely for market purposes.

The source of the data, is the source something about an individual that the entity storing the data generated? Is it third-party information, in which case is there a confidentiality interest related to the third party? You know, where did this data come from?

Another source question is is it public source

data? If this came from an entirely public source, something, you know, we have all been talking about recently, what effect does that have? Do we want to

incur as high a cost to provide access to data that was routinely provided publicly as we would to data that would be considered private?

And also to the extent, how is it personally identifiable? It's interesting, one thing we sort of never said in here is, of course, personally identifiable, that's the touchstone, that must be first personally identifiable, but I guess I would also like to add to that list, how is it personally identifiable? Is it by something that is unique to that individual name or Social Security number? Is it purely by an IP address? What makes it personal data in that sense?

Thank you.

MR. MEDINE: Just to follow up on your first point, the purposefulness of the information, I guess the collection and use, we earlier talked about the notice principle. To what extent would you tie that to notice that is -- from a consumer's point of view, if they don't know what the company's doing with the data, the purposefulness may not be a relevant determinant in terms of providing access? That is, they know the company has the data, but they may not know what the

company's doing with it. Therefore, they want to see what's going on, but would you link that to the notice where the company says we just collect your data for

this limited purpose but no other, and therefore it makes access irrelevant?

MR. CATE: I think you certainly could. I think you are going to end up with multiple categories, so you have a situation where frankly there is no access and no notice because there is no direct relationship with the consumer to start with, and that to my mind would be the third party who's just processing data along a chain from point A to point B on the internet. If it happens to get stored in our server along the way, I'm not sure we should have to identify those people to provide notice or provide access to it. We're not accessing the data in any way. Why should anyone else be able to access it?

There might be the second situation where you say notice is appropriate and appropriate -- and access is not, so that we provide notice and it says, as part of operations, we store e-mail messages on backup tapes, and -- but we're not providing you access to those backup tapes unless you show, you know, require a specific showing, probably some form of wrongdoing or something like that.

And then there might be a third situation or there might be 300 situations where you would say notice and access, and of course, they are closely tied

together.

MR. MEDINE: For the record, Stewart Baker is here.

Lorrie?

DR. CRANOR: Hi, Lorrie Cranor.

Two points. First, on the sensitivity, while I think that it makes sense that the individual ought to be able to best judge the sensitivity, I don't think that's something that individuals can judge. I don't think it's a meaningful question to ask somebody how sensitive is a piece of data, especially when asked out of context.

You give people a long list of data and say, you know, tell me relatively how sensitive this is. That's just not a meaningful thing to do. I think people may be more concerned about how data is used, but the question of sensitivity I think is too abstract here.

On the access, I was reading the information that the BBB provided us and their statement on the kind of access that BBB seal holders have to provide I think is maybe a useful starting point, where they

don't have a precise definition but they do talk about whether the company itself has access to data in their normal course of business, and I think, for example, if

there's a company that routinely creates a database record of a person's data and uses it internally or shares it with another company, then clearly it's something they have their hands on, they can feasibly provide access, and not only can they do it, but it's data that they are accessing, and I think there's a big distinction between that and stuff which is stored on backup tapes somewhere and nobody is actually accessing.

MR. MEDINE: Ted?

MR. WHAM: Ted Wham from Excite@Home.

I have two points. First of all, I want to say how happy I am to be part of the club that understands how these things go up.

MR. MEDINE: There are some benefits to being on the committee.

MR. WHAM: Exactly, you have got to get on the inside.

The second thing, the discussions that we have had here about the valuation of data and the -- and from two different perspectives, so first of all, I think it was Dr. Gavis who made the point -- I can't

quite see your name -- but he talked about how the

combination of data elements are working not in a

linear manner but in a geometric or exponential manner

as one issue, and the second thing brought up by a couple of different people, I think Dr. Schutzer brought this up, about how the consumer has to take and make a judgment about the data element. Both of those are taking and adding levels of complexity to the data construction that are very troubling to me.

I think when we look at data, we're going to have a lot more success in terms of coming up with recommendations in terms of looking at things. If we can say a data element is what it is, a birth date is what it is, very black and white, has the following type of meaning, and it has the following type of access requirements and needs within the industry as a whole.

There is many instances of people who would say that their address is very personal information, but there's a long history of government programs that require the provision of a physical address for you to be able to use those. There's many people that would say that their children's Social Security numbers are absolutely critically personally identifiable information, highly sensitive, yet we routinely require

that parents provide the Social Security number of their children in settings for health insurance, in settings for IRS filings, et cetera, to be able to do

those types of things.

We don't look at -- we don't let the consumer come through and say you can't have this type of information, and I would think that as a means of, you know, providing standards of behavior, it's almost impossible for the industry to come through and say, I'm going to do a combination of the number of data elements that I have crossed by the individual consumer's sensitivity of that data element, I don't know how I'd get there. And I think that was the point made by Mr. Purcell from Microsoft.

The points about sensitivity of information, and I sat on the committee, so I'm very familiar with the construction of some of these elements, is that there are some elements that you would come to and that we would all likely agree, in a very broad consensus, are sensitive information that would have a higher threshold for disclosure and a higher threshold right for provision.

Your -- whether you tested positive to an HIV test is something that I think most people in this room would agree is highly sensitive information. That's

just not something you want spread around in a great degree of freedom, but it doesn't change the fact that that data element has a certain threshold in all of its

applications. Either you can share it in a given circumstance or you can't share it, and it gives a standard of behavior which industry can meet.

MR. MEDINE: So, I guess which way does that point -- if it's too complex to have the interplay between the various data elements and consumers' sensitivity about those various data elements, how do we go about defining the application of access?

MR. WHAM: I think we look at it and say what is the nature of the relationship, how the data was provided, what is the nature of the use of that information, and what is the nature of the sensitivity. So, those are the first couple, you know, bullet items out of the committee's work itself, and from that you come up with very black and white, deterministic methodology about whether you provide access to that information or whether you don't provide access to that information, that industry can now have a test it can hit as opposed to a wishy-washy, well, in some cases you have to provide access to it, unless it's being used in this following different manner, and so forth.

That was one of the reasons why we spent so

much effort breaking out the categorization itself, is that we said there can be disagreement between, you know, two honorable men about whether access should be

provided to a specific area, and I think Deirdre and I, you know, might go to hammer and tongs over some of these issues, whether we would provide access, but at least you can say that it fits within this bucket, clickstream data, for instance, fits within this bucket, and we come to a set of recommendations that may not have a unanimous opinion, but we do say it is black or white so that the FTC and the members of industry and so forth can know what they're doing in a very clear manner.

MR. MEDINE: Okay, Frank?

MR. TORRES: Frank Torres with Consumers Union.

There's been a lot of comments about a lot of different issues, and it's tough to keep track of everything that's being said as we go around the table, but I do want to touch upon a couple of points that have been made.

One is trying to draw the distinction between kind of public versus nonpublic information, and I was reminded in an e-mail that I believe Beth Gibbons sent to me that said, you know, it used to be kind of a given that names and addresses were public information,

they are published in telephone directories, and I forget what the percentages were, but there's a large percentage of people who choose not to publish their

names and telephone numbers in telephone books. So, we need to be sensitive to that, that we can't have some of the assumptions that we have had in the past.

The point that was made on, you know, maybe the benchmark should be feasibility and cost, and I was glad to hear the comments about, well, if this data is being collected and used and shared with, you know, in the financial services context, a third party or shared with an affiliate, then obviously that information is in a form that could be provided to the consumer. And I would take it that in those cases, perhaps decisions are made based upon that information, and this gets to the -- you know, this is the raw data that goes into the black box that gets to the credit score that consumers have access to in one way under the Fair Credit Reporting Act.

You know, I think at a minimum we need to use that as a guide to, you know, maybe some types of information where decisions are being made about you. You know, since decisions are being made about you, to me that says inherently it's in a form that is accessible. It's a little bit different than the data

that's kind of out there being stored.

And I guess excuse me if I'm a little bit

naive, but why would companies have all this data

stored that are just sitting out there, you know, that just -- you know, I have heard that from a couple of folks, saying, you know, we have this data and we store it and it's on tape but we are never going to use it for anything.

MR. MEDINE: You drew a line between decisional kinds of data and sort of the raw data that goes into the decision-making process. How far up the -- because it was raised earlier, how far up the chain would you go in terms of providing access? Would you provide access to the --

MR. TORRES: I think that's -- Frank Torres again, but that's a question that we need to address, because, you know, in Europe, thank God, when you provide information, when you go into a bank to get a loan, they have got to get your permission before they use it for any type of secondary purpose. Without the same type of protections here, just in the realm of privacy, let's say, that information that you provide to, say, a lender here gets shared with, you know, who knows who down the street and is being used for all sorts of other purposes.

I think it's important to look at all of those downstream purposes, and to a certain extent, you know, maybe we do need to provide some access, you know, for

the downstream uses, especially as information gets commingled and then that information is used to make a decision about you.

MR. MEDINE: Andrew?

MR. SHEN: Andrew Shen.

Back to I guess a couple of older points about the transactional information. I think the categories that were provided in the access one outline sort of enveloped that. I think if you look at interactive data --

MR. MEDINE: Could you grab the microphone so folks can hear you? Thanks. Just speak right into it, yeah.

MR. SHEN: Well, back to transactional information, I think the access one outline does cover that category, and I think we have to be aware that there's lots of other types of data that are collected that do not necessarily indicate a single commercial transaction. I think everyone around the table knows that's a very controversial topic right now.

Second, Frank kind of stole this point, but I think it's a key point. I mean, why is all of this

sort of information that's generated and kept around, why is it stored? I mean, you can relieve a lot of the responsibility if you just -- on security and access if

you just delete that information. Why do you have it?

The other question that came up earlier is maybe one cut that you provide access to is information that was provided as opposed to information that was sort of derived or inferred. I think one of the important reasons that you have access and why it is a fair information practice is so you can know about that provided information, know what else has been done to that that you don't really realize is being done. You really want to know all that information, what you may have not known at the outset.

MR. MEDINE: John Kamp had his hand up a while ago, if you are still interested.

MR. KAMP: Actually, the point was already made, and Dan Jaye has a point I want him to make, actually.

MR. JAYE: I just want to address the issue of why that data is kept on tape and archived. The primary use is for audit purposes, is that you have to keep some data around in certain applications, because you may be audited later on, to say your numbers were correct, your ad tallies were correct. It's not

because it's going to be used for -- on a consumer-specific basis for making decisions about the consumer. It's actually -- it's a record of your

business, and if you -- there's some cases where you can destroy records of your business and there are other cases where you can't.

MR. MEDINE: Okay.

Richard?

MR. PURCELL: Thank you, Richard Purcell.

Perhaps it may be helpful if we think about this area of our work in a classification system, which would include perhaps three elements, and, of course, three-dimensional matrices are difficult, but at least they let -- they lend themselves to the derivation of database rules which allow for an accurate management of customer information, and I think accuracy of managing this customer information and interactions is a key goal we have to keep in mind.

We can easily define such a complex, and if we come up with nonimplementable system, what will suffer is the accuracy of our data management practices, which would be a complete waste of all of our time.

What I would suggest is perhaps a system whereby we have classifications of data, which would include sensitive, nonsensitive and perhaps other

classifications, categories of data, which they've done a good job of here in detailing -- I've got a couple of additions I'd like to add to that -- and sources of

data, which could include customer-contributed, captured, could be derived, could be inferred or could be third party. There I'm sure are other values that we could put into that.

But the intersection of these three types, whether it's sensitive -- let's say there's a piece of sensitive information that intersects at the same time with a category of information that's interactive which also is sourced from a third party. Let's use Ted's example of an HIV-positive diagnosis. That's clearly a sensitive piece of information. It's clearly a -- could be seen as interaction in the sense that it is a diagnosis, and it comes from a third party, and a pharmaceutical company for some reason gets that.

Given those three values, a database rule can be written for the discrete handling of that bit of information. That rule might be different if that same data element came with a different set of three criteria or values, if it was sourced differently, if it -- well, that same one is always going to be sensitive, so I can't use that, but if it was, for example, perhaps categorized differently. So, there

may be ways that we can create a dimensional matrix.

The other thing I'd like to just suggest as additions to the categories are identifiers that

include biometrics. We haven't -- here we've talked about numerical identifiers, GUIDs and LUIDs, that's a new one, but I think that also we have to anticipate that there's going to be perhaps even a category of data that is -- that are -- can be called identifiers, and GUIDs are not the same as an identifier -- as a biometric identifier in that they are ambiguous. A GUID can be shared by -- because it's a machine-based element, but a biometric is so unique as to be unambiguously identifying an individual human being.

The other I would suggest are authorization levels, essentially the privileges that an individual has for access to information. We have to keep in mind that -- and we'll get to this in the -- in our subgroup four's area, but we have to keep in mind that we're not necessarily defining access limited to the consumer's access to data. We also have to be sensitive to the fact that there are a bunch of human beings operating this -- these systems. They also have access to this information.

What are the rules that we're going to lay out that a system administrator or a database manager is

going to have in terms of access? And so authorization levels apply very strongly to that category, but they could also apply to consumers accessing their

individual data.

As an example, what is the authorization level of a parent to get access to their child's information?

MR. TORRES: Dave, I just have a quick question, Frank Torres.

When you talk about a database rule, what does that mean? Is that a code that's written or is it just a policy that is enacted?

MR. PURCELL: Thanks, Frank, Richard Purcell.

A database rule is essentially a script that is invoked when a data value is entered into a system, and that script is an instructional that tells the system exactly how to handle that piece of data in a very highly specific way. For that reason, any ambiguity around that can create grievous errors, and in this area, an error could expose data in a manner that is against policy and that may be against an agreement that you have with your customer, as well.

MR. MEDINE: I want to go on around, but before I do, I just want to inject another issue for people to consider if they want to address it either now or later, which is access by people with disabilities, is

that a -- that was not addressed in the first group's discussion, but it might be relevant to determine if there ought to be special considerations in that

context. And again, people can feel free to address that now or perhaps in the working groups for the next session.

Ron?

MR. PLESSER: Unfortunately, this is kind of like an online chat room, we are all coming in at different points, but there were three points that I wanted to make.

First, on behalf of the ISP industry and why there's backup, I mean, it's obviously for disaster relief, for -- you know, if there's a breakdown, you know, different policies -- different ISPs have different policies in terms of when e-mail is looked at, you know, is it destroyed as soon as the recipient picks it up, well, how long does it take for the recipient to look at it, what are the outside limits, but primarily, at least in -- and I certainly agree with what Dan Jaye said about auditing, but I think it's very critical to know that, you know, as we've seen in the last couple of weeks, one of the critical elements of the internet is reliability and dependability and trying to build that up, and one

needs the backup tapes and backup information to do that. That's not the only reason, but it's certainly one reason.

Second is on this issue of sensitivity, I don't know that I disagree with what anybody has said, but it seems to me we're losing or missing a 30,000-foot view, which is sensitivity does vary as to sector. When we did the Privacy Commission report in the mid-seventies, the way we dealt with sensitivity is really looked at sectors. Name and address may not be sensitive at all if it's derived from a real estate record or from a public telephone book, nonlisted or whatever. It may be entirely different if it's the name and the address identified with a cardiac rehab clinic or something of that nature.

So, I think what we really -- the way -- I think one of the ways to solve the issue is to look at sectors, and it's not going to solve all the problems, but it starts to give you a cut that is helpful, and I guess I'm just surprised hearing this conversation go on for an hour and not hear that there's at least some difference on sectors.

Third, on the issue of the transaction, I'm not suggesting in the least that interactive data be eliminated from this list. I think it's helpful and

it's important to have it. What I am suggesting is there should be a separate category, if you want to technically call it a subcategory or a separate

category of transactional information, because not only from what Mary had said, but as we are now getting very much involved in consumer protection issues, one of the fundamental consumer protection rights is that the record of the transaction off the net be recordable on paper, be -- or recordable in some form and that the -- and then maintainable by the consumer, so that transaction information is becoming an important category.

Interactive data should stay in there to the extent that it doesn't cover transactional, but I think as we go into the options, if we lump them all together, it will be much more difficult to get to some resolution than if we try to split it out. So, that's my point on that.

MR. MEDINE: Okay, Ron, just going back to I guess Richard's matrix, Ron, would you then make sector one of the determinants in Richard's matrix of what information you get access to?

MR. PLESSER: Yeah. I mean, I -- I mean, it was hard to -- for me to kind of fully conceptualize what Richard was saying, but I think that in splitting

it up, certainly sector is an important issue. And I now have his diagram.

MR. MEDINE: Let me make an important access

point for this committee, which is the people in the overflow rooms aren't getting access to this information unless you speak into your microphones, so please when you're called upon, put it close to you so that folks in other rooms can hear you.

Deirdre?

MS. MULLIGAN: I think you've done an excellent job steering the conversation, David, and I want to step back for a second that the purpose, at least, the purpose of the scope and categories group I think from the focus of the -- from the perspective of the people who were on the group was to set out the framework and not to make the decisions, and I think that there's a number of things that have come up. I was also on the cost and benefits subgroup, who have highlighted for me the fact that these are useful in conceptualizing the other issues.

For example, Lorrie Cranor raised the point that, you know, in thinking about access, a critically important component is is it data that's being used in a form that is tied to the consumer. And I think that if you look at the cost and benefit paper and you apply

it to this, you say, what form is the data in? What kind of system? Is it a transactional log system of people's records, you know, stored by a credit card

company where they're routinely used to make decisions and they're, you know, collated with the person's name on top?

And so that the -- you know, the purpose of the scope and categories was hopefully to provide, as I think Richard said, one axis to feed into this rule set, and I think the discussion has been really productive as to what are the other axes. I think, you know, from my perspective it's come up pretty clearly that in thinking about access, many of us don't believe that sensitivity is an important -- an important factor to play into that rule set; however, we do view sensitivity as being a critically important component to play into the security rule set.

And I think -- you know, so I think we're starting to pull that apart. And I'd like to hear a little bit more from other people about if you're thinking about -- which I think is important, because I think the cost issue is one that might be very important as to where the FTC comes out on this issue, but in thinking about how you reduce costs, coming up with clear, simple rule sets that can be built into

programs and systems is incredibly important, and so I really appreciate that Richard Purcell brought us back to that, and if we can think about some of the other

fixed axes that would be useful in the access section, I think that would be great.

MR. MEDINE: Also, just keep in mind that simplicity benefits consumers in understanding what they're getting access to.

MS. MULLIGAN: Absolutely.

MR. MEDINE: And obviously benefits firms in understanding what they need to provide access to.

Rob?

MR. GOLDMAN: I guess listening to the discussion, I want to weigh in a little bit on use and making of decisions with information, which has not been brought up as one of the dimensions on the three or four-dimensional cube but one that is interesting at least and seems to find its way into most of these outlines somewhere.

I want to share an experience that I have had at my company since these outlines have been circulated that makes -- I think use is a difficult one, a difficult one to work with. It's interesting but hard in practice. Dash.com is a startup. We provide customers with access to almost all of the information

we collect on them. There's a small piece of information which is the operating system they used when they signed up for our service which is not

currently part of their profile page.

We work with online merchants. One of our salespeople during this past period was talking with a computer retailer about making offers to members of our service for no-money-down financing for computer. Right now we don't provide access to that old -- to the operating system variable, but that variable is one that we wanted to consider in choosing who to -- whom to make the offer to, who would be likely to be in the market for a new computer.

It's not something we provided access to, and it's something that we were considering using. So, I guess the question would then be, when do we need to provide access? Is it after the decision has been made already? That's a little late, it would seem, but it's hard to know how information will be used ahead of time. And just to further complicate it, I've seen financial decisions, credit information and loan decisions throughout these documents, and zero-money-down financing for a six-month period could be considered a credit decision, as well, which -- and I'm sure our merchant would have considered it a

marketing decision, but I guess that line is vague and difficult.

So, in practice, use, although important, seems

like it's a hard one to pin down and certainly would get away from us, I think, in industry.

MR. MEDINE: Dan?

DR. GEER: Yes, Dan Geer.

The only point I wanted to make is to the extent we're trying to imagine the future in making these rules, I think it's worth mentioning that in a very short time, the number of devices that are on networks and the number of entities which are making and breaking connections and all of that will be totally dominated by things that do not have a keyboard. Your refrigerator, your car, you name it, everything will be there, and the information that's hardest to deal with in that circumstance is what I believe would be called traffic analysis. Who's talking to whom and when and what did they say?

That kind of stuff is, on the one hand, a rich mine, and on the other hand, it's a rich mine, and the question is which way do you want to go, and I just want to make sure that everybody understands, just as the comment was made about biometrics a moment ago, the technology frontier here is advancing at a speed which

I think is going to be very difficult to anticipate in a rulemaking proceeding such as you're attempting to go to.

MR. MEDINE: Let me just clarify for the record, this is not a rulemaking proceeding. This is a committee that's going to express its views independently to the Federal Trade Commission.

DR. GEER: Okay, sure.

MR. MEDINE: No rules being promulgated here.

DR. GEER: As a layman, there are words I'm sure I will step on, as that was one.

MR. MEDINE: We just need to keep the record straight.

DR. GEER: Okay, cool, but I just want to make the point that the technology frontier is advancing, and what is interconnected is advancing at a very fast clip, and the large -- the majority of the internet will be wireless in almost no time and so forth. So, as we think about this, we cannot imagine that there's going to be a person to ask of -- a decision of. It isn't going to be there. You're not going to ask my refrigerator how it feels about whether or not its contents ought to be visible to the grocery store. I mean, you are just not going to do that.

MR. MEDINE: Can I just turn that around, then,

because there's been a discussion back and forth

earlier about whether companies keep information, why

do they keep information, how do they use the

information they keep. To the extent that a company keeps information about your refrigerator's habits identifiable to you, should that be a determinant of your getting access to that program?

DR. GEER: There are other people here who understand that far better than I because they do, in fact, have those types of requirements, and they are not optional, but I would say that if you are worried about the reliability of a computing environment, you record as much as you can if for no other reason, for instance, when things go to hell, and the last couple of weeks have been a good example of that. If you didn't have the kind of data that scares you, you wouldn't be able to diagnose the problem you didn't know was coming.

MR. MEDINE: Just to clarify, it's not so much then what you keep but what you use, and if you use that refrigerator in association with a person to --

DR. GEER: I cannot make a distinction between keep and use, because the cost of reproduction of electronic information is zero; hence, it is never unrevealed; hence, once it exists, it exists.

MR. MEDINE: Rick Lane, did you still have a comment?

MR. LANE: No, I didn't.

MR. MEDINE: Lance?

DR. LANCE HOFFMAN: Lance Hoffman.

A couple of points, and this is a very good segue into what I'm going to say. We cannot predict the future, but we have to design for it anyway. That's one reason I think we came to that figure we have in access group four. And Richard has a model of keeping himself in check. He only showed it looks like a telephone and a regular mail and a computer. We talked about refrigerators and cars and all of these things. He didn't put them up there. He was very, you know, sedate that way, but they're coming, okay?

So, the point is we can't predict what's going to happen, but what we do know is we don't want to make rules -- sorry, I'll change that expression -- we don't want to make decisions that are so binding that they get us in trouble later on. We don't want to come to standards too early.

Having said that, I think time may wish -- we may want to consider time as another access of some sort, because time has been left out here, and things change over time, both the decisions, the access rules,

whatever, change over time, and as we've seen in recent weeks, companies' decisions change over time. They might say at time T-1, we are going to do this with

your data, and then at time T-2, lo and behold, they change it, maybe without even telling the consumer, and what do you do then?

Well, the key here is the records. If you have records and if you keep records, then you can go back and assess what's gone on, okay? Record keeping I claim is a cost of doing business. You're absolutely right, the point was made earlier, lots are kept for auditors. Indeed. Well, the consumer more and more can be his own auditor. You're already your own auditor when you read your bank statement, okay?

So, I don't think it's any different. I think one of the costs of doing business is being able to keep additional records about the metadata that is in these systems.

Final point -- oh, two other points. One is Ron talked about sectors. Sectors are a good way of categorizing, but they don't always work. We see these conflicts all the time between the U.S. and Europe especially in terms of privacy and regulation versus not. Ron Plesser, I guess he's not in the room right now, I'm sorry, but he gave the example of real estate

records, but, in fact, you can go on the web, and it's been widely publicized, look up -- combine real estate records with where people live, and there are, for

example, anti-abortion websites that say, you know, here, target these doctors and that sort of thing, very frightening kind of websites in the opinion of many people, perfectly, you know, legal I gather. That's another thing to consider.

The final thing on disabilities, as I move back and forth here, the Worldwide Web Consortium has done a very good job on -- I forget -- what's it called, the accessibility project or something like that -- accessibility -- WAI, Web Accessibility Initiative, and if you just look at that homepage, there's tons of stuff all related to this, all of which could probably just be logged in lock, stock and barrel.

MR. MEDINE: Let me throw out another issue for this group to discuss later today, which is the issue of correction of records. We're -- obviously once someone gets to see their record, one possibility is they will determine that the information is incorrect in some fashion, and I would encourage people, if they wish, to address the issue of people being able to correct the records.

Alex?

MR. GAVIS: Just to clarify a point earlier that was made about how long or why do companies keep records, I mean, particularly in the financial services

area, we have a number of books and records requirements, both from banking and securities regulators, which require us to keep information, you know, for three to five years.

In addition, we have suitability obligations. When we are actually going to make a transaction, we have to collect certain information to make sure that the customer was aware that it was suitable for them.

And then finally, in addition, for auditing purposes, we keep it for litigation purposes, because if there is ever a dispute later on as to a transaction. So, there are a number of things in our industry. I think there are probably similar requirements in the health care industry, although I am not an expert in that area.

MR. MEDINE: Greg, did you still have a comment?

MR. MILLER: It was made.

MR. MEDINE: Dan?

DR. SCHUTZER: Dan Schutzer.

I would like to clarify that when I was recommending the sensitivity, it was that for the

purposes of what we're talking about, data access and security, we should be more concerned with the sensitivity with which data is handled and to which

access is provided and the sensitivity to an individual.

As an individual, certainly when I see the data type and you tell me how it's used, tell me who you're sharing it with, I make my own determination as to how sensitive I am to the data, but another factor in determining whether I want to provide you that data or not is how you're going to store that information and how you're going to make it accessible. That's to say that if you came to me for a loan application and you ask to provide my Social Security number and I feel you're going to safeguard that, encrypt it, and it's only going to be accessible when I want to look it up, used in the way you demonstrated, that's one thing, but when I go to another site and they request information about my Social Security number and they are going to make it available by just public directory yellow pages, that's a whole other thing.

Another issue is if we're looking at these new devices, before we get to the refrigerators, we have set top boxes, and when you start to look set top boxes and cable head-ins, sometimes the information that's

stored in cookies, which is sometimes unencrypted, is

now stored in a head end, okay, run by system

administrators and sometimes accessible to people who

can penetrate that. I'd like to know that, because that will determine and influence whether I want that information provided to that party or not.

MR. MEDINE: Okay, thanks.

Stewart?

MR. BAKER: Thanks, Stewart Baker from Steptoe.

I appreciate now the difficulty of this, and I thought I would draw an analogy to the Freedom of Information Act, which I think in many respects we are creating for private industry here. FOIA has value, but it is also abused routinely in ways that probably should be considered here as we think about how we want to structure an access rule, and I'll just sort of throw out three ideas.

You know, the biggest -- among the biggest users of FOIA are competitors and other ill-wishers who are trying to find out information about other people who are being investigated, and that really obviously raises the question of people utilizing the access rules to find out what the business methods of competitors might be, how are they evaluating data, what process do they roll it through, what kinds of

criteria do they use to evaluate a particular application or customer just on their own, and we have to -- when we talk about inferred data, we have to

think very seriously about how do you protect proprietary methods of analyses.

The second thing that happens in FOIA -- here's a story, I don't know how many of you have had background investigations, but if you have, you should FOIA the records of that background investigation. That's something I did, and it was quite interesting. The government went through quite carefully, they had all of the interviews that they had done with everybody who had ever smoked tobacco with me, and they carefully blacked out the names of the investigators to protect their anonymity and left in the names of all the people who were talking about their experiences with me.

And it occurred to me that probably from the point of view of those people, this wasn't the best way of dealing with the situation, but that raises the question, what do you do with third-party reports? What do you do about complaints from a chat room directed to a particular e-mail address or screen identity? Almost any information supplied by a third party has the potential to put that third party at risk in the wrong circumstance. And so including

23 third-party-supplied data in the access is going to be

24 a serious problem.

25 Finally, occasionally -- this also happened to

me. This is the last personal story. When I worked -- after I left the government, somebody filed a FOIA request asking the National Security Agency to compile a dossier of everything they had on me, you know, all the documents that I'd seen, touched, written, et cetera, something that the National Security Agency is actually prohibited by law from doing except when somebody files a FOIA request to do it, and I think that raises the question of do we want to use this to create -- the real irony was it was a so-called privacy group that filed it -- but the question is do we really want to have databases assembled in order to provide access?

And I recognize Dan's point is quite good, of course, it's all theoretically part of a database, so you can't really separate it in theory, but if you're going to have a test, I think here it needs to be is this the kind of search, the kind of database that is used routinely by the business, because if it's not, it's going to be very expensive and we're going to be encouraging the creation of links that don't exist now.

MR. MEDINE: Thanks.

Given the hour, it looks like we have about five more comments, Josh, Frank, Dan, Ted and Larry. We'll start with Josh.

MR. ISAY: Hi, Josh Isay.

I was just going to go back to sensitivity for a second, and maybe what we should be considering is the sensitivity of use as opposed to the sensitivity of the data itself as another cut at this. So, for example, if it's an address by itself, that may not be sensitive. If it's an address used to decide your auto insurance rates, maybe that is a sensitive use. So, it's just another cut at it.

MR. MEDINE: Frank?

MR. TORRES: I share again just a couple of comments. First, if my refrigerator knows my eating habits, is it the one that gains the weight? And will we reach a state where we program in our diets, so when I run out of ice cream, it refuses to order it for me? And I mean the technology is just fascinating and this discussion has been eye-opening. I thought I knew a lot about what was going on, but I realize I know very little actually.

On a couple of points, just one, I think it's crucial that we address access for disability. Hopefully that will be a very uncomplicated section to

get at, but I do think we need to contemplate that here.

You raised the correctness of the records, and

I know a lot of the subgroups are trying to get at that, when is it appropriate and when not, and just some initial comments that I think it's worthwhile for both the consumers and the business community to ensure that whatever records are floating around out there are correct for a number of different reasons, I think.

But you know, again, going back to the decision making, I think that's crucial. The decisions that arise, of course, are what do you need to correct it? You just can't go in and say my credit report's wrong, I want to fix it, so change these numbers and these numbers and these numbers. You have got to have some backup. But also in the same vein, it should be very easy for a consumer, you know, to be able to get in there and correct it.

Just over -- and to get to Stewart's points about, you know, information being used by competitors and the risk of third parties, I mean, I think we're coming -- at least Consumers Union is coming at this from the perspective of trying to be very reasonable about different approaches and realizing that it -- in the area of financial and medical records, it's

important to take a look at exactly those types of issues, and I think it goes to who actually has it. Is it you -- how do we authenticate, actually, who

actually has that access and when is it appropriate for somebody to have that and, you know, maybe can I give my permission to somebody else to have access to those records or not? These are just issues that I think we need to get at during this discussion.

MR. MEDINE: Dan?

MR. JAYE: I just want to make a comment about the practicality. When we talk about access, I like to hear the online discussion very much, but I think there are -- once again, routine use can be interpreted a number of different ways. I just want to point out, and I apologize, I have a background in parallel databases, but there is a fundamental difference between random access and sequential access to data.

For example, a credit card company doing credit card scoring may process millions of records, but does that mean that they have an index on that table that allows you to randomly go in and select a specific set of transactions and retrieve it in realtime for a consumer to access? That's not necessarily implied, and that the rate of growth of the internet does exceed Moore's law, which is the rate at which CPUs are

getting faster, especially with the proliferation of wireless devices, and at the same time memory prices and memory -- the amount of memory on computational

equipment is not getting significantly cheaper year after year, and then finally, the time it takes for a disk drive to do a seek to retrieve a particular record has not significantly changed over the last ten years, and, in fact, as data increases and disk drives get larger, that problem is actually getting worse and worse.

So, in fact, there are compelling cost savings for companies to keep data in forms that allow for occasional use for processing, for statistics, for reporting, but not necessarily allowing the massive volumes of particularly transactional and interactive data to be available online.

MR. MEDINE: Those are actually excellent points for our access three discussion on costs and benefits, and I hope we will revisit some of those.

If we could just have two more brief comments from Ted and then Larry.

MR. WHAM: Ted Wham with Excite@Home.

A couple of quick points. I wish I could claim this as an original idea, I don't know to whom to attribute it within this group, but in terms of

correction of info, I think we might want to consider having a correction of information as part of the access requirements only for the information that the

customer directly supplied themselves. There is other information which we are going to have about that customer which is simply not going to be correctable. If we think that they ordered three books and they say no, I only ordered two books, well, do we go and correct that? Do we provide access to it?

If they say we didn't see that page, well, we think you did, is that something they should have access to? So, I think it should be the personally supplied information that would be the most minimal to correct.

Secondly, with privacy information and references, the point Stewart brought forth, recognize the privacy threat brought forth simply by correcting those references. So, if somebody says they don't mind providing their birth date information and so forth, to what degree are you creating a profile about that information that creates in and of itself a privacy risk?

And the third point is that for any type of discussion that we have had around customers or consumers being able to specify their own interests of

23 privacy of a specific element, recognize that that's

24 going to be an extremely difficult implementation in

25 the anonymous type of data which is collected, you

know, in mountain folds out there on the internet. So, how do I take a customer who I don't know and allow them to tell me what their preferences are in terms of the sharing of data?

MR. MEDINE: Larry, final comment before the break.

DR. PONEMON: I fortunately only have one point, and I think -- but it's a long-winded point, actually.

MR. MEDINE: So, there's good news and bad news.

DR. PONEMON: I'm a little disappointed, to be honest with you, because I think we're missing the -- that we're missing the big picture or the boat, and the big picture and the boat is we all bring certain ethical frameworks to this table, and quite frankly, until we tackle the big issue, and the big issue is -- I know we're not setting rules, but what we do here may be useful in setting rules. That's my understanding of our assignment, and if that's, in fact, true, before we get to rules, what framework are we going to rely upon? And I don't think any of our work, including our

subcommittee, really addressed that issue.

So, I would like to maybe move back a little bit, maybe we can do this in the afternoon, to ask what

are the fundamental ethical principles that we think are important here to our work? And that could be the integrating theme of all of our chapters.

Now we can take the break.

MR. MEDINE: Now we have something to think about. We will take a break for 15 minutes and come back at ten of. Thanks.

(A brief recess was taken.)

MR. MEDINE: If people could take their seats, we can get started. Okay, if we can get started, we have a very important announcement from Stewart Baker, a matter that was within the committee deliberations, so if people could be quiet and have a seat, Stewart Baker would like to make a very important announcement.

MR. BAKER: First, in thinking of access, there's a whole set of standards for industry technology that I didn't -- information technology access standards that's been put out by the access board. It's going to be incorporated into regulations for the Federal Acquisition Council by August 7, and that will cover a lot of the access to high-tech information.

But the most important thing is I knew the FTC was too cheap to bring us snacks, so I bought cookies for everybody.

(Applause.)

MR. KAMP: Now, will you be collecting our clickstream data as we eat your cookies?

DR. JONATHAN SMITH: There's a motion detector at the top of the box.

MR. PURCELL: Be careful, they are cookies.

MR. MEDINE: Yes, we appreciate your contribution to the committee.

I wanted to ask a few people to make a few brief comments as a follow-up to the last session. I do want to move forward, but I think it will be helpful to put things in perspective.

The first is Richard Bates.

MR. BATES: I just want to touch on one thing, and David, you mentioned this earlier, but the most important thing from businesses' point of view, and I think it's true from consumer groups, as well, is simplicity, and whatever we recommend has to be simple so we can understand it and we can do it right, and I thought we tried to do that in our little group, and hopefully we did to a certain extent, but whatever we come out with, it's got to be able -- it's got to be

easy for people to understand, to work with, and I think that should be the hallmark of everything that we do here and every recommendation that we make. So,

thank you.

MR. MEDINE: Again, obviously the group -- I think that's a useful comment, and we will proceed as we wish, but I think we've done a very good job of breaking things down into their individual pieces, and now we need to build them back up again into options. So, thank you very much.

David Hoffman?

MR. DAVID HOFFMAN: David Hoffman from Intel Corporation.

Thinking back on the conversation from last hour, I went back to Richard's diagram that he offered for the identification and subgroups, and I looked at the different appliances that send the information in, and it actually has the telephone and it has some letters here, and it occurred to me that we spent an hour talking about scope, but we never talked about where the information was coming from, and we never talked about whether we were just talking about personal information or whether we were talking about something greater than personal information, something that might not be completely personal information.

I think we've got a lot of work to do on both of those issues. I don't think we've talked about it, and I have difficulty talking about anything else until

I really have a firm understanding of where we are from a scope perspective. If someone communicates a large degree of information that would not be personally identifiable over the computer but then they call up support and they give personal information over the support line and there's an ability to link the two, how's that covered? What do I tell my clients? How are they supposed to provide access or security for that?

MR. MEDINE: Okay, I think that again will be a useful thing for the subgroups to consider as they develop options in this area in terms of what you have access to.

For the balance of the morning, up until roughly 12:45, I'd like to proceed with the next three access subgroups, and we don't necessarily have to absolutely put blinders on across the subgroup lines, but I want to start off with the subgroup on entities. They pose a number of questions which I'd like to I guess hear comments on about how access relates to the fact that information flows, and it flows to affiliates, it flows to joint ventures, it flows to

joint marketing partners.

Essentially how far up the line -- we talked a little bit earlier about how far up the sort of

analysis and manipulation line access should flow, but now a related issue is how far up the corporate line or the corporate affiliation line ought access to flow. And I don't know if people from the subgroup would like to address that or -- Frank would like to address that.

MR. TORRES: During the discussions of the Financial Modernization Bill, a lot of distinctions were drawn between affiliates, parts of the parent company, and say third parties, say third-party telemarketers and other things, and the Comptroller of the Currency and other folks were fairly consistent in saying that, you know, are these distinctions without a difference in the minds of consumers?

I'm sure that there are business differences, but the fact of the matter is the data gets collected and used, and does it -- you know, for the consumer, does it make any difference, you know, with whom it's being shared and used by? The fact of the matter is it's being collected and used and shared.

And so I think the distinctions are important to make, but at the end of the day, these might be distinctions without a difference, so...

MR. MEDINE: Well, I guess maybe to turn that around, one of the issues in the financial modernization debate is who should the first entity

give you notice and choice about for subsequent information flow. Here I guess there's a slightly different question, which is going down that information flow line, should you be able to tap in at any point as a consumer and get access to your information or do you have to go back to the place that initially gathered the information from you?

MR. TORRES: Well, I think we need to look -- to be realistic and reasonable in the approach, and to the extent that the information is, say, collected by your bank and then shared with the third-party telemarketer or say shared with an affiliated company. I don't know if it makes any difference where the notification or where the access point comes into play, as long as it's at a reasonable place where the -- where either the decisions are being made or -- you know, so, I don't think every -- at every step along the way maybe is it right for a consumer to have or is it necessary for a consumer to have access but at least at some point.

Then the business can decide where, you know, perhaps -- you know, who should be responsible for

that. The main thing is that the consumer, you know, gets the notice, gets the access.

MR. MEDINE: Okay, Ted?

MR. WHAM: Ted Wham with Excite@Home.

There's a couple things I want to address in terms of that. The first one is that there's a notion that data is owned by just one organization, that if you give me your name, that I'm the only one who knows it, and we should recognize that data is owned by multiple organizations that collect it through nonduplicative manners.

The second thing is that if you provide information to me, you know, there are big smiles every time that cookie box comes around, you know, but if you provide information directly to me, then I think that there's a right of action and a right of correction to that which is available, but if you give me authorization to be able to share that information with third parties, I think we need to look carefully at what the responsibilities are for that third party to correct that information, because it's kind of, you know, the horse is out of the barn at that point, and the third party is a buyer of that information or is a recipient of that information from a trusted source as opposed to directly from the consumer that supplied it.

The best example I would have is that anybody in this room, you could supply to me your name and address, and I could go buy what is known as overlay

data in the marketplace, and I could find out, you know, with a pretty high degree of accuracy what your income is, how many children you have, whether you own or rent, what car you drive. There's all sorts of information which is available on the public marketplace.

So, I'm in the internet business, and we go and we buy some of that information so that it helps us target our advertising more accurately, and if somebody comes through and says, well, wait a minute, you think I've got kids and I don't, I can correct that information, but that really doesn't serve the consumer's interest as well as if we get the -- the consumer back to the originating source of that information and say, well, really, we got that information from a third party. What you want to do is correct it there.

MR. MEDINE: Is that -- you pose a distinction between getting information from a third party. Does it matter if it's an affiliated company, joint marketers, joint venturers sharing that information or that information is being bought and sold on the

market?

MR. WHAM: I think you want to have some delineations very carefully about where those lines

come through. You know, when we talk about affiliates, third parties, joint venture partners, joint marketing arrangements, I see this wonderful ability to create shade everywhere I go. Well, they are not really a joint venture partner, they are a joint marketing partner, you know, something like that. In general, if there is a tie-in of ownership, if it's the same company or if it's shared amongst companies. So, if Excite@Home owns other service firms, I don't think that there's a distinction. Any one of those should have the responsibility for correcting that information. If we share it with an unaligned company with different ownership and so forth, I think that's different, very black and white.

Joint ventures, as long as we define those clearly, very explicitly, then I think we're fine in terms of saying that there might be a responsibility or may not be. I don't know if I have an opinion, but we just have to be clear about these distinctions.

MR. MEDINE: Jonathan?

DR. JONATHAN SMITH: Jonathan Smith.

I did want to make a point. One of the

interesting things that we haven't really touched on but we have been hitting on like edges of it is what is the value of the information? I mean, I think that one

of the things that's very interesting that I see, people that I know who buy a lot on the internet, they will give away information for coupons, for example. So, what they're doing is they're pricing their information, okay, they're assigning some value to that personal information, and they're accepting that price for giving away their information.

Now, they may not have priced it right. This is the same kind of issue like, you know, when you sell or buy a piece of real estate, how do you figure out what the right price is? I mean, you know, what happens when you sell a piece of real estate, though, is really you have no control over what happens to it after you've sold it, and it's forever, you know, so maybe one of the things that would be interesting to spend a little time thinking about would be, you know, is the information something that, you know, the property rights transfer in the same fashion?

I mean, it's actually kind of a useful conceptual idea to think of the information as having some value, because it obviously does in the marketplace. For example, many of the valuations of

modern new-age companies are, in fact, predicated upon the value of this information, and that value seems to me to be a very different value than the consumers seem

to place on exactly the same information, and maybe all the value added is in the data fusion.

I don't know, I don't have answers, but I'm -- you know, this is one of the things that's actually a good way to think about it, which is the value of the information.

MR. MEDINE: Okay, David?

MR. DAVID HOFFMAN: I just wanted to come back to Ted's point about the definitions, and you go through that we do have at least six different terms that we haven't defined right here. I do think that if we try to define all of those separately, I agree with Ted, I think that's a task that will create more mischief than clarity, but I would actually offer a different option than what Ted offered.

I don't think the direction that we should go is saying whether it's an ownership issue. I think we have to look at it from the perspective of the consumer, and we have to look at it from the perspective who do they think that they're giving the information to, who do they think that they're dealing with? When we have a world of multi-national

corporations operating with different brand names and different businesses that people have -- and maybe in completely different sectors, I'm not sure ownership is

the way to go.

MR. MEDINE: So, would your operational rule then be that you would send the consumer back to the entity that they interacted with as opposed to affiliated entities? How would you apply that in practice?

MR. DAVID HOFFMAN: I would send it back to the affiliate that they dealt with originally with the opportunity, also, for them to -- if they had been provided notice that the other entities were also going to get the information, that notice -- I don't see how you can deal with this without dealing with what notice, if a third-party transfers, there are going to be. The notice requirement would have to also obligate notice or other entities that the consumer wouldn't perceive that they are giving the information to and them having the ability to contact them, and then if it's taken back to the original entity, at least that that's going to be done timely.

MR. MEDINE: Okay, James?

MR. ALLEN: Yes, James Allen.

I wanted to go back to the point Ted raised

about, you know, where do you correct data? Where does a consumer correct data, at the point that they're interacting -- at the entity that they're interacting

with or at the ultimate source of that data? I think that's a very good question and a very difficult one, actually, to grapple with, because the reality of it is, at least in the direct marketing industry, a lot of these databases are aggregations of data from many, many sources, and the aggregator is trying to pick the best piece of data to use.

To maintain traceability of actually where the data came from is every bit as big a problem as the problem Richard was pointing out with trying to control sensitivity down at a granular level this morning, and I think what's absolutely critical is that regardless of whether you can trace the source of the data back or not, that the consumer does and should have the right to correct the data at the point that they're interacting but with the entity that they're interacting with, and that entity should accept the corrections of the data if, in fact, the consumer's got a valid challenge to the accuracy of the data, regardless of whether that correction can be reflected back to the original source or not.

MR. MEDINE: I guess maybe just to clarify one

of your points there, you're saying that essentially if the data gets aggregated and incorporated with other data, it may lose its source of origin?

MR. ALLEN: Yes, that's exactly what I'm saying.

MR. MEDINE: And so an affiliate may -- unless they're required to may not be able to even track it back to the original source in terms of access and correction issues?

MR. ALLEN: It may not be economically feasible to maintain such a system.

MR. MEDINE: All right.

Ron?

MR. PLESSER: I just want to follow this line directly with what the person from the other side was saying. In the public record databases that we've worked with, similar to the Individual Reference Service Group and the FTC, and the group has been at some level of disagreement on this issue, and it raises precisely this question. If we are in these cases replicating public record bases, real estate records or others where -- or court decisions or whatever those issues are, the people who -- the databases who are providing it have taken a position that they will notify the individual where the information has come

from and kind of who to contact if there is otherwise public information.

If there is nonpublic information, then we all

agree we take on the obligation of providing access, but if it's otherwise available -- and there is even a concept of that in the Freedom of Information Act for government, that they don't have to provide FOI access if it's otherwise available.

The problem, particularly if you look at something like a real estate database, is what happens if there's an error? If Lexis/Nexis or whoever is purveying that information provides access, makes the correction, then when it -- it's still an error in the original database that other vendors are going to propagate. So, the question we thought or we continue to think is that it serves the consumer better, rather than fixing it in kind of one of the outlying spheres of distribution, but kind of pushing it back to the center sphere of distribution, so that if there's an error, it's corrected at the source.

That argument may or may not be the same in terms of marketing databases and others, although I think we think there is a -- there is a common trend, but certainly in -- and the problem is on the public record database is that part of what's being sold is

the integrity of the data, and the integrity of the data is a reflection of what that data looks like in the public record. So, if you change it, it may be

right to change it, there may be an error, but you no longer have an integrous database, because you're no longer reflecting what's in the source.

So, I think that has to be taken into account at the FTC, and we're continuing to discuss that issue with a great deal of contention, and seriously, for the record, we are very interested in the outcome of this -- of this discussion to kind of guide that outcome, but it's a very difficult issue, and I'm sure it has a lot of parallels in other environments.

MR. MEDINE: Deirdre?

MS. MULLIGAN: Deirdre Mulligan.

I wanted to respond to something Ted said just briefly and then suggest a model. I think when individuals give an organization data, they don't think that you all of a sudden own it. They generally think that you have just taken on stewardship, perhaps you've become a trustee, you've taken on some obligations, but consumers, when it's their data, they still think that it's theirs, and I think that sets up a model where as data flows to third parties, to affiliates, whatever, that the individuals' interests in those data continues

to flow, and those interests clearly, you know, from my perspective include an access right and a correction right.

Now, I think that the correction issue can become complicated, and I think where there might be a general rule that those rights flow with the data, I think there can be some very compelling purposes where a correction wouldn't be appropriate in certain instances, and I think one of the most compelling can be taken from some place like MedicaLogic, which is there's certain kind of data, like a health record, where not only does the information reflect my health care, but it also reflects a doctor's standard of practice, and so I can't -- if I choose to contest data and change it at a record source other than the one that is at the doctor's office, I could be impacting on a record that really could come back and bite them, because it reflects on their standard of care.

So, I think there are some very legitimate concerns. Ron and I might have a shared perspective, we might come out differently on what the right answer is in the public records context, but I think there's a shared perspective in that there are instances where correction is appropriate at a specific place rather than broadly, because of other compelling interests,

and it may be -- I don't think it's a compelling interest to say it's most efficient here. I think that you can correct it as -- I'm not sure who the person is

sitting directly -- diagonally across from me.

MR. ALLEN: James Allen.

MS. MULLIGAN: James Allen. I think you're right, that at times it might be much more efficient to correct it wherever the consumer is, but it also might be, as Ron said, in the consumer's best interest also to direct them to the source of the inaccuracy to begin with and that those things don't have to be in tension. We could do both, recognizing that there are going to be instances where we can't, and that's okay, too.

MR. ALLEN: James Allen again.

Just for the record, I want to --

MS. MULLIGAN: I was agreeing with you, actually.

MR. ALLEN: -- say I actually think that the corrections should be made at the source, but if not feasible, you should be able to do it at the point you are interacting.

MR. WHAM: You could do both.

MR. MEDINE: Greg Miller from MedicaLogic.

MR. MILLER: Greg Miller, MedicaLogic.

Just a couple of points. In listening to this

discussion, one has to wonder if what our work isn't all about is setting a set of protocols for profiling in general, and I just offer that up for us to think

about. Are we not really heading towards recommendations as to profile protocols and what ought they be?

The second point I want to make is I query whether or not it's a reasonable burden for the consumer to have to chase and trace the information. Once upon a time, there was a famous statement that said if you want to know the answer, follow the money. Today the statement is if you want to know the answer, follow the data.

And finally, to Dr. Jonathan Smith's point earlier about value, I wonder if value isn't a relative thing. What is the value of your credit card number being exposed and wrongly used? Well, it's either $50 or a $500 cap to be exact. Well, what's the value of someone finding out that you have a sexually transmittable disease? I'm not sure that value is always a monetary issue here, and I think it's interesting, and I suggest to you that actually an observation that Deirdre and I made here offline a moment ago is to think about value as being inversely related to the consequence of its access.

MR. MEDINE: Richard?

MR. PURCELL: Richard Purcell.

I'm gratified that the conversation is taking

this course, partly because I think we can connect this back to Larry's -- Larry Ponemon's earlier comment about the moral framework within which we need to establish our work.

I believe that one of the primary issues that we're now discussing is transparency. The question about how much and -- how much information a customer or an individual is allowed to know not only about themselves but also about the data provider themselves. This is not really limited necessarily to information about what you know about me but has to be inclusive of also what information I know about you. That would include who has this data other than you by your work. Where did you get this information if other than by my work?

Ron mentioned the question of data integrity and whether a database remains integrous if there are errors in it. I would position myself as saying we have to also think about the integrity of the data provider, because if a data provider allows bad data or corrupted data to exist in their database upon which they're making decisions or upon which they are making

revenue, then we have to also think about what is the integrity of that provider themselves, and I would say that the individual needs to have a basis for making

those kinds of decisions, as well.

Finally, I want to raise a caution that was raised in our prior meeting earlier this month. We have to make a decision here whether or not our work is going to inexorably lead to a recommendation or guidance principles that say data must be consolidated. There's a real problem with that conclusion in that in order to protect your privacy, I essentially now am being required to assemble more information about you than I otherwise would have access to.

Now, it certainly eases the burden of access. Certainly if I can provide a single point of entry for an individual to look at the data that we have about them, then I have facilitated access. At the same time, I have also facilitated my ability to surveil or to intrude upon the privacy of that individual, because I know vastly more about them than I otherwise would. Is that a data protection step or is that a data intrusion or a privacy intrusion step?

These are hard questions, and I would say that this group is going to have to come down on one side or the other of these questions.

MR. MEDINE: On that point, is that -- in the old days it used to be that information was kept in dusty files and took a lot of time and effort to put

together to create a profile or provide access, and in this electronic era, is that really still as much of a distinction? That is, is access really forcing the creation of those profiles or accumulations of information or is it so easy to accumulate that that is going to happen anyway?

MR. PURCELL: Richard Purcell in response.

Even in this era where data management has become far more facile, far more -- far more easy to manage, we still provide our customers with specific services that are based on infrastructures that are not necessarily consolidated infrastructures.

Mr. Hoffman just made the comment that if a -- an individual has a relationship based on information they've provided with a business and they call on other services of that business, and we will use technical support as one of those, is there a requirement for me then, as a business, to match up all of the information that I have about a customer across all of the various services?

Today, largely, those services are relatively independent of one another, and they're based on

differential infrastructures, and there's not necessarily data flowing between these different data sets. If we required that that data flow between these

data sets, we've gone down a bit of a slippery slope in order to provide access but potentially creating a cause for omission.

MR. MEDINE: Dan?

DR. SCHUTZER: I agree, I think it's important to know the source, even the nature of the source, because that can affect the nature of the correction. In other words, if -- let's say the source is my grades, the nature of the source is coming from the professor, I can't necessarily just at whim change it, but it's fine to know the origin, the identity of the source. If it's coming from let's say a supervisor's evaluation, it's not entirely clear that you're entitled to know who that person was or that you are able to change it. So, I think that simplicity would be nice, because we understand today we don't carry on like that, who is the original source and so forth.

So, if we could move into that kind of a way of managing that, I don't know that, the transition, and for simplicity I would say, even though I'm going to bring it up, there could be a whole trail here in terms of the original source, it goes to someone else, it

goes to someone else, and the data can get corrupted somewhere in the process. I think that would probably be too complicated to try to implement exactly finding

the entire audit trail. I'd recommend probably just the source and the nature of the source.

And, of course, being able to compare the data, it's quite possible that the data I'm viewing in this site was entered in error, that the source actually had it correct.

MR. MEDINE: As we move forward, I have a couple of -- I would like to sort of shift the discussion into the cost-benefit, not that we haven't been in it already, but to talk about some of the costs and benefits, like correction and how to provide access, what is the cost structure that's entailed with setting up access for consumers in an essentially otherwise highly automated database system, but we have a few more comments that may or may not address this issue.

Tom?

MR. WADLOW: Tom Wadlow.

Yeah, I wanted to actually touch on some of the things that were being said here, but what triggered me was Mr. Allen said what I thought was a very interesting phrase, traceability is just as hard as

sensitivity when it comes to data. There's a very interesting distinction between the two there in that sensitivity of data is in many ways subjective.

I might have a piece of information I might not want someone to know, but other people might have analogous information that they don't care about or how it's going to be used, things like that. That information is very hard to pin down, the sensitivity of that.

Traceability, on the other hand, isn't. You really do have the ability to know where that information came from for the most part, and if you don't know it now, you can reasonably easily devise processes by which you can learn where that information came from. So, it sort of becomes an interesting thought here, if you imagine that what you require of organizations is the ability to get some transparency and look in that -- into what information they have collected about you, where they've got it and what uses they're putting to it, rather than focusing on the information itself and the sensitivity of the information or that it's a lot of implied stuff, a lot of subjective stuff, having actually measurements of the things that can easily be measured, the traceability of it, what use is it being put to it,

what uses, in fact, the company might wish to declare that they are explicitly not putting this information to. That's all very, very objective stuff, and I think

that's very valuable.

MR. MEDINE: I guess just getting to cost issues, from a company, say, that might be buying three different mailing lists that they want to just merge into one and then send out a mailing to a variety of people that might be interested in their product, what are the economics for them of having to tag where they got -- whether this name came from source A, this name came from source B and this name from source C?

MR. WADLOW: There is actually two issues there. One is tagging the specific piece of information with its origin and then the second is making a more general declaration of here's where we got our information from. If we got your name, it's likely to have come from these sources, and then you have at least some transparency to it is what I was thinking. You know, one might imagine it, taking it back to a web example, right, that you could go and ask a web server of some type what its policy was and it would show you a diagram, you know, here's where all the inputs are, here's all the outputs, and here's your data in the middle. Here's what we know about you in

that sense.

MR. MEDINE: Dan?

DR. GEER: Dan Geer.

As a point of technical information, in my view, as a guy who works in security all the time, having the issue of the consumer able to correct data is actually technically much harder than you might guess, because it implies first that you know it is the consumer correcting his or her own data, and secondly, a whole lot more authenticity, authorization control and so forth.

The difficulty in correcting multi-point write databases versus protecting write-once databases is really substantial, and I just want to say as a cost issue, while we're talking about this cost and benefit thing, having everybody able to correct their own data wherever they find it either creates a new class of risk, which is I'll correct yours, or it creates a very much higher bar for what identity control will mean in an environment where this is possible.

MR. MEDINE: So, in a sense, you would up the authentication requirements considerably if there's an ability to go in and change the information as opposed to simply access the information?

DR. GEER: That's correct. I mean, I fill out

web forms all the time. Half the time I lie on purpose. That's my right. I don't want to correct it. If you want to make it possible to correct it, then you

have to be really, really, really sure it's me and not my brother, my evil twin and all of that, right?

MR. MEDINE: Sure. Dan Jaye?

MR. JAYE: I'm actually going to -- Dan Jaye.

I'm going to try to tie together actually the entity discussion and the cost-benefit discussion here and draw on a point that was made about a protocol. There is a project underway called the Customer Profile Exchange standard under development, and I hope that it will be heavily informed by the work that actually comes out of this committee, but one of the concepts we have is to have privacy built right into this protocol.

There's been a bit of press about it. One of the costs that we're concerned about that we're trying to figure out how to address is that if you have in this concept the idea that the privacy implications of data are attached to the data and travel with the data whenever it's transferred, so that we can deal with onward transfer privacy issues, one of the concerns is what about Legacy systems that you are interfacing to.

Suppose I'm taking an order from an order processing system and I'm giving a name and address and

a packing slip data to Federal Express so they can

fulfill the package for, you know, transient use, but

suppose I have some sort of onward transfer propagation

of, say, access requirements or correction, how do I ensure that the Legacy system on the other side of the protocol has the ability to, for example, keep track of the privacy implications associated with that specific set of data?

So, once again, as we look at the cost-benefit, one of the things we need to look at is that it may be that there's some general transition period or some need to think about that -- the fact that there's going to be a -- potentially an impractical cost for some businesses to retool Legacy systems to be able to support some of the onward transfer access and security implications.

MR. MEDINE: Let me just ask even more directly on Legacy systems, what about access at all even to a Legacy system that may not have been indexed based on the individual as opposed to the address or other -- some other demographic information? What are the cost-benefit issues with regard to access to older systems?

MR. JAYE: I think that's a very real issue. Actually, the UK Data Protection Act, which the issue

of the costs of implementation were a major subject of discussion, one of the major issues is they did have a concept of how files were keyed, both electronic files

and offline files, and had different sort of standards of how those things needed to move into the jurisdiction of the act.

To my point earlier, maintaining a file that's effectively a sequential file that's only accessed in bulk could be much less expensive than now throwing an index on it that allows it to be accessed in realtime, and some architectures might not be feasible. I think in today's technology, that issue becomes much more apparent when we're talking about interactive data than necessarily customer records.

In other words, cardinality, the number of records we're dealing with for a customer with a typical business is usually small enough that the index overhead requirements aren't that bad. It's when you start dealing with the huge volume of interactive data, if we step into the range of saying you need access to those individual records of the fact that I clicked on this page and I clicked on that page, back to the consumer, that's an area where the cost implications start to need additional consideration.

MR. MEDINE: And I guess one more follow-up

before we move on is along those same lines. Do we essentially urge or expect the firms to build in the indexing on a going-forward basis so that access can be

provided, or do we have a situation where that firm chooses not to build it in, then the consumer doesn't get access, and then trading that off with Richard's concern of if we create incentives to build it in, are we hiding privacy risks? How do we sort of weigh those competing considerations?

MR. JAYE: I think it's a cost-benefit, and you have to look at the implications. If the data is innocuous, particularly if it's anonymous data, that's one thing. If we're talking about data that's tied to personal identity, we still have to look at what's the potential implications of the use of the data. How's the data going to be used? I think, once again, the sort of test of how does the company have access is a very good test. If the company really is using it in less controversial ways, it may not be worth, you know, a cost to index and maintain random access to a large amount of data, but there's other data that fundamentally the consumer absolutely should have access to, and the cost is less of a consideration.

MR. MEDINE: And I think it will be an interesting communication issue to consumers is when

they should expect access and when they shouldn't.

James?

MR. ALLEN: Well, my comments are directly --

James Allen. My comments are directly related to what Mr. Jaye was saying, but it was really triggered by what Richard was saying earlier, that you can actually put the consumer's privacy at risk by consolidating data in order to facilitate access. Well, there's this other problem where if you're collecting so-called anonymous or innocuous data that's only identified by a GUID, but in order to give a consumer requesting access to it and to adequately identify that consumer and assure that it's not some malicious person trying to get access to it, now you have to maintain the consumer's identity with the data.

So, now in order to give access, you're, in fact, probably putting the consumer's privacy at risk, and I'm also -- I don't really know -- I don't know about this issue, but I don't know if there have been any court cases to test the admissibility of data that's collected that's only identified by GUID, and if people can subpoena data that's identified by a GUID and use it in court, then clearly you want to give this sort of access to it so they can make sure it's correct, and then if you have to maintain their

identity to do that, then...

MR. MEDINE: Thanks.

Ted?

MR. WHAM: Ted Wham from Excite@Home.

I need to go back a couple steps, and I want to bring up a philosophical consideration on two different areas from earlier conversations.

The first one was regarding the data value when a customer does a transaction with a site, what that value is, and I want to argue very strongly that, you know, theoretically we live in a capitalistic society, and as long as that is a voluntary transaction, it's not required as a statutory requirement, then presumably the customer is in an excellent position to determine what the value of that data transfer is relative to the value of the gains that are brought back, and that in any transaction, in any voluntary transaction, you know, of that type, both parties gain more than they give up, and I think it's a mistake for us to go through and try and assign different weightings on that value other than what the market has set for itself in those voluntary cases.

I thought there was an excellent point in the entities discussion about a voluntary versus I believe it was derived and the third one was required by

statutory requirements.

The second one I want to talk about is to touch

specifically on Deirdre's response back to me about the

organization being the steward of the data versus the owner of the data, and I want to pull it outside of the online environment, and I want to use kind of a case example of all the people that are in this room, okay?

I knew a couple of you before I was assigned to this committee, and one of the things that happened when I was assigned to this committee is that I got a mailing from the friendly folks at the FTC and it came in PDF, WPD, DOC, it was very handy, came in a couple different formats, but it included all your names and all your e-mail addresses, and I took all that information, and I dutifully recorded it into my Outlook database, which is my little customer file, I guess, if you would, so if I wanted to contact any of you via e-mail, I could do so.

During the courses of the meetings that we have had here and during the courses of the subcommittee work, I have developed inferences about all of the people here. Some of you I have decided are very capable, some of you I've decided talk too much, like me, some of you have different capabilities.

MR. TORRES: I want access.

MR. WHAM: So, first of all, I would argue very strongly that no one in this room has any right of access to that information that I'm collecting about

you, even though you gave it to me -- or even if you didn't give it to me, it was a third-party transaction, I guess in this case it was the FTC that gave it to me.

The second thing, my inference data that we're using in this discussion -- we haven't spent very much time on this at all, but it is none of your damned business what my inferences are on you, and I'm certain all of you have inferences on me.

When we're talking about the requirements for an organization to provide data back to its consumers and we're talking about whether there's an absolute right of access, I think we're missing a big boat. There is not an absolute right of access in this society in any endeavor, and I don't think that there should necessarily be an absolute right of access within the online environment and certainly not to all of the data. There is certain data which I believe is absolutely off the table.

Now, I don't want to come across as saying that I don't believe that there's access to some data, because I do. I believe that the information that customers supply about themselves is absolutely up for

their access and for their correction. Further, I believe that there are other categories of information that is available for their access and not necessarily

their correction, the examples that I've provided earlier about what you purchased or, you know, if you were in the hospital, say what day was I born, and they say you were born X date, 1946, and they go, oh, I don't want to be that old, therefore I was born in 1964, right, those types of things aren't available for correction.

But to start with the philosophy that access is enshrined somewhere is I think completely against how we run this country and what we should be about. Instead I think we need to look at it from what are the reasonable things we want to do as a society.

MR. MEDINE: Andrew?

MR. SHEN: Thank you, Andrew Shen.

A few general statements, just right off the bat, a little reaction to what Ted just said. I don't think we have to go into the I guess political or moral or philosophical arguments behind access, but I think in the -- at least in the access one subgroup, we presented at least three good reasons and hopefully compelling reasons why access is important and why it's included as a fair information practice. I don't know

whether, you know, it's downright un-American to do that, but --

MS. MULLIGAN: Apparently it is.

MR. WHAM: I was being too strong.

MR. SHEN: Also I would like to throw out that access could also include the right to delete information, and I think this is increasingly a point in the modern world, and as the entities outline showed, a lot of information transfers to third parties, affiliated parties, joint venture marketing deals, and a lot of that we don't realize is going there. So, I think that a person who that information describes has a right to remove it from places that they had no idea that information was going to.

Second, in reaction to Richard's comments, this very interesting sort of dilemma between consolidation and access, in some ways I think on a theoretical level that's very interesting, but on a practical level, it's not really much. I think what we see is an amazing amount of consolidation out there and not much access, and I think those two need to be balanced, but it's definitely out of balance right now.

And the consumer profile exchange that Dan Jaye referred to is I think one compelling example of that. I think you're seeing a lot of consolidation out there,

and consolidation is becoming so easy that companies

can transfer back and forth baseball cards,

essentially.

And the last point is on the costs and benefits, I think one element that hasn't been taken for granted is how data minimization, you know, one subspecies of data minimization and that anonymity can really decrease the costs of access, security, authentication, because these are all costs you incur when you collect information, but if you collect less information, then the costs will go down.

MR. MEDINE: Let me say something about the cost structure. We have said a little about the costs to businesses of providing access. What about cost shifting to the data subject, what -- Andrew, what are your views on whether there ought to be -- it's permissible to charge the data subject for access to their own information?

MR. SHEN: I mean, I -- you know, it's hard to quantify exactly how much you should provide. There's a lot of, you know, existing statutes, the Fair Credit Reporting Act, where you are assessed a fee for accessing that information. We also have to consider, you know, how much of an interest there is by consumers to actually exercise that right. So, I'm sort of

dodging the question here. I can't come up with a precise answer for you.

MR. MEDINE: I guess we can all think about it,

because we have talked about the cost side, and there are certainly some precedents for cost shifting, and the question is when is that appropriate, if at all, I guess.

MR. SHEN: But at least -- Andrew Shen again, but at least we have to consider how much technology on the internet is making information access easier. So, I don't think that cost should be prohibitive in the current world.

MR. MEDINE: Lance?

DR. LANCE HOFFMAN: I am very worried about the cost being prohibitive, and those who know me are saying, what is he doing saying that? But I am. I'm very taken with Stewart Baker's argument. What I am worried about is another FOIA misapplied, another Freedom of Information Act misapplied, and I don't want to see that.

And Andrew, I'm also concerned about -- I don't think the costs are that much -- you know, everything is being driven down to zero, so it won't cost anything anyway. I think we have to consider more carefully the secondary and tertiary things that are happening, and I

think Ted had a very good example, let me take it further, with the FTC, this committee.

We have a database of, you know, 40 or so

people, plus staff, but when I got my appointment letter, went to the webpage and so forth, and lo and behold, there were all these recommendation letters and such, self-recommendation letters and other recommendation letters, which I guess people knew, I don't know whether they knew or not, but there they were and are up on the webpage, and you can infer a lot from there.

Now, take that and electronicize it, okay? Pretty soon you have got databases talking to databases, talking to refrigerators, talking to Peapod, this and that, and the grocer and people like that. We can have data going back and forth and back and forth and back and forth and a lot of activity but nothing really getting done and, in fact, us getting in the way of in essence maybe performing what is reasonable for the consumer. So, the real issue is what is reasonable for the consumer.

It may be, answering your question, David, that an access charge of some sort might limit a lot of abuse, but at the same time, there would be some sort of lifeline service or even free service for

appropriate accesses and corrections, and then the question is, what's appropriate? And that's what we ought to be talking about, because otherwise I'm really

concerned we're going to try to write something up that we can't do. We can't even foresee what's going to happen, and we're going to be in a deep pickle later on.

MR. MEDINE: Rick, I want to call on you, and I'm sure you have something to say, but let me also pose a question to you, which is in the cost-benefit area, there's certainly a lot of small and large firms in this marketplace, and obviously the costs of providing access will have a different impact certainly on a small firm versus a large firm. I was wondering if you have views from the perspective of the Chamber about whether -- what the -- how we ought to address the fact that we have widely varying size companies in this marketplace, and plus whatever other comments you can make.

MR. LANE: Well, I think like the Chamber, our macro answer is let the marketplace determine that, would be our first point, but the concerns that I have when you talk about costs and benefits is the liabilities of access to businesses. If there is information that is changed by a third party, somebody

who didn't really have access, is it the business --

can the business be brought to court, are there

liabilities that attach to that, and you also have

credibility of the business itself.

In addition, when you were talking about getting and tracing data all the way back, business plans are made up of how you gather information. So, the concern of a business might be that if we provide how we got that information, that's proprietary information to that business, because they may have a really great list or have been able to bring together a bunch of great lists, and a competitor says, well, gosh, they have great lists, I want to see how they're getting all their information, and all of a sudden they do a search, access, and they find out how all this information is being gathered. So, there are some business concerns that we need to look at.

But one of the biggest ones that we're afraid of as a business community is the whole liability issue and what does it mean when you provide access, and the security obviously is critically important, but it all gets back to the liability issue.

MR. MEDINE: Thanks.

Rob?

MR. GOLDMAN: Rob Goldman, Dash.com.

I can represent small business and sort of startup entrepreneurship a little bit in the discussions saying that the question was posed earlier

saying how is it different or is it difficult when there were dusty old files that sort of needed to be pulled together and assembled versus the way things are today, and I think I can say safely it used to be time-consuming but not terribly difficult, and today it is fantastically complex but not nearly so time-consuming, and the resources necessary to conduct the work today are much more specialized resources. They are much more expensive resources. They're very difficult to find, especially in this marketplace.

I can imagine if -- if we as a startup had to provide access to all the information that was collected by our merchants, their affiliates and the third parties that do business with us, we would have an entire database staff, which we have been trying very hard to build and have not been able to find people for, dedicated to that problem alone. We wouldn't be able to focus on the business problem that we're trying to solve whatsoever.

So, I think there's a real risk, especially since you have seen a lot of vibrant innovation in the space, that if the access burden, especially in the way

of consolidating data from various parties, is too high, that you'll see a lot of that get stifled.

One other point on costs and benefits, and this

is a philosophical point that I think is important. The costs are very easy to state. There are cost estimates everywhere. I sit in meetings all week where I have proposals put before me with spreadsheets of costs. We know, you know, specifically how much it costs per customer per byte of storage. We know how much it costs to migrate one system to another. There's free information on it, there's trade information on it, there's sort of information everywhere on costs.

The information on benefits is much more difficult to pin down. The benefits are very vague, they are very general. How do you put a value on sort of increased trust in the medium? How do you put a value on more innovation in the space? How do you put a value on deeper customer relationships, more robust lifetime value, the willingness of consumers to try new products and the willingness of businesses to provide them?

There are -- those are the benefits that we're talking about often, and it's really hard to put a number on them, and it's hard to compare them

effectively against the costs. So, I think what happens often, and I've seen it happen certainly quite a bit in the space in which Dash competes, is that

people just discount them, discount the benefits altogether, focus on the costs and make their decisions that way. I think we as a company have chosen not to do that. It's been very expensive, which is maybe not necessarily a bad thing, but certainly in this room we should consider the benefits. Even though they're vague, they're important and need to be addressed.

MR. MEDINE: Did you want to respond?

MR. LANE: Just to follow up, Rick Lane, U.S. Chamber.

Just to follow up on your comments and having started a couple of small businesses myself, when you're trying to staff your business, I mean, you don't want to have to just -- it's bad enough to have to hire lawyers and accountants and the cost of that, but now you are going to have to have -- to hire somebody to handle access, and so that's a real cost that's taking away from the development of your business, which, in fact, your business model may have nothing to do with access in and of itself. So, you have to look at it.

As a small business starting up, you have to now just have a mandatory access person all the time,

because you're able as a small business to gather so much information quickly, as was discussed before, but you may not have the personnel to handle all that

information and all the requests that may come in.

MR. MEDINE: Ron?

MR. PLESSER: A couple of quick points going back and then maybe one recurring thing in this.

First of all, just in terms of the source and access discussion, I think it is important if we can look back at kind of the old world, is the DMA for many years, many, many years has had a provision not on access to records but on source. So, it is the DMA guideline, at least in terms of the old world of marketing lists where you did get lists from another person, and if you look at your mailing label, there's a little number code on top of the mailing label, and that always identifies where the list came from, because, you know, if you're going to use that list again, you want to know it.

So, I think the issue of source is really a much different issue than access, and I think if you look at least in the marketing world, source has already been, at least in the self-regulatory regard, been dealt with.

The second point, and maybe this is also

relevant in the flow of conversation, I agree with the last comment, that I think consumers have interests that have to be respected. Privacy is a critical

issue. Businesses, whether or not they're big or small, have to respond to it. To talk about property interest, though, to me takes it all the way in the wrong direction and the wrong track.

The Supreme Court cases so far makes the property decision -- makes the property argument winnable to business. I mean, it's clear that a customer list, an employees list, information even of a check that goes into a business becomes commercial data and is valued in the flow of commerce. So, if we use the property analysis on the basis of current law, consumers would be absolutely out of the system, which is totally wrong.

I think, you know, they have interests, their interests have to be respected whether or not they're property interests or not, and I think to start to try to define them as property interests really misses the point, and I think it's a good kind of public comment, but really from a legal perspective, it almost misses the point completely.

In terms of the benefits, and if I can turn to -- there are benefits to business. I mean, both at the

Privacy Commission stage and in OPA, the integrity argument is the business does get value by having consumers -- there was a big fight in the Privacy Act

for the government, and I think the answer is by having access both to medical records and other records in the government, the databases shrunk a little bit. They also got a little bit better.

If a service person gets to see their medical record once a year, which they're required to do, or on transfer, the medical records tend to be more accurate, and I think there is a -- there is a real benefit there that I think business recognizes. Obviously there are costs, and I agree with the Chamber and others that these costs have to be -- but I think if you look at what OPA talked about about access, not access as an ultimate kind of right the way Ted was necessarily going but access as a way to assure better accuracy and integrity of the database.

So, I think to that extent, you know, we should -- and Deirdre may want to talk more about what the subcommittee did, but I think one of the things that we all supported was the issue that business as well as the consumers benefitted by consumer access because of the better integrity of the database.

MR. MEDINE: Lorrie?

DR. CRANOR: Thanks for calling on me, I had my hand up for quite a while, so I have some comments to go back, way back to the entity, because I have had my

hand up since then.

MR. MEDINE: We have lots of threads going on here, so that's fine.

DR. CRANOR: First there was some discussion about whether you could make distinctions about entities that consumers would understand, and I would argue that for the purpose of notice, that may be important, but assuming we're not discussing notice specifically here, for the purpose of access, I don't think we need to make that distinction.

I think what's important is that if I know that if I go back to whoever I've been dealing with, that I should be able to get access, and either they provide it for me or they provide me the door to whoever is going to provide it, it shouldn't make any difference to me. It should be seamless, and I shouldn't have to go on a wild goose chase to find it. Whoever it is that I'm dealing with should point me in the right direction and make sure that I can actually get access there.

So, I think that's important with the entities, and also it goes as well to the cost of access. There

is not only monetary costs, there is also how difficult is it for me as a consumer to figure out how to get access.

I think a good example to look at as sort of a case study is what happened with the Fair Credit Reporting Act, and I think this is a case where you can get access and you have a right to correct it, but there have been so many horror stories of people who have discovered an error, corrected the error, just to have it keep re-occurring because that data is propagated up and down the chain, and all these other databases that it's in keep reporting back to the credit reporting agencies this error, and some consumers have had a hugely difficult time trying to get it corrected everywhere, and this is not just a little trivial matter. This is things that are, you know, preventing people from buying houses and getting credit and sometimes their jobs.

MR. MEDINE: Thank you. I just note that Congress did at least consider that issue when they amended the Fair Credit Reporting Act to require credit bureaus, once they delete information, make sure it doesn't re-appear, but I'm not sure that --

DR. CULNAN: It's a good illustration of the problem, because everybody acquires third-party data,

once it's not corrected over and over, and unless it's corrected at the source, it does you no good to correct it in the person that's licensed the data's database.

MR. MEDINE: Okay, Frank.

MR. TORRES: I'm kind of in the same predicament, so I want to go back a little bit, but I think the point was made that there is a cost to consumers. We have been talking about the cost to businesses, and not just is it a pass-along cost to consumers, but if the credit report isn't correct, and it was nicely illustrated that there is a cost to consumers here, and I think Ted was the one that mentioned that, you know, how do we resolve the issue of having all this information out there.

Somebody else mentioned, you know, is this a case where we will have to actually start compiling information, and I think that's where this, you know, might be a security risk a little bit. I think the point that I want to make here is just because you've got the information doesn't mean you have to use it. So, I -- you know, everybody's -- you know, it's wonderful sometimes the technology that's out there, but, you know, just because you've got the technology to gather all this information and you use it to gather all this information doesn't mean that you've got to

then turn around and use the information or provide the information to somebody else, and I think that just -- I think we need to think about that, because I think

we're starting to reach the assumption that because the information's there, you know, will it be used, and I get the impression that it is being used, and that's a different issue.

To go to the points that were made about liability and trying to protect information for proprietary reasons so you don't allow access, a couple of points there. As -- I think consumers should be concerned about the gatekeepers who are the inputters of the information. Sure, it's one thing if you, the bank customer, are providing information to get a loan, but then if information is coming from third parties, whose job is it to verify the validity of the information that's being provided by the third parties that then influences the cost of your credit, how much you pay for a loan, the interest rate you pay, whether or not you get certain types of insurance, how much those products cost you.

And so I think we need to look at those issues. I understand the liability for business, and I appreciate that, but these issues shouldn't be a red herring to say, well, in that case, we need to not

provide consumers with appropriate access. To fix it, the same thing about looking at the interests of the person accessing the data. If I'm a business entity

and a competitor comes to me and says we want access to your data, you know, what legitimate purpose do they have to get access versus a consumer going to a bank saying I think there's something wrong with some information, I know it's been reported wrong on my credit report, you know, what are you using as the basis for -- what's going into the black box to determine my -- your way of scoring my credit, which might be different than what's reported on my credit report?

It's a little bit different there than, you know, Chase going to Bank of America and saying give me your info.

MR. LANE: But Frank, they don't go as another business. They go as a customer. They don't tell. It's not --

MR. TORRES: But then the customer should have -- I think there are ways -- I think there might be ways to get at it, and I appreciate that.

MR. LANE: I just wanted to clarify that.

MR. TORRES: The final thing, and I'm sorry for taking so long, but the example that Ted gave I think

is a good one about, you know, profiling people around the table and taking a look, but a person compiling that information is a lot different than a business

entity compiling that information, and I would like to think that there's very little Ted can do to affect my life, and I don't really care if he thinks that I talk too much. Let him put that -- you know, that's fine, and if he keeps it to himself, all the better.

It's a little bit different if a business takes that data and uses it to, say, red line when it comes to whether or not they are going to provide insurance products and things like that. So, I think there are some distinctions that we need to make during the course of our discussions, as well.

With that I'll shut up so Ted doesn't write bad things about me.

MR. MEDINE: Dan?

DR. SCHUTZER: Dan Schutzer.

First I'd like to comment on the sequential data thing, because if you're a large processor, you're dealing with tens and hundreds and millions of records, and there are sequential tapes, it could be incredibly costly to try to get that information, even if you're storing it. We talk about passes and sorts that can last a whole day just to get one piece of record out

for somebody. So, bear that in mind. You might consider in the sake of simplicity that we really are talking about master records that are kept online that

people would have access to.

Another thing is the nature of the data. If we're talking about, as was illustrated, you know, the credit report or a financial transaction, that's going to be or should be kept absolutely accurate, and so that's maintained. Now, when you talk about marketing kind of data, most marketing data, of its very nature, is basically noisy and dirty. So, don't be surprised if you find a lot of times that the data from the third -- that's been acquired, by the time you process it, it's better than the original data, okay, because sometimes the data we're receiving has typos, errors, omissions, even translate that to the web.

I mean, you might be tracking an IP number in the clicks, but the IP number is not always the same person. So, we might have a proprietary algorithm to help us sort of decide which ones to throw out. Statistically, it might be a more valid sample, but it's just marketing data. It's not, you know, financial records that we want to keep. So, sometimes the source is not really a good source anyhow, okay? And the third or fourth party that's processed it

23 actually has better data.

24 And finally, as a thought of what might be --

25 when you might want to pass fees or not, one

possibility is someone who abuses the system by the frequency of the use. So, for example, we provide routinely, you know, people can come look at their accounts, their transactions, their balances. Now, I suppose if somebody were going to be pinging us, you know, every 15 minutes to see the same information, then eventually that might be justified to tell that individual, well, you do more than, you know, 100 accesses in an hour, then we might have to charge you for that, because it's eating into the overhead of our communications server and so forth.

MR. MEDINE: Again, I think that's a useful point for the group to address, is are there circumstances where you give free access, do you get to limit access and so forth.

Why don't we take four more comments on this subgroup's work and then consider whether we want to take a break before we tackle the final group or we want to barge on, but let me go with James, Deirdre, Tatiana and Jerry.

MR. ALLEN: Actually, I -- Frank made my point for me, which was that the Ted's example was great, I

agree with Ted completely, he can choose who he takes out to dinner or not, and I don't have a right to that information, but at the point in time where a service

denial starts -- service -- the decision to grant or deny a service is made, then I think the consumer does have a right to that.

MR. MEDINE: Deirdre?

MR. WHAM: Can I jump in on that?

MR. MEDINE: Very quickly.

MR. WHAM: I don't think anybody's got a right to know if I'm Nordstrom whether I'm going to offer you, David, you know, a 10 percent off coupon. I've denied you a service, but that's my business right.

MR. ALLEN: Yes, and actually I agree wholeheartedly with you, Ted, on that. There's a fuzzy line somewhere, and the legislature and regulators have decided in some sectors where that line is, and in other sectors they haven't decided where that line is.

MR. WHAM: Right, and the only thing I want to be careful of is that there have been some people who have argued that there is an inherent right to access to inferred data, and that's where I get scared.

MR. MEDINE: Although there's also been a discussion earlier of decisional data, and the question is what types of decisions, I suppose, would that apply

to.

Deirdre?

MS. MULLIGAN: Deirdre Mulligan.

I actually did want to pull us back a little bit on track, too. One, we're talking about a very mission-specific task here, commercial entities that collect data. We're not talking about your data, Ted. You're lucky, because tomorrow we might be.

And two, that while I talked about access as being something that follows the data, we're talking about entities right now. We're not talking about what data do you get access to, which was the earlier discussion about scope and categories, and I think you and I may disagree about what the scope of access is, but we can probably agree that there are things that are not going to be accessible for various reasons, and to the extent that we can try to build consensus rather than pick battles where they don't yet exist, I think we should.

So, I think that the general principle that if I should have access to data, that that access right should flow with the data, is one at least that I think is a very supportable concept and doesn't put you and I at odds arguing over what do I have access to, where you say not to infer and I might say yes, and I think

for moving the task force forward to putting forward recommendations, to the extent that we can identify consensus, it would be useful.

On the cost-benefit issue, I think there are some important things that were both pulled out in the subgroup outline that deals with this access question and have come up here. I think the retrofitting question, are we talking about Legacy systems, are we talking about moving forward? I think the costs of those things are very different.

I also think that when we talk about moving forward, sometimes I listen to folks talk about the cost of access, and it sounds like every single commercial entity on the entire planet is going to design their own system from scratch, and I laugh. I know there are a limited number of operating systems, there are people who provide the back-end databases for all you folks, and I know some of you are in very specialized markets and you design your own, but I think to the extent that we can move forward in designing standards, to the extent that this feeds into those standards processes, it's very useful, because it's a way to mitigate some of the costs that incur to each specific business if we actually build it into a more generalized protocol. So, I think it would be

very useful to move us in that direction.

The third point is on Richard Purcell's centralization question, which I do believe is one that

merits a lot of attention, and Andrew, you and I may disagree here a little bit. I do think that there is an enormous amount of consolidation that we're seeing, and as Lorrie said, and as the BBB principles reflect, if business is using information in a way that affects consumers, so if I'm pulling a record on a consumer, that clearly that record should also be available to a consumer, right?

But I do think the question of forcing centralization raises some privacy questions that we have to ask. However, I do want to point out that those privacy questions I think usually don't stem from centralization but actually from the tension itself, and the perfect example is I think that many internet service providers today find themselves in a very responsive proposition of providing access to data to law enforcement officials, to private parties seeking people's identities.

They don't have centralized systems, but they're retaining data, and I can tell you that law enforcement doesn't care, if it's easy and inexpensive for you, they want it if you've got it. So, what I'm

suggesting is yes, centralization can heighten some of the privacy concerns, but that, in fact, a lot of those concerns stem from retention to begin with, and to the

extent we can look at those issues together, it would be useful.

MR. MEDINE: Tatiana? Would you identify yourself?

MS. GAU: Tatiana Gau, AOL.

I'd like to start out by echoing Deirdre's comments about Ted's example on access and also kind of the question he threw out in the air that is the principle of access a fundamental right of the consumer. I believe it is in certain cases, as I think most of us do, and just to kind of illustrate that example, on AOL there are various areas within your account that you can go to access information about you that we might have.

One example might be your wallet on AOL, where after entering a separate password to authenticate yourself, you're able to view your name, address, any shipping addresses you have on file for any of your relatives, products you've purchased. For security reasons, you can only see the last four digits of your credit card number, but you can from that point on also make one-click transactions.

Another example is your billing information. You can go to the billing area and view a log of all of your sessions, what screen names you've signed on with

and other such information, where we believe there is a need for the user to actually have access to that information. The only area where information can be corrected is in the name and address area. You cannot correct whether or not you were online on X date, because that's what our system records, and we do not allow correction of that.

From that point, I'd like to jump to the cost and benefit perspective where those -- in the two examples I gave, those records are accessible to the member from different databases. They are not in any way linked together. And similarly, AOL, with the billions of transactions that occur on a daily basis, we have a data center the size of about ten acres in Virginia right now, and we have others elsewhere in the country. It would simply be completely out of the ordinary course of business for us to try to connect all of those databases together going to Richard Purcell's point.

To have to create a consolidated record on a member of ours pulling from different databases that we have would simply be a task that would require enormous

cost, and furthermore, would require an enormous amount of time just to run a search to pull data, even if those databases were connected in some fashion.

The final point I would like to make is that with respect to what is going on in Europe, as AOL is active in Europe, particularly in the UK, for example, one of the principles of access is reasonableness of access and that there -- the access actually be able to be provided during the due course of business, and there is an actual purpose for the collection of that information.

We have encountered situations where we have been encumbered with requests to delete data in the UK from, again, our systems, which don't allow corrections. In those instances, we have had to come up with some roundabout solution where rather than deleting we simply clear the record, so to speak, by typing in Xs. I mean, that is literally how we have to deal with that problem.

Now, it's okay in a situation where in Europe or specifically here in the UK right now, requests for access are relatively rare, but if we move in that direction here in the United States, I think we have to expect that the U.S. consumer, once they learn of their ability to access information, is, in fact, going to

exercise that right just along the lines of people all sending in for their credit reports when the fair -- when that was first allowed.

MR. MEDINE: Thank you, Tatiana.

Final word from Jerry.

MR. CERASALE: Hi, Jerry Cerasale, Direct Marketing Association.

I want to look at the cost-benefit side very briefly, and assume that I come up with a great product, a great golf product, and I go on the web at JerryCerasale.com. We found recently, especially during Christmas season, that consumers tend to go to websites of which they know, so I'm going to try and drive some traffic to my website. I'm clearly not going -- I decide not to use e-mail, so I'm going to go out and get from Golf Magazine their list, I am going to rent the list for a one-time shot for a mail piece trying to drive you to this great website that I have.

From my perspective, if the name of the street is spelled slightly incorrectly and it gets delivered, it doesn't bother me. If I have your middle initial incorrect, I'd love to have a correct middle initial, but generally speaking from a marketer's standpoint, looking out at prospects, they're not too concerned about that. And that's looking at the use of that

data, and why is it that they're not concerned?

Because I'd love to be able to reach you and spell your

name correctly, spell your street address correctly.

It's because the cost of perfection outweighs any benefit to the marketer. I'm trying to reach someone, getting a response rate, you know, below 5 percent anyway, but then you look at it from the other side, that you suddenly come to JerryCerasale.com and you purchase something from me. I clearly want to have correct information. I want to ensure that I have your name correctly, your address correct, because I want to deliver the product, and your credit card number correct, and that's important for me.

And so maybe -- so, there is some access point here where I do want correction, but I don't necessarily want it from the marketing list. And it's really interesting, yesterday, to get the addresses right and have it from credit card information is important, because fraud is going down in use of credit cards in large part because of the addresses that we have. So, I'm interested there, but I'm not so interested in marketing, because I'm just trying to get a hit and get to you, and the cost of perfection is expensive, and I think we really have to think about that, even on the access side.

I don't want to require every small, new business to create an access position and eventually an access department, as I get larger, similar to the way

you have to do it with tax departments in companies. It is just not correct. To do that, you are going to drive the benefit of consumers of new small businesses, lots of choices on the web, are going to be hampered if you create a huge barrier to entry on marketing data access. You have to be -- look at the use and what you're using the data for.

I agree totally with Frank, if you're going to not give me a loan, if you're not going to give me insurance, those kinds of things -- that's important information you're making that kind of decision on, but if I'm Nordstrom trying to get a 10 per coupon to you, granted you don't get it and it's probably a problem, but the cost of perfection for me to get that 10 percent coupon to you is prohibitive.

MR. MEDINE: Thanks. I hear all the computers chirping, which suggests to me that they need a rest. So, why don't we take a five-minute break, and we'll resume with the last access panel.

MR. PLESSER: How long is the break going to be?

MR. MEDINE: Unless people want to push

forward. Do people want to press forward? That's fine. What's the sentiment of the group, press forward? If people want to stand and stretch, let's

move on to the last issue of identity authentication, authorization. That's certainly been an important theme.

I guess one question to consider in this context is to what extent should -- and we have touched on this a little bit, but to what extent should authentication methods vary with the category of information, the sensitivity of the information. Do we have a one size fits all authentication scheme? What's the approach? I don't know if there are people on the subcommittee who want to address that or anyone else, to pick up the discussion?

Richard?

MR. PURCELL: Richard Purcell.

There's a couple of points we've made, so I'll go through them as fast as I can to get into the discussion phase. One point we want to make is not only authentication mechanisms for consumers inquiring for access regarding their own data but also for those people who are not necessarily the data subject themselves and what kind of authorization mechanisms are available for them or should be made available to

them for access to information.

As David indicated, there are -- we're

recommending that -- for discussion that there are

varying strengths of access that should be made available depending on the sensitivity of the data. Certainly the categorizations or descriptions need to be fleshed out with the group as a whole. There are essentially two major areas of authentication that we're concerned about, and that would be the authentication by people who have a preexisting account and can be authenticated against information that they've provided, and generally that's done today in the weak sense using a member ID or a personal ID along with a password that has been predetermined in a prior engagement, and secondly, access by others who have no preexisting account. This could include system operators but could also include consumers who did not contribute information to a system but with some knowledge know that that system has information about them, keeping in mind that this is -- can expand somewhat.

When I send a -- when I enter a ship-to address for somebody else, when I purchase something for a family member or a friend, I'm entering information about that person into a system, not necessarily with

their knowledge or consent, and how do you provide access to those people about the information that that system stores on them when they have no preexisting

account?

There's a point that we made that isn't noted here that I think is perhaps worthy of consideration, also. In the illustrative model, we indicate that an individual uses various means, bi-directional means, of gaining access to and receiving information about the information stored in a system about them. It may be worth considering whether or not or how authentication would occur with somebody who is acting as an agent for a data subject. I used the example earlier of a parent who may need to be an agent and access a child's account, so -- and there may be other situations where somebody has to act in an agent capacity in order to view somebody else's account.

Finally, we have taken a shot here at defining a glossary. We use words in this group and in the industry not always with the same meanings but using the same words. We'd like to encourage the group as a whole to create a sense of definition around specific words. This is a hopefully somewhat provocative attempt at getting people to come out with better definitions. I'm not sure that we want to start

arguing over the meaning of words here around the table, but it certainly is an effort that I think that is worth accomplishing as part of the guidance that

we're chartered with here in order to create unambiguous definitions for specific words.

I think we all run into that problem today in lacking communication in this emerging marketplace where a language is yet to be defined other than in a dynamic sense.

MR. MEDINE: Thanks. One thing I hope people will address, rather, as the session goes on is the issue of agents that you describe. One of the trends that seems to be emerging on the internet is the ability of a site to gather lots of information about you and your relationships with a variety of firms for bill-paying purposes or for tracking other things, and that is essentially premised on that website getting access to your account so that they can provide that information, and the question is, is that appropriate if you've authorized them? Can a site limit access to only the data subject? If people have views on that, it might be helpful for the discussion.

Ted?

MR. WHAM: Ted Wham with Excite@Home.

I particularly liked the write-up from this

group, from whoever was responsible for it, I think there's some great depth here. I have three comments here about this topic.

The first one is about the relative tightness of passwords, security systems, you brought out by biometrics and tight security and so forth, and I'll direct your attention to the password definition which is on page 6 of this write-up that -- if you didn't have an opportunity to look at it. A weak alpha-only password being John Doe, all lower case, or perhaps a mixture of upper and lower case, but validated under either case, versus the upper case/lower case mixture including numerics, J, zero, that's a numeric 0, for instance.

There is a limit to what a website can do based upon their business model to enforce a higher level of security. So, if you wanted to have a real good secure model, you would have something similar to the latter or probably you'd have it even tighter than that where you couldn't use an E and turn it into a three or you couldn't use an O and turn it into a 0 and so forth do this.

A personal experience, I had a database administrator that created a number of password accounts for everybody and didn't create a mechanism

for the users to change their passwords, and they were very tight passwords, kind of nonintelligible and random strings of numbers, and everybody solved that

problem with the yellow sticky note, put it right up on the monitor of the computer. They couldn't possibly remember what it was.

So, the first point is on the business need to have a level of security that is based upon what the consumer will demand. We at Excite could not have a tight system. It would drive customers away.

The second thing is that within a loose type of a password scheme, which is very common out there on the internet, and we're talking about access to personally identifiable information, are you aware of the really ugly, silly things that consumers do to their passwords that are out there? The number one most popular password is the word "password." The second most popular password is an exact repeat of the user name. And the third most popular is some combination of one, two, three, four, five, six or some sequential listing of characters, something of that nature, which is a problem, and consumers have a low bar for themselves in terms of their tolerance of tight security.

So, whatever our access and potential

capabilities for correction are going to be barred by that, and if Rick wasn't scared about liability before, he should be now.

MR. MEDINE: I have heard that the most popular password in Washington, D.C. is "Redskins."

MR. WHAM: Interesting. Now we know yours.

Similarly, most websites already have, if a loose password isn't loose enough, we have an additional mechanism to have it looser, we have a password hit mechanism, where if you forget your initial password, we provide a way to go retrieve that. One of the most wonderfully loose ones is a set of four predefined questions. What's the home town where you were born in, what's the name of your pet, et cetera, and if you can supply those, you can get it back.

We actually had a system administrator within our chat product who had additional rights on our system, who could go in and disable accounts, you know, and she was born in Peru, and her question was what town were you born in, and she was born in a small town in Peru, and a malicious user pulled out an atlas and went one by one and went in and did that. When we talk about competitors being able to do this, this is already happening. So, all of this is bound to happen now.

My third point is I want to touch again on page 6, the personally identifiable information, although it this conforms with my understanding of it, we had

really very colorful discussions within access one about what PII is, and I want to throw two things out there more for thinking within the group than anything else.

First of all, the definition of PII is oftentimes household identifiable information. So, when you talk about personally identifiable, I think that gets down to a person, that's within the definition, right, but most people would say -- and for instance the COPA regulations talk about PII being information, and it really doesn't get you to an individual, it only gets you to a house, okay, and from that you can derive one of the three things. So, it's just kind of a point of reflection more than anything else.

The second one, a large point of question in access one, is is the record PII or are the fields or combination of fields PII? So, if you've got a record where you have got no ability to tie it back to an individual consumer, say it's a cookie-based record or a local UID based record, and I think we all agree that that's anonymous, but there was not clarity within our

own group where if you have got a record, where you have got say a first name, last name, address, zip code and phone number, just for conversation sake, whether

the other data attributes about that individual are also called PII or not. That was an open issue, if I understood it correctly.

MR. MEDINE: Stewart?

MR. BAKER: Yeah, Stewart Baker from Steptoe.

Just two observations. First, we can't expect technology to solve this problem for us. Digital signatures have been everybody's expectation for, you know, it's the technology of the future and always will be. Digital signatures are only as good as the person who does the registration that decides which signature you get, and those techniques can vary from pitiful to strong.

Second, I feel obliged to raise this, liability is going to be a big issue here. If you are a company and you are asked for access to information about a person, if you're asked about law enforcement, they bring a court order or a subpoena which confers on you an automatic immunity for compliance in good faith. If you don't get that in this context, then you have to put the bar as high as possible, because if you make one mistake and it results in harm in a person, and

just releasing an address could produce that harm, you are going to be sued and potentially held liable for not having had strong enough security. So, the default

is to the strongest possible security unless we can find a way to confer some kind of legal protection on people who follow other malicious methods.

MR. MEDINE: Quick response?

MS. MULLIGAN: Deirdre Mulligan.

I think a quick example is in the identification area, identification as it's tied to access, is the experience of the Social Security Administration with the PEBES database, and I agree that perfect identification is difficult, because we don't have good systems for issuing authorization permissions, right, and identity cert things; however, if you can stream down the data to which you are providing access, for example, if I say this is my account, you shouldn't have to give me my name and address and phone number, because I've said it's my account.

If all you're providing back is, for example, in the PEBES example, first they were providing employers, earnings, et cetera. At a second modification where they strengthened the authentication a little, but it was still not, you know, me showing up

with a photo ID, all they provided back was what I would be getting in disbursement of benefits. So that the risk of a third party accessing that data was so

reduced that you could also reduce the authentication.

MR. BAKER: But if I say I want to check to make sure you've got my address right --

MS. MULLIGAN: Absolutely, but what I'm saying is there is a sliding scale there, and I think in providing access, if you have somebody who says it's my account -- I say it's my account, you shouldn't need to give me my name and address, because I've said it's my account. So, if the data that you're going to provide me access to is relatively benign data, people keep talking about clickstream data as being very benign. Some of it may be, some of it may be not, but you can mitigate the risk, the liability potential, by thinking about what it is that you provide access to.

So, I think that these things are really tied together. So, I'm agreeing with you, but I think we need to parse through it a little more.

MR. MEDINE: Well, COPA has certainly introduced the sliding scale, and we're happy to hear more about sliding scales if that's the group's wish.

Alex?

MR. GAVIS: Alex Gavis.

I think in terms of intelligent agents, which you mentioned earlier, to some extent we use agents all the time in our lives. We hire brokers to do our work

for us. We hire people to clean our houses, et cetera. We hire people to do all sorts of things, and to the extent that in the agency context on the web, that there's a duly authorized agent that's acting on your behalf, it seems from a legal matter it probably should be a valid arrangement.

The question is how do you make sure that the authentication of that person carries back to you, and that is an issue which is or could be troubling, but I think it can be worked out.

In terms of security itself and authentication, I think an important element is going to be disclosure, and if websites are willing to disclose up front the kind of authentication practices that they use, to some extent customers will then be willing to opt in and opt out of those practices. I'm not saying it's necessarily a cure-all, but there are certain ways in which disclosure can at least provide a mechanism by which customers can affirmatively decide whether this is a website -- a commercial website operator they want to use or not and whether they think practices are sufficient for their purposes, for example, disclosing

that you use PINs and Social Security numbers or disclosing that you use digital signatures or -- and how that process works, I think would be an important

element.

MR. MEDINE: And I hope we will take up that issue of disclosure in the afternoon session, and the balance to be struck between disclosing too much to give away the system and disclosing enough for people to make an educated choice.

MR. JAYE: Just, once again, a different take -- Dan Jaye, by the way -- on this issue about liability and the sort of natural tension between security and access. The -- there also may be situations, particularly when there's -- you're dealing with onward transfer where a company will want to, in order to be sensitive to privacy, put contractual obligations on its data partner, and that data partner then may have obligations that place a very high threshold, you know, to the extent of even saying preventing access, on access to the data at its site or at its -- at that entity, specifically because of the contractual obligations put on it by the data controller, the data source, who is in effect just trying to ensure that there is no misappropriation of data.

MR. MEDINE: Okay, Rick?

MR. LANE: Rick Lane, U.S. Chamber.

Deirdre, I'm just curious, when you were

talking about my account, just to clarify, because maybe I missed the point, when you say you type in and you know it's your account, but if you're not looking at the address, then what are you looking at? So it says, hi, Deirdre. I don't -- what's the next step after that?

MS. MULLIGAN: Well, it depends. I mean, I'll give you an example. Actually under COPA, the children's privacy bill, there's a two-part process where you can get access with a lesser authentication device as a parent to kind of the categories of information that have been collected but not to the name and address of the kid. If you want to actually -- and correct me if I'm -- I think that's the right break.

If you want to get access to the full account -- okay, so this allows a parent to get probably a pretty easy online access to find out what has this site collected about my kid, what kinds of data, but if they actually want to get access to the exact data, then they have to go through a more rigorous authentication process, because you want to make sure

that you're not giving the name of a kid to the wrong person who actually isn't the parent, because the risk is much greater.

And so it's a way of both providing probably a simplistic, streamlined form of access that is very good at promoting a customer's ability to access data that might be useful but doesn't give them everything that's there but still provides a mechanism for them to get to the full record but with a heightened authentication piece, which is probably more costly to the business, perhaps a little more costly to consumer as far as it takes delay, you probably have to fax something in, you have to do some proof, and so it's a way of kind of balancing those out and offering alternative systems.

And I think when we're talking about -- Jerry was talking about marketing data, there may be marketing data lists where, you know, it wouldn't matter if you saw what's on that list about me, because they're so benign, it says, you know, frequent credit card user, lives in D.C., you know, I'm saying if you didn't know that it was my name, it wasn't Deirdre Mulligan, you said this is what we have, you couldn't use it in any way and harm me.

Now, if he was disclosing my name and address

to you, that would clearly be a problem, but there are ways to look at these and pull things apart a little bit.

MR. LANE: So, you are talking more about notice, if you're talking COPA, here's the information that's collected or the type of information we have on our customers --

MS. MULLIGAN: No, this is under the access provisions.

MR. LANE: -- compared to -- compared to having -- because again, once you have put your name in there, you are trying to access something, I guess.

MS. MULLIGAN: Maybe I didn't do a good job explaining. David, would you like to explain?

MS. RICH: Well, under COPA --

MR. MEDINE: Jessica Rich is our resident expert on COPA.

MR. WHAM: You better get a microphone.

MS. RICH: Hi. Under COPA, to obtain access to simple categories of information collected on your child, we actually -- the rule doesn't require authentication at all, because it is exactly like notice, and that's the conclusion we reach. To obtain the specific information collected, you know, on -- collected about your specific child, there's an

authentication requirement.

MR. LANE: Okay, that's what I was saying, okay.

MS. MULLIGAN: But you wouldn't --

MR. MEDINE: A sliding scale, also, depending on how much information.

MS. MULLIGAN: -- but the line wouldn't have to be quite that bright. The notice could be much more generalized notice and the categories could be not quite specific. Because perhaps I've said I might collect 300 categories of information in my notice, but the fact is on you, Rick Lane, I've only collected eight categories of data. I'm just saying that you can think about these things in a balanced way. You don't have to say every single form of access needs to be a highly authenticated, identification-based method.

MR. LANE: Unless you're -- Rick Lane -- unless you're talking about liability.

MS. MULLIGAN: No, if the liability is mitigated because the data that's being released bears very little -- could have very little impact on the individual.

MR. LANE: Subject to interpretation by a jury and courts and everything else.

MS. MULLIGAN: I mean, yeah, everything is, but

I'm suggesting that there are ways to think about structuring systems that help with that problem.

MR. MEDINE: I want to call on Dan, but I guess

to put another issue into the discussion that we want to address which is we've talked about authenticating who the individual is. The other issue is are we sure we're gathering all of the information in your files about that individual because of the natural tendency people have to use a nickname, variations that may make it hard to accumulate all the information you have. So, you may be trying to provide access, but the question is do you succeed in providing it. I don't know if people want to address that, but I just want to put that out there.

Dan?

DR. GEER: Dan Geer.

In some way, this is a response to Stewart inasmuch as I'm a security geek, that's what I do, and Stewart has been in places where this is taken quite seriously, as well. As the -- as the value of the information grows, you really only have two choices. One is to compartmentalize, and the other is to heighten the cost of getting in in the first place. Those are your only two choices. This is physics, okay?

If you compartmentalize, then there's this question of data fusion as a right that we've been talking about, and you make it harder. On the other

hand, if you raise the price of getting in, you very quickly exceed, just as was said about password choice on the public situation, you very quickly exceed what you can expect them to do, and you're left then with only a few things that are strong enough to make fused data safe, despite its being fused.

Biometrics is the only answer in that regard, but I would point out that biometrics are not a secret. My thumb print is not a secret. What you have done is you've forced the question of secrets, which is the only way we currently protect data, to where it's -- what I'm using to access it is no longer a secret. Rather, you have pushed it to where a security access device is the issue, and it's the bank ATM that's looking at my iris or it's the palm print reader that let's me get onto the airfield from the concourse at the SFO or whatever. So, your choices are very limited here.

From a technology point of view, everything else is wishful thinking, and most of my job is to avoid wishful thinking, that's what I do. So, I just want to be clear that you either compartmentalize or

you raise the cost of access. If you raise the cost of access, we very quickly exceed what the average person can do, you're down to biometrics, and now you have got

to have provable access devices.

MR. PURCELL: Richard Purcell.

I just want to point quickly to the naming convention that we kind of landed on for our group, which is a little bit long, but hopefully it helps break out this -- the thinking about this. We are thinking about in this space identity, as well then as authentication, as well as authorization. Biometrics do a good job of identifying an individual. There may be need for additional strength in order to authenticate an individual's -- a known individual's access to a known set of data. There may indeed further be a reason to authorize or to examine the privileges that that person has to certain parts of the data that are being revealed.

Now, to David's prior point about fusing data and people using different forms of identity, we have to be very careful. If I can identify you unambiguously, if you can authenticate yourself, and if you have the authority, then I will let you look at the data that's relative to that identity. If you've identified yourself in three different ways, you will

have to further identify yourself in all three ways uniquely and in different moments in time in order to look at the data that is contained or linked to each of

those identities.

MR. MEDINE: Jane?

MS. SWIFT: Just two quick points. On the first, I am glad we entered into a discussion about biometrics, because I think one of the biggest issues we face at the state level when it comes to the time where sort of the rubber hits the road and we're trying to protect consumers is identity theft, and particularly in the area of biometrics, I'd be interested to understand how as we increase methods of authenticity and identification, we also protect the fact that if you steal someone's electronic thumb print, it's not exactly easy to change.

So, how do we, you know, guarantee that those things that are very, very difficult to change that maybe now are being utilized for my own protection do not, in fact, give me greater risk, and I think that probably is the conundrum on a lot of these issues, and to the much more mundane, I know this is not a rulemaking body, but I would propose in the best of intentions that you find some way to cool this room off before the afternoon or whether or not catching a plane

to the afternoon isn't going to be what determines participation.

MR. MEDINE: We appreciate the feedback,

thanks. Let's take a couple more comments, then we'll break for lunch.

Deirdre?

MS. MULLIGAN: I wanted to respond to the suggestion that providing notice was going to be useful for consumers in assessing security, and I think this is where we have a market failure. I don't think consumers can assess the appropriateness of security devices. I think, you know, if you look at something as simple as credit cards, debit cards and check-writing cards, I don't think consumers are faring that well, are they? Just that -- I mean, we have a -- you know, you have an issue here where the people who are in the best position to assess the security are not consumers. It's, in fact, businesses, and I think that that does go to the liability question, which Stewart put on the table, that when you have a problem where the person whose data may be at risk versus who is actually defining the device, which I agree with you, it's -- we're talking about devices here, are different, that you have to figure out how to make sure that the liability is appropriately placed.

The marketplace has done that in the credit card area, I think, although I think that by shifting the liability into the tax realm, it has actually

deadened the evolution of better authentication of credit cards. So, maybe it's not a good example. So, that's one.

And the other issue was actually what Jane Swift raised that I think the other part of the security device question is what risks are you building in on the back end for further erosion of privacy, and when we think about thumb prints, we can think about capturing raw thumb prints, we can think about capturing, you know, encrypted ciphers that can go one way. We can think about lots of things, but they are not things that consumers should be asked to think about, because I don't think they have the expertise. I don't think I have the expertise. I'm going to look over to Mr. Geer here.

MR. MEDINE: Two quick comments. Greg and Frank, then we'll break.

MR. MILLER: Greg Miller, MedicaLogic.

We actually are making extensive investigations into biometrics now at MedicaLogic. We use them throughout our physical facilities for patient record depositories. We are also evaluating the application

of them and the appropriateness of them for consumers' access to medical records, and I just want to point out that at the end of the day I submit to you that whether

or not you're using a biometric or you're using a digital certificate, the issue boils down to one of cryptography. So, we will leave it to that for a discussion offline for anyone who wants to go down that road.

Secondly, there has been a lot of discussion about the theft of identity using biometrics, and I just want people to bear in mind that I think Dr. Geer's comments about costs and the cost model, and your decision is absolutely what we should be focusing on, because as we're finding out, the scalability of biometrics and theft identity are very interesting. You can just forget the Hollywood sexiness of it. You can't just go take someone's fingerprint off of a cup and suddenly you have stolen their identity. Biometrics actually take a three-dimensional look at that, and the minutia files that are developed from them pass the duration of the algorithms, but the algorithms are finite, so there's a domain space problem.

Biometrics at the end of the day are a machine-level authentication service, and I submit to

you that's it. Once you start traveling biometric minutia across the wire and using them as an authentication, so if someone can walk up to a kiosk,

authenticate themselves and go to that extent, you are going to have problems. It's called name space violation. Here's the problem. If biometrics become a standard across everywhere, a finite number of algorithms, finite number of ways of doing it, suddenly it only takes one space violation, and now I have you across all spaces.

If I violate -- if I find out or reverse-engineer your thumb in the banking industry and you're also using that to get into your car and you're also using that to get into a hospital, the whole thing breaks down. So, I don't -- I want to caution us to not run down the road thinking, wow, biometrics, Hollywood sex, this is great. It's not a panacea. There are limitations, and it's probably a sink hole to go into too far on the technical minutia.

MR. MEDINE: Okay, last comment, Frank?

MR. TORRES: My comment is really brief, and then I'll let Ted go.

MR. MEDINE: If anyone else wants to speak, we'll let them go after lunch.

MR. TORRES: Just real quick on biometrics, I

think we need to take a balance to see the usefulness of biometrics. I know banks started requiring thumb prints before they would let people without an account

with the bank cash checks at the bank, even if it was a -- say an employer -- an employee trying to cash a workplace check, and in some cases, with some populations, they were very nervous about having to provide -- you know, why provide the thumb print. What level of security did that really provide in that circumstance?

So, the solution to the authentication question needs to fit the circumstance. I mean, the banks certainly weren't scanning the fingerprints and calling up the -- calling up people's information before they actually processed the check. So, we just need to be sensitive about the effect that biometrics might have on certain populations.

MR. MEDINE: Thanks for the final comment. We will resume at 2:00. We have a restaurant list. We certainly encourage people to visit the Top of the Trade on the seventh floor. Thanks.

(Whereupon, at 12:45 p.m., a lunch recess was taken.)

AFTERNOON SESSION

MR. MEDINE: Why don't we get started on the security issues. Let's move into security, and what I propose to do is to go roughly until about 3:30, take a break, finish up the discussion of the three security groups by around 4:30 or so, give an opportunity for public comment, if anyone from the public wishes to make comment, and then organize ourselves into different groups to develop options as we go forward.

MR. MILLER: David, I just want to point out to you how warm it is in this room, you can see this water bottle.

MR. MEDINE: For the record the water bottle is wilting. We apologize. Seasonal changes do things to heating. We're not quite as high tech as many of you are in adapting to changing environments, but we're working on it.

(Discussion off the record.)

MR. MEDINE: We're working on it. In the meantime, let's focus on the security. The faster we talk, the faster we can get to a cooler place I guess.

Again I again commend the security groups for

their work and try to focus again on security issues

from translating the wide range of possibilities to

operational standards and implementation methods, and we

touched on this a little bit, but is security a one size fits all situation? Are we going to vary it based on the sensitivity of the information, based on the kind of web site, based on the financial abilities of the web site.

Again, I don't know if people in security one want to make some initial comments or others want to jump in. Please let's remember to -- for the benefit of the court reporter to identify yourself and speak into the microphone.

MR. WHAM: I think we got our wires crossed. I'm going to begin with a comment from the last session that I didn't get an opportunity to make before the break if I may steal that.

A couple things, quickly on biometrics, I'm very excited to see about biometrics --

MR. MEDINE: And identify yourself again.

MR. WHAM: Ted Wham. Thank you.

MR. MEDINE: Appreciate the comments.

MR. WHAM: I would recommend that we take a look and focus of what the cost benefit is of that for a free internet photo site such as ourselves with

literally 50 million users. I was in a discussion at the end of the last session where people were crowing about the benefits of thumb records that would get down

to $20 per unit mass production, and I thought a hundred million dollars, that's awesome. That would be a great thing to be able to provide for all users, but that may be a long way out on the horizon before that happens.

The second thing, you're going to have forgive me, I'm going to return to my point earlier. The comments were made that -- the example that I provided was a personal example, and I would like to point out that example applies equally as well to most business settings Excite@Home is a very large user of Sun Computer system boxes intending to not prefer the offerings from our neighbors to the north on the Internet service.

But on those boxes, they sell us literally web servers that come in on the pallets, and the sales reps who deal with us I'm certain are keeping an enormous amount of information about us and are making all sorts of decisions about our price sensitivity and about our willingness to take special offers where there's no right of access, and yet it's inferred data that in a commercial setting is absolutely applicable.

I'm not aware of very many instances at all

where there is a right of access by an individual or a consumer in a non Internet setting to infer data from business organizations, and I think it's a terrible

precedent for us to moving down that path in trying in that direction.

MR. MEDINE: Any other people who would like to make comments based on that discussion?

Okay. Moving on again to security issues, anyone want to kickoff the discussion of how we go about establishing operational standards for security? Dan?

MR. SCHUTZER: I think that --

MR. MEDINE: Could you just identify yourself for the record?

MR. SCHUTZER: Dan Schutzer. I think that we all mentioned, security is not perfect, and it's going to change back and forth according to what you do and what cost trade-offs and terms and risks are, so I don't think we should legislate what level security anybody needs.

What we should do is let the market decide that, but what you need is a disclosure of the security. In other words, what you need to do is you need to let people know to what degree are you protecting things and even if they want to, what techniques and to what extent you're protecting the security and let the marketplace

decide, and of course your liability is also dependent upon that.

That said, there also needs to be a companion

program in terms of awareness, that people are aware of what the various kinds of security risks are and what the various kinds of security safeguards are in understandable terms.

MR. MEDINE: Deirdre made the point earlier about the consumer's ability to evaluate and weigh competing security systems, and maybe she'll comment further on that.

MS. MULLIGAN: I guess what I would do is go back to Greg Miller's comment. He said security -- we were talking about authentication, the most important component is encryption. You say the word encryption and most consumers, their eyes glaze over, and I agree that education, people need to be more aware about the importance of security, but I am very doubtful of whether or not the average consumer is going -- in order to evaluate whether or not security is appropriate, you have to be able to evaluate the risks and the threats.

And I think that consumers are not necessarily in the best position to evaluate the risks and the threats because they don't know how you're using data on the back end. They don't know what you're doing with

it. They don't understand security protocols. They don't understand technology.

There's a reason why I don't do the purchase of

our security components for our web system because I don't have enough knowledge, and if I don't have enough knowledge to do that kind of evaluation, I don't think it's an appropriate -- I don't think that providing notice is enough in a marketplace where consumers don't have the ability to assess.

I think there's a really question about competency, and I'm not suggesting that the average consumer is not smart.

MR. SCHUTZER: I disagree. I would say that if you asked me two or three years ago if people would know what a URL is, how many gigs in a PC. I think the understanding is marching forward, and I think that just the mere fact that you're sitting here talking about -- throwing around terms like encryption, it's not so mysterious.

It doesn't have to be that hard to indicate to somebody what's the concept of it. I'm not saying you're going to go down and talk algorithms, but I think an education program can make it worthwhile. We make an education program to the people in our credit card -- who use our credit cards and so forth, checks, what's

the risk involved of giving certain kinds of numbers

away, what kind of fraud they can have and so forth.

I think it can be done.

MS. MULLIGAN: Oh, I absolutely think education is important, but I'm suggesting that education alone is not sufficient because I don't think that the person who's in the best position to evaluate whether or not a certain level of security or a certain technology or a certain protocol is reasonable or appropriate is going to be the consumer.

MR. MEDINE: Let me pose a question and then call on some folks to the right here, but to the extent that security is part of Fair Information Practices, there's a threshold question I guess of whether everyone should have some security the way -- or not.

I mean, if it's a purely marketplace decision, then not, but if it's part of Fair Information Practices, does that suggest a minimum requirement of security or not?

Again this is something where we look to the committee's thoughts on that subject matter without prejudging the question, but it would be useful to get your responses. Is there a floor of security that is part of Fair Information Practices that everybody should have and then people can do better and the marketplace

23 can determine how much better or should the marketplace

24 determine whether there's security protection at all

25 and how does that relate to the concept of security as a

Fair Information Practice. Tom?

MR. WADLOW: A couple things. I guess -- oh, Tom Wadlow, Pilot Network Services.

(Discussion off the record.)

MR. WADLOW: A couple things actually based on some of the discussions that we were having at lunch, one comment that I wanted to make is we were talking a lot about access and security here, and I think a lot of people would benefit from, perhaps this can be taken as stated by the chair, access to what, security of what, because I think that really focuses a lot on this discussion. If we have a good sense of what that is, that will shape a lot of this discussion.

Having said that, the other thing based on some other comments here that I wanted to make up, I wanted to make sure some comment came out of, was people talk about security and we can have security and we can do this.

It's very important to realize, this is what I do for a living, and Dan is also in a very similar situation. I can't speak for him, but I know we treat security not as a thing that you have, but it's a

process, and if you don't think of it that way and if you don't really have that in your rein, you're going to lose a lot of the aspect, and you say, Oh, we have

biometrics, therefore we have security or we have encryption, therefore we have security.

That's crap. None of that is security. Security is the process by which you employ various things including those tools, and that's a very important distinction, and it is one that is I think very much lost in the general public. I mean, most of the public's impressions of security comes from movies quite frankly, and we think that, not like the movie, tends very much to be something that they don't understand or really don't want to get involved in.

I do spend a lot of time trying to educate people on security issues, and I think that there are a lot of subtleties here that I would not expect my mother or anybody's mother for example to need to understand, but it becomes very important for groups like this to understand.

MR. MEDINE: Thanks. In terms of the focus of this group, again the charter in the bylaws largely speak to it, and I hate to confine it too carefully, but I want to leave a lot to the group to give us feedback about what it views as the scope of this group's

mission.

Obviously we're focusing on online information collection and access to that information and security

of that information, but again I don't want to -- I don't want to limit your possible consideration and the possible options that you might put forward.

Stewart?

MR. BAKER: Sorry.

MR. MEDINE: That's okay, finish your cookie.

MR. BAKER: It seems to me based on the work we've done in the various sub groups that there are at least three options for dealing with security if you want to have a regulatory solution, and one of them is to require appropriate security at various levels. Another is to set minimum standards. Another is to require disclosure of your security practices.

All of those have problems. Trying to set security standard is probably the most impossible. Security is inherently contextual. It depends on how badly people want what you've got, how much it will cost you if they get it. There's no point in spending $40 million to protect $400,000 worth of assets, and it's possible to trade-off any number of procedures against any set of technologies to get the same level of security.

So it wouldn't be possible for anyone and certainly not the FTC or a voluntary association to set one set of standards, which leaves us with minimum

standards and notice.

Minimum standards by themselves are also very hard because what constitutes good security depends on what attacks were invented last week, so you have to have a system of setting those standards that takes into account what was done last week.

Also a lot of stuff is not worth stealing, and so you don't need very good security most of the time, but if somebody is determined to get it, then they can get it, and so it's hard to know what the minimum should be for something that isn't worth breaking in to steal.

Finally, on disclosure it sounds like a nice solution. I'm not persuaded myself that -- speaking as a lawyer who would have to give legal advice on how to write those security disclosure statements, what would you say that wasn't packed? You can say we use SSL. Well, big deal. You can look at the block on the bottom of your screen to tell they use SSL and then you put in a bunch of blather that sounded secure and didn't actually say anything, and you just wanted to make sure that it's not so concrete that the FTC can find you didn't actually do it.

So if you really want to have security disclosure standards, then you have to start prescribing the content of those notices, and then you're back in

the question of what attacks are we going to ask people to provide information about in their security measures, how much detail do we want. There aren't any easy answers.

MR. MEDINE: Going back to your first two points about standards and minimum levels, the way, as you know, the law finesses that often times is says that you should have reasonable measures in place, and obviously reasonable is inherently contextual, that is based on reasonable in response to the latest attacks, in response to the amount of quality of information that's being protected and so forth.

Is that a standard that gives you enough to advise your clients about what to do?

MR. BAKER: Up to a point, but the question then arise reasonable from whose point of view? I mean, every piece of data that's on a corporate system has value to the corporation or they wouldn't keep it there, maybe not much but some, and so they'll want to protect it up to a point.

So you might think, Well, I spent enough from my point of view to protect that data given its value to

me. Now, what about certain circumstances in which it's more valuable to the consumer than to you, should you be spending more and how do you know because in many cases

you won't know that this is sensitive data until it's been compromised and you've been sued for not having reasonable measures.

So I think the question of who's perspective you're using is probably the most central one, and if you're going to use the consumer's, how do you get that information in front of the data holder.

MR. MEDINE: Paula?

MS. BRUENING: Paula Bruening with TRUSTe.

Paula Bruening with TRUSTe. I just wanted to comment on some of the things that Deirdre had mentioned about the consumer's ability to understand notification about security and the detail that's there, and I would like to sort of talk about just briefly from the perspective of notice in general, and I think we have to be very cautious because I think notice seems to be over and over the cornerstone of the Fair Information Practices that we're relying on and the system that we've created here to protect consumer privacy.

But I think that we have to be careful that we're not overburdened the principle of notice to the point that it becomes something that in general is just

impossible for the consumer to work with.

I mean, at TRUSTe we look at notices all day long, every day. They are getting bigger. They're

getting longer. They're getting more complex, and they're getting more legalistic, and we have to keep pulling our licensees back from that to make them cleaner and more streamlined and easier to understand.

And when you're talking about something that is as technical and complex as security, I think you have to be very cautious before you run head long into looking to disclosure to solve that problem of security as a sort of single approach.

MR. MEDINE: Thanks. Greg and then Lorrie.

MR. MILLER: Greg Miller, MedicaLogic.

MedicaLogic would like to offer some small pieces of empirical data for some experiences that we have. As you can imagine, people worried about their health -- the sensitivity of their health care data and how it's secured and private, particularly on the Internet settings has been a very instructive study for us.

And we've had a pilot program running across four large hospitals in the United States where we've actually been doing focus groups and collecting data, and I just want to submit to you that one piece of data

I'll give, you believe it or not, a significant minority of individuals when asked had no idea what the lock on their browser window meant, sad but true. Bear it in

mind.

Number 2, we found that talking about security is a lot like talking about air line safety folks, and you want to get through that video and then get on to hear what the service is all about because it's just not something you want to spend a lot of time dealing with, right? When something goes wrong it's fairly very cataclysmic.

So we're finding what people are looking to understand is privacy and appreciate that security is an implementation of privacy, and as this was pointed out earlier by the gentleman from Pilot Network, security's more than just a technology. It's people and process, and I think I mentioned that at our last meeting.

And I think what we need to be looking at here are guidelines, and I know from my work in this group here, the idea was to put together guidelines that would perhaps be best implemented by somebody, say a TRUSTe who really takes the responsibility for figuring out how to convert all the techno babble into an assurance that built, and here's the vital word, trust amongst the user community that what was happening was protecting the

23 privacy and confidentiality.

24 MR. MEDINE: Again, I think it would be very

25 useful, the options stage of this process is again to

present the options of disclosure on the one hand versus doing it on the other hand and how those two relate in terms of accountability. Lorrie?

MS. CRANOR: This is Lorrie Cranor. So I agree with most of what Stewart and some of the other speakers have said, but I think coming up with notices about security, even for an audience of security experts is just not a task that's going to work.

I think if you were to go up to one of the security experts in the room here and say, Well, my web site uses this type of encryption and this type of firewall and whatever, is it good, they'll say, Well, no I have to see the whole system, I have to really look at all your processes.

It's not just whether or not you're running this kind of firewall that determines whether or not you have good security, so if you can't get a security expert to figure it out based on that sort of notice, how on earth can you expect the consumer to have any idea?

So I just didn't think that's going to be useful, so what do you do? It would be nice if we could come up with a standard for security and say people

followed that, we know they're good, but again it's constantly changing.

The threats keep changing so I don't think

there's -- we can come up with some sort of list of best practices and the IETF and others have done that, that help to some extent. The other thing that's happening is that some companies are buying insurance in case they have security problems, and their insurance underwriters I'm sure are examining their systems and trying to determine if there is enough security that they feel comfortable underwriting the insurance policy.

So I think a group like TRUSTe or the BBB could have some sort of insurance, but unless they're held financially liable in case there's a problem, it's not clear that they would have the ability to do the kind of checking that is really needed to assess somebody's securities.

MR. MEDINE: Thanks. Also, just a question, against what standards would the TRUSTe or BBB judge security on a case by case basis. Ron?

MR. PLESSER: Well, two questions. One is, again from looking back at the privacy commission days and having a little bit of that perspective and maybe talking this to 30,000 feet, the Department of Defense in implementing the Privacy Act spent a lot of time

going through all the record systems and doing all this

work and getting the consent and knowledge and setting

up all these systems of access and all this stuff.

And then one of the bases, I think Manila at the time or maybe it was in California, decided that as part of being good citizens on a paper reclamation, they sold the printouts to a trash dealer, who then sold it to fish guys that literally wrap fish and so the payroll histories of all of the people at the base could kind of -- was imprinted on fish that they were wrapped in.

So I mean I think that we can get a little crazy about again the detail of security and talk about some reasonable procedures, and it shouldn't -- you have to take reasonable efforts. I think it is a good standard. I think the question is really not one of notification. I agree with what Lorrie said.

To tell a consumer anything more than you were going to take reasonable steps to ensure the security of the data is unreasonable. What is reasonable is to require or to suggest that companies have internal claims that they have to document and in advance to themselves what privacy protection -- what security protections they've taken given the relative value of their judgment of what the risks are.

Will a jet plane come in and crash -- maybe if

you're at the end of the runway, that's not such a funny risk to consider, and if you're someplace else, maybe it is a funny risk to consider, but the company should do

this themselves, assess their own risk and assess what they think is reasonable response to that risk is.

And then if they suffer a loss, they're going to be responsible to -- did they take reasonable steps to avoid any anticipated risk, and I think maybe if the Trade Commission goes in and looks and says, you didn't even consider this, you didn't even try, you didn't even think about the fact that you were at the end of the runway and a jet was going to come in or whatever the thing is.

So boom that's deceptive or unfair or whatever your authority may be, not that I'm suggesting there be any, but that's the standard we think. That's the way you do it. I don't think you do it as a disclosure to consumer. I think you in the end have to decide whether or not they took reasonable and best efforts, and they really had to define it. Maybe industry codes can help, but it really is something that has to be done by an individual company.

I think what I'm suggesting is very close to what the requirements are at the Securities and Exchange Commission where they do not require the maintenance of

financial records, reasonable efforts to be secure, but what they require is that you've done a plan in advance to assess the security risks and how to prevent those

security risks, and if a public company then has a loss, a security loss, the SEC goes in and looks at that plan and thinks and sees if that plan was reasonable in light of what happened.

And I think that's the approach you have to take, not setting any specific standards or detailed disclosures to consumers or any other usual things that the Trade Commission might look at.

MR. MEDINE: How do you factor in the points that Stewart made that value of the security to whom? And the identity theft is a classic example where the victim of a identity theft, it's a tremendous value to avoid being a victim of identity theft. For a business to give up the identity of one consumer inadvertently proves less harm to the business than it does to that consumer.

How do you weigh the consumer interest in that process?

MR. PLESSER: Well, I think if you're a credit card company and you have vital information about a lot of consumers, then I think the risk of identity theft is great, and you have to take strong action. I don't

think anybody is going to hold anybody to full safe standard.

But if you're a catalog company and you don't

have that detailed transactional information and you take reasonable efforts but perhaps not as strong as the card company, so I think again it's what you look at at the end to -- you as government look at at the end, so I think that gets worked in in terms of the nature of the risk, but I don't think there's any absolute -- you can't -- no one can really set up the standards that a company is going to apply in a particular circumstance.

I think Stewart and I agree on that. I think a company has to do it, and then you can judge if it was reasonable.

MR. MEDINE: Deirdre?

MS. MULLIGAN: I want to agree with a lot of what Ron said. When I think about measuring -- he said set up some standards. I think you asked the question though where is the rub, and the question of reasonableness all depends on what your exposure is, and unfortunately we have another incidence where the exposure -- the risk of a security failure may not be borne all by the person who's making the security decisions as to what's reasonable.

And so there's another question about, How do

you increase the incentives to improve security when the risk may not be obvious, and I think that's where questions of liability, questions of -- and liability

can be created in a number of different ways.

I mean, if there was a requirement, for example, to notify consumers any time you had a security breach that led to the disclosure of some piece of their information or an inappropriate access to their information, I think that all of a sudden the assessment about what was reasonable security might change a little bit because while it's not financial liability, there's certainly an increased incentive to pay attention to your assessment of reasonableness.

So I think there are some ways to impact on what's reasonable, but I think that leaving the determination of what's reasonable purely up to a single company doesn't allow businesses to benefit from the collective knowledge that's out there that's in a way that's most productive.

So when I look at things like the CERT advisory, I think there are some reasonable things that can be built in, so, for example if you're running a specific back end program, that it would be reasonable to me to expect that if there are known bugs and known failures that have been documented and that there have been

alerts about, that within X amount of time you should close those holes.

And unfortunately we find that that doesn't

happen all the time, and I don't think that it is -- it's not reasonable not to educate yourself about the risks of products that you're using, and I think that that's where there could be some useful development of, What are the things that you should consider in developing your reasonable plan, and saying, Yes, of course you're going to develop it based on your business.

But that you have to go and look in this place, this place and this place to determine what would be reasonable to incorporate.

And I think if we can move in that direction, it would be helpful.

MR. MEDINE: Jane, your card was up earlier. Do you wish to comment?

MS. SWIFT: No.

MR. TORRES: Okay. Frank?

MR. TORRES: Frank Torres, Consumers Union. I also think Ron raised some interesting points about how we go about maybe getting at that -- the reasonableness question.

What I would like to raise is that kind of

something that I think has been a little bit left out, and that's the consequence question. I as a consumer -- hopefully there will be some plain English as far as

disclosure goes to tell me truthfully what I can expect from your site as far as security goes, but at the end of the day, I don't care what program you're running.

What I want to know is you're doing the best that you can do to keep my information safe, and if for some reason the information gets out and there's some consequence to me, identity theft, my credit card numbers get exposed online, on those types of things, how do I resolve that?

How do I get redress? What steps would you take to close down the open doors that allows this information to get -- how do I go about -- will you help me go to my credit card company and resolve my disputes with them?

So in addition to just the basic security question, I think it will be very difficult or if not impossible to say you've got to follow this standard, that standard or this standard. We recognize the risk.

To carry on the airline analogy the safest airplane is the run that sits on the ground, but that doesn't do anybody any good at all, so we've got the FAA out there that says you have to meet some minimum

reasonable requirements or there's some government overlay there, but ultimately it's -- people are going to fly on the airlines that are the safest or the ones

they perceive to be the safest, so maybe that's a fitting role for the Commission to take on.

MR. MEDINE: We'll look forward to your recommendations on that. Tatiana?

MS. GAU: Tatiana Gau. I would like to start out by saying that it's interesting to see that these discussions are becoming more and more similar to the discussions that were held last week on Tuesday at the White House, The Internet Summit on Security, and there were a lot of the issues that we're discussing that were brought on the table, but fundamentally the points that I would like to mention relate to again security as being something more of a process.

One of the things that is clear is that different companies are putting different amounts of money into dealing with security as a process, whether it's an investment in technology or investment in people.

And I want to stress the people aspect because not only is it an issue of having the technology in place, but having the people to update the technology when alerts are put out and bugs are discovered and

fixes need to be implemented, people to monitor the processes to make sure that in fact they are running properly, and thirdly, people to respond to an incident

when it happens. If a breach does occur, are there people there to respond to it quickly and close the hole?

And the experience in the room among the large industry planners was that, yes, there's a certain shall we say percentage of companies on the Internet today that do have shall we say crisis staff or security staff that are available 24 by 7, but the vast majority do not have people that are available under those kinds of circumstances.

The other point I would like to make is there was great discussion of evolving standards, that it's hard to actually set a standard benchmark as to what kind of security companies should have, but there was discussion of penetration testing, similar to kind of an idea such as a licensing entity such as TRUSTe.

There are also companies out there that actually do auditing with ethical hackers, and they'll see if they can penetrate your systems. If a company invests in that kind of an audit and publishes the results of their audit with the appropriate caveats in case a breach does occur obviously, that in and of itself is

probably more useful to consumers than having some explanation of what the technology is that's being used.

Thank you.

MR. MEDINE: I guess that raises a question as to whether companies ought to commit to being audited and tested as part of reasonable security measures.

Larry?

MR. PONEMON: I love the word audit, very good. Let's use that word more.

Stewart, I think I disagree with the idea that there are no standards. I think we can actually create a too dumb to live standard, and it looks something like this. Can you imagine getting on the walkway with your local airport and you see a plane without wings. In fact, they're putting on the wings. Now, would you fly in that plane, and the answer is I hope not.

That's the too dumb to live standard. That means you basically do not do things that are clearly going to be very silly, right, or very dangerous or very risky, but I don't think that adds any value. I think what people expect is a certain level of disclosure and a certain level of security, and they pray that they are safe, that they are not the next victim.

They expect organizations to produce the risk in

the form of a statement that articulates in clear and concise language that these are the risks. When you transact business with us, these are the risks.

Now, believe it or not when we do a financial statement audit of a large corporation, we actually evaluate the integrity of the technology infrastructure. We're already doing a lot of that stuff, so I'm not sure if it's impossible to create reasonable standards in a relatively short period of time. I'm not saying we as an industry. It could be us or it could be government, but I think it is probably doable and certainly doable in my lifetime.

I don't think though we could ever be in a situation where we will not have -- we will have good disclosure or great disclosure and good security or even great security and still avoid the liability issue, so I think whatever we do, we always have to think about something will go wrong, bad things happen, and we need to have a very good, very tight remediation strategy, and so that's all we can do.

If we try to do more than that and try and apply perfection, no one's going to go anywhere, so I think we can and we should work to develop some baseline standard that is hopefully higher than that too dumb to live standard.

Thank you.

MR. MEDINE: Thanks. Dan?

MR. SCHUTZER: Well, we heard a lot of things so

I would say that what have we heard? We've heard that there's obviously some minimum level best practices that isn't really tied to technology at all. Do you have a security officer? Is he trying to keep up with the software and the technology? Is he giving people background checks to those people who are sitting there matching the data? Are you planning to tell people that when they send you data, it's all at their risk or you can offer them some kind of recourse.

These are simple, straightforward kinds of best practices and disclosures you can make about that without getting terribly technical, and certainly I still think that education plays a key role because the truth of the matter is is that independent of firewalls, cryptography, all that kind of stuff, it's social engineering that normally breaks in and gets you your access, and social engineering is walking around your own end consumer and their lack of ignorance which they need to be educated in to just who they should trust when they're giving a kind of information.

So if somebody phones you up and says, I'm from Citibank but they've initiated the call, I'm from

Citibank, could you please tell me your password or something like that, then you would be remiss to give that password. You didn't initiate it. You didn't

contact the individual body. They contacted you. How do you know who they are?

So I think that some combination of education, of disclosure at a gross level say, Here's the kind of best practices, we're not going to tie you to a specific cryptographic algorithms or something? Do you have some of the basics? Do you really have some professional security staff? Do you do ethical hacking? You have to describe of course what ethical hacking is. You don't have to show the results.

That could get down to bits and bytes while you're doing that. Are you keeping abreast? Are you checking out your people? Are you using the normal good prudence? And the disclosure, because you may find that the kind of business you're in and for the level that you're doing, you want to just say, No, I don't have that, this is the kind of business I'm in, you're at risk if you use it, but I think the kind of data I'm asking and the kind of service I'm doing are not going to put you too much at risk.

The bank said that then they wouldn't have any customers anymore, so it depends on the nature of the

23 business you're doing and what kind of risk you have,

24 what you might want to advertise and what the customer

25 should come up with.

MR. MEDINE: Thanks. I would like to continue the discussion but transition it into the next subgroup which is not significantly different from what we've been talking about, focuses on managerial and technical steps, and one of the things you talked about was employee screening and training and access issues.

So Rebecca had her card up before that, so you're free to talk about the prior or current or both.

MS. WHITENER: Rebecca Whitener. Actually several of the points I was going to make have been made and have been made very well, but I wanted to again go back to the whole issue of the importance of the process and the organization, and in fact in looking at what does make up appropriate security, generally companies have used some form of risk assessment to determine the appropriate mix of organizational types of processes and/or technology that is necessary to address risk.

However, many times that risk assessment has been built on the risk that the company perceived in terms of their information assets from the standpoint of the confidentiality, integrity and availability of those assets so that if it was company financial, proprietary

information, it would be very miss and critical, and we want to make sure we have the appropriate safeguards and the controls of that information.

I think as we begin to talk about customer information and appropriate risk assessment and/or security safeguards for that, it may be in a different mind set or a model that companies are moving in to because in reality, the risk associated with disclosure, customer information, particularly customer names and/or contact information, may not have been as high on the list in the past as it is now becoming as the risk is beginning to be seen as a far greater risk for improper disclosure.

So perhaps what companies need to be aware of is that in their current processes for evaluating risk assessment and determining the appropriate controls, that they begin to view company data a little bit differently than they have in the past.

I like the analogy of the airplane, but another analogy that I also like to use in terms of what consumers expect when it comes to security is that when a consumer buys a car, they don't but that car because it has great brakes, but they sure expect that that car have brakes when they buy it.

And so in many cases it's the same way when a

consumer does business with a company that they trust and they have confidence in, they don't necessarily have to know how those brakes work or how the security works,

but they sure want to have the confidence that those brakes are in place.

MR. MEDINE: Thanks. Dan? Alex?

MR. GAVIS: Alex Gavis, Fidelity. I think in terms of the custody and storing of data which would be sort of internal practices, I think it's very important to consider a reasonableness standard and a standard that sort of takes industry by industry because I think the only way, particularly if you're looking at sort of broad mandates or broad sort of policy making in this area -- the only way that you'll be able to handle it is by essentially looking to best practices in each industry because there are different industries that handle different information differently and have different sensitivities and have different levels or need to store information.

But I think there's another part of security that's important which is I would term maybe connectivity security which is how the customer connects to you via the Internet, and I guess an analogy would be we have telephone systems, automated telephone systems that we use that customers can call in and actually pick

up their account balances or perhaps even do exchanges and trades.

Well, they could connect to us via a cell

phone. They could connect to us via a secured phone line, and with that kind of connectivity, in a sense we can't prevent them from connecting with us by a cell phone. However, we can use disclosures to educate them and to actually talk to them about the way in which they might connect up with us.

The same way with the Internet. We can actually use disclosure to talk to our customers about browser encryption, what is 40 bit encryption, what is 128 bit encryption, and in fact with financial data and information, our customers are very interested in learning from us how we connect with them and what kind of security measures we use.

And in fact disclosures I think and the use of educational disclosures are very, very important in this area.

MR. MEDINE: I think it would be very useful to again hear her the committee's views on this issue of transmission security and the obligation on the part of the web site to provide a security method of transmission. Is it a notice and choice situation for the consumer as to whether they choose to do business

with sites that don't provide transmission security?

Again either your thoughts or committee thoughts in general would be very helpful on the issue even on

route what are the responsibilities of the parties.

Lance?

MR. LANCE HOFFMAN: Lance Hoffman. I think even before we get to transmission security in those in some sense technical details, I'm taken a lot by what my fellow committee members have said, and I want to extend it. We have on a number of web sites but certainly not all of them privacy statements already. It may be there should be a security statement as well, and I'll get to that more in a moment because I can see this sort of akin to the ingredient label.

You get an ingredient label on food or on vitamins or things like that. You don't have to -- you can choose. You the consumer can choose exactly what you want, and if it's simple enough it may actually be useful. It has to be simple because I have found teaching computer security for 25 years, utility trumps security every time, okay?

Given that, what can you get it down to? Well, there are only a few things. One is people. We have so many people doing security or so many people per -- for the size of our business per a hundred or a thousand

customers or whatever it is.

The next thing is audit there is no way you can say we're doing 128 bit encryption or this or that or

anything else that is not going to confuse people more than it's worth I think. Much better off saying, Last time we were audited by so and so was on this date and here's the URL to the executive summary or something like that.

So there's people, audit, and the third thing is liability. If you don't like this, here's your recourse. That simple, that kind of statement on what's going on in security doesn't bind you, doesn't tie you up to a given security architect which is going to change all the time, does address indirectly raising the standards of both what security has done and who's going to do it.

Do you have any idea what the average tenure is of a security officer in an installation? Last time I looked several years ago it was three months. That's the career path. So I mean we've got problems here. I think a simple label might do more than anything else. To put in standards is pretty premature at this point.

MR. MEDINE: Stewart?

MR. BAKER: That was great, so you've got the auditors, the computer security guys and the lawyers all

hired in one speech, and I especially like the airline analogy. I expect it to be told many times now, At the recommendation of the FTC please put down your reading

materials for an important message. I think the internal plan idea has a lot of promise, but it does separate the I'm too dumb to live from people who have thought about it and provides for some flexibility.

And I suppose if you have a disclosure of some elements of it given the FTC's deceptive practice jurisdiction, I think it still leaves us with a question of, Well, what do you do if it isn't good enough or how do you decide it isn't good enough. I don't think the idea of going in after there's been a problem and then finding the plan inadequate is a good one.

All patents are obvious after the fact, and all security's inadequate after it's failed so that's probably not the right way to approach it, and again I think it's very hard to leave people responsible for the consequences to consumers.

I have -- I'm carrying around this device that the state of Virginia gave me that discloses the best way to steal my identity. It gives my Social Security number to anybody who looks at it, and then you just have to find out my mother's maiden name which isn't all that hard and you're done.

MR. MEDINE: Again for the record that was your driver's license.

MR. BAKER: Yes. Does this mean Virginia is

liable for having disclosed this private information about me or have they now made it public?

So I think that is a problem, and I think also the idea that we can say, Well, dummy, you didn't follow the CERT advisories. I'm willing to bet there's nobody in this room who has all of the CERT advisories accounted for in his machine with the possible exception of I guess Tom.

MR. WADLOW: Thank you.

MR. BAKER: That's a very expensive proposition, and I think trying to set a minimum standard is just not going to work for us.

MR. MEDINE: Rick?

MR. LANE: I would just like to echo this. Security I think is a process, and how you go about it depends on what the needs are, but also getting to best practices, we held The Partnership for Critical Infrastructure at the Chamber last week. We had over 120 corporations talking about how we protect the nation's infrastructure, and it's not just physical but network security and it was kind of in addition to what was going on at the White House.

The biggest problem in terming best practices was the sharing of information and the antitrust laws and FOIA. So there are current laws in place that

hinder the ability of an AOL to talk to a Yahoo about security, so I mean there are some issues out there that need to be addressed on a broader -- before we even get to the best practices, can we even share best practices or is that a violation of antitrust?

MR. MEDINE: Let me step into my role as an FTC official, not on the competition side, but I want to just note the fact that the Commission gave the Direct Marketing Association an opinion that they could require as a condition of membership adherence to certain privacy practices.

We are very willing to entertain that possibility elsewhere and would be happy to engage in dialogue and have discussions and not let notions or undue fears of antitrust liability interfere with good efforts.

I'm not going to say that that's going to cover the whole territory, but it's worth I think a dialogue so we see where the lines are drawn.

MR. LANE: Just to continue on the transmission side and get back to the wireless issue, I mean I have a digital phone here that was secure three months ago that

is no longer secure. If I make a trade over that or whatever I dial into has a potential of being tapped into, recorded and used by somebody else.

Is that the fault of QualComm who makes the digital phone? Is it the fault of the end person or the end company I'm going to who for whatever reason can't stop or prohibit me from using my digital phone, or is it my fault for not knowing any better?

And if we try to legislate that, it's the business's fault for a consumer not knowing any better we get into a really dangerous territory.

MR. MEDINE: We have a critical infrastructure commissioner formerly. Mary?

MS. CULNAN: Mary Culnan, but that's not what I'm going to talk about. We did address, did raise the issue of the antitrust information sharing issues in our report so hopefully something will be done about that.

But I want to go back to the -- I agree with the point that's been made that security is a process and it's very context driven and it changes and all this kind of stuff, but in the financial world there is an analogy that might help us. If you want to invest in a publicly held company, you don't have to go in and you can't go in and look at how they do business and how they keep their books by themselves.

But if you get their annual report and open to the front page, there's a statement with standard language from the public accounting firm that has

audited them saying they adhere to Generally Accepted Accounting Principles, and that doesn't say they implement all the CERT advisories.

But it says for their situation, they play by the rules, and you can have some confidence that it's okay to go ahead and do business with this company, that they haven't cooked their books.

I think that might be a good analogy. It's an easy to understand disclosure once people have learned what it means, and it provides a way to have a sliding scale. The only issue is who does the audit and who provides the notice in a way that's fair to small businesses and big companies since doing an audit is very expensive, and Larry left the room, and in a way that's not scoopable, right.

MR. MEDINE: Right. Ted?

MR. WHAM: I don' know how Mary got on the list before me because she stole one of my points here much to my chagrin, but very similarly, it's the UL for auditing rights or it's the Underwriters Laboratories. There's a set of rules that come in to there, and you can simply say, I followed the set of rules or I didn't

follow the set of rules.

I was reading an annual report on the way here for an investment that I've had for about a year and a

half that has just done terribly. I'm almost holding the investment out of morbid delight anymore to see how much worse it will get and whether I come back up, and I was going through and looking at the report, right, and there's the blather from the chairman, right?

You never read what he says. Who cares what he or she says. It's the stuff which are coming down into the actual financials itself, and I can have confidence that there's something there even though I have no idea how they're actually doing the audit because there's somebody who does have some idea of what an appropriate set of standards is who's come through and said, Yes, they've played by the rules.

Auditing was invented by Pacioli I believe back in the 1500s, and yet they find ways to set standards and those standards change. For us to say that we can't set standards is I think to let ourselves off the hook far too easily, that it is possible. The only question in my mind is what is the appropriate body to set those standards and what are the mechanisms for those standards to resolve overtime and things progress and become available for them.

Another point was brought up on disclosure information. I'm 110 percent in agreement with what Lorrie was saying, with what Deirdre has mentioned. The

average consumer is not going to be able to care, know what the difference between 128 and 40 bit encryption is nor are we ever going to successfully teach them what that is.

I think that instead if we can point to a third-party and say, You met the standard, you did not meet the standard, that's going to be a much more effective way of doing that.

The final thing is assessing costs and appropriateness of measures. There's two different ways I think someone earlier brought this up, that there's the cost to the organization if they disclose the information, and there's the cost to the consumer if they disclose the information.

I think market forces will take care of the cost of the organization. The organization will implement appropriate security measures to make certain that they're trying to protect that asset to whatever value it is to them. If it isn't very valuable then they won't spend much money on it, conversely if it is.

The issue is if it's more valuable to the consumer, the identity theft example was brought up, and

again I'm going to agree very strongly and steal Deirdre's ideas here, this is a market failure. There is not a market incentive that is appropriate enough to

take care of the organizations around this table to make certain that they value the data to the same degree necessarily that the customer does.

And that's why you have governments. That's the province of legislation to put that in there because if left just to industry, we're going to act rationally and value it based upon our own needs around those things including the risks of PR and so forth if that information is disclosed.

To be able to determine what the appropriate security is, however, for that information, that means you need to know what the value of that information is to the consumer, and I don't think I can succeed as a business of having a security implementation for this record which is different from this record.

I don't think I can do that, which again ties down to a premise that I hold very strongly, and that is that I think that for any given class of data or data element there is a security threshold that you have to hit, and it's very black and white, did you hit it, did you not hit it, is it, you know, medical information that you can't share or is it financial information that

you can't share under any information or is it adverse information that isn't as bad if you share it, et cetera.

And there has to be some way of valuing those data costs to the consumer to hold industry then responsible.

MR. MEDINE: By the way, just to make it clear, we do pay attention to and take seriously what our chairman says at the FTC. Dan Jaye.

MR. JAYE: Dan Jaye. A couple points related to the security management and insurance process. I am very concerned about audit being the only solution for the smaller companies, albeit there may be -- there may arise a set of outsource services that allow smaller companies to have all the security protections of a larger company because they get the economies of scale of using an outsource service, although that introduces another bunch of issues in that you have to trust the outsource service which is now holding customer data on behalf of lots of different companies, so there's sort of a little bit of a catch 22 that you have to work through.

But I go back to my prior life in the financial services industry and there certainly are when we deal with sensitive data a variety of techniques that can be

used that I think can credibly create assurance of security. I remember being bonded as an employee of a company that had sensitive financial information and

having to have my fingerprints taken and actually wondering as an employee the loss of anonymity, that all of a sudden it was public record, that I had my fingerprints in some database somewhere, but -- which does bring up the issue of employee privacy and right of data, but I do think that there's certainly a clear high watermark.

There's privacy audits and, sorry, data security audits that I have been in in my prior life and current life, and I do think that once again it is possible for accounting firms and entities to issue guidelines such that in a privacy policy you can say, We have been reviewed by such and such and they've -- for a copy of their opinion or to reference the summary of their opinion, you can reach that.

My concern is as we look at the sensitivity of different types of data that we still don't create an impractical market for the smaller entrepreneurial start ups and innovators to enter and compete because they can't afford to have five out of the six first employees be data security and privacy compliance officers.

MR. MEDINE: You touched on the employee issue,

and again if people would like to address the issue of security vis-a-vis your own employees and access controls and so forth and whether there are clear

standards there or not as compared to general technology standards, that might be helpful.

Frank?

MR. TORRES: Frank Torres, Consumers Union. I think in getting to that point a little bit, clearly we need to develop mechanisms so that the smaller companies who are doing business online aren't at a competitive disadvantage when it comes to security. I mean, there are small restaurants that still have to comply with the health code and still get inspected.

Maybe we need to think of something to help out the small businesses in this regard. I was happy to hear Ted's comments and others that people do think that there can be some minimal standards that are developed to provide the consumer with some assurances because after all, isn't that what we're about, and that is to -- what can we do as far as security goes?

I think it's one issue that we all agree on that something needs to be done, so that the consumers using the web have confidence that the security's protected, and I think that we need to exercise some caution when -- in thinking about if I do trades online, am I

assuming the risk or is it -- or can I depend upon the company with whom I'm conducting these trades that they're doing what they need to do?

Because if we've got a bunch of consumers that all of a sudden lose the money because of a security breach and the response from the business community is, Well, you should have read our statement, it's going to be a strong disincentive for people to offer good words of advice to consumers saying, Well, gee continue to doing business online as opposed to, Well, there's nothing that you've got that you can latch on to to provide you with some confidence when you do do business online.

So I think we need to exercise some of that to secure data.

MR. MEDINE: Thanks. Andrew?

MR. SHEN: Andrew Shen. I think I share the same skepticism of a lot of the earlier speakers about notice and choice. I have some of that same skepticism to all sorts of privacy practices, but security especially. I think a lot of the terms and technologies ought there, even the little browser window locks, are still beyond a lot of people.

And on a second sort of larger point, I think it's really interesting that so far in the realm of

security, we've talked a lot about dispute resolution, auditing. We didn't extend any of the same topics when we were talking about access because wherever we draw

the line of access, what is proper access, what is reasonable access, wherever it may be, there still needs to be some way to verify whether it's through TRUSTe, PricewaterhouseCoopers, FTC, that those companies are actually providing access to all the information that is there.

MR. MEDINE: Thanks. Dan Geer?

MR. GEER: Yes. Dan Geer, @Stake. On the security front, I assume that this is common knowledge, but if it isn't I would be remiss in not saying it. For all of you who don't deal in that arena regularly, by far the greatest threats to any business are internal and not external by far, and so businesses, if they are not themselves too dumb to live, already have a considerable incentive for data integrity and the like on an internal basis.

And I suspect that most of the conversation today has not dealt with that because in some sense it solves itself. Either you pay attention to your internal data or your trade secrets walk or whatever it might be. I mean, there are serious incentives there. There's no argument. I think those of you who use the

phrase market failure, and I'm not an economist so it's possible that I misunderstand it, but there's no market failure in terms of protecting yourself on the internal

side because it's well understood in the regulated industries, which tend to be the ones, by the way, that collect the most data because most of the time they are the ones required to collect the most data.

With that being said, I'm not myself all together certain that we have had enough market trial to know that we have had a market failure in the consumer space. In the field I'm working in now, as far as I can tell for Internet start ups in particular, first mover advantage is so substantial that anything you do that loses your first mover advantage is as close to suicide as it can be.

And in particular having any kind of failure that costs you the one thing that you trade your -- on IPO day you trade in your reputation capital for money, that's what you do, and anything that costs you your reputation capital, whether it's that you can't keep your servers up, I don't want to pick on EBay, but you get the idea, or that you put too many credit card numbers in the same place, CDU -- those kind of things which take -- CD Universe, right, those kinds of things which take the reputation capital that you are amassing

which is the only value you have, of course prior to revenue, those things I would argue are such a strong incentive that the only thing that keeps people from

paying attention are the same things that keep them from paying attention to anything else that doesn't -- doesn't lead them to getting out the door as fast as possible.

I don't think, in other words, that we've had a sufficient market test to declare a market failure even though I would not know how to explain most of what I do to most of the people I do it with, and so there's no argument that this stuff is complex, particularly at the edge where you're talking about protecting yourself against the unseen villain kind of thing, but don't confuse that with the absence of incentive.

MR. MEDINE: With regard -- let me just follow up.

MR. WHAM: I'm going to try to intercept one quick comment. I'm going to through a market failure out there and enforcement failure, in my opinion I believe it was XXXXXX, correct me if I'm wrong somebody here, please, that was identified and sanctioned by the FTC for deceptive trade practices where they said they selected

(GROUP OF SPEAKERS:) GeoCities.

MR. WHAM: GeoCities, thank you. The day after that enforcement action came out, if I'm not incorrect, the IPO kept getting enormous explosive, about five X

times their initial offering. The cost of some of this information are not borne by the market. There are costs to the consumer in many cases, and I think it's very risky to be dependent completely on the market.

MR. GEER: Well taken. I don't want to debate you personally, but my actual training is as a statistician, and one outlier does not a trend make.

MR. MEDINE: Can I go back to your point about internal threats? Can you -- is it possible to articulate a minimum standard of care with regard to internal threats, or does that also fall under reasonableness?

MR. GEER: Sure, speaking as someone who has tried to sell security partners for better than a decade, there are only two people who are willing customers. That is someone who has just been embarrassed in public and someone who's facing a management audit. You can wave now. Those are the only two people -- that's the only two people who are ready customers that think that they want to buy.

Now, in terms of where the threats are, by and large the threats in a large -- in a corporation of

internal -- internal misuse represent the misuse of legitimate authority. It's not a question of whether this person is who they said they were or whether they

actually had authority. It's misuse of legitimate authority. That tends not to have a technical solution, but it tends to have a process solution back to this point of technique versus process.

MR. MEDINE: Deirdre?

MS. MULLIGAN: Deirdre Mulligan. I wanted to talk a little bit -- you were talking about cell phone connection. How do you deal with client side or individual decisions and the security risks that they may pose? And you have that both if you have an employee who's trying to dial in or use a remote device to access information, how do you deal with the risks that that poses because they're not on site but also from the consumer perspective?

And I agree with you that it's hard to sometimes derail those risks without some costs, but I do think -- I want to get a little personal CDT experience. We sometimes run different kinds of petitions and things where we ask people if they want to join.

And sometimes in order to participate, they give sensitive data. We had one where we were allowing individuals to, for example -- we were assisting them in

opting out of different things, some of which might require financial account identifiers because they were for banks, some of which required Social Security

numbers, and we had both a fairly high level secure server where we were handling things, but we also found out that there were individuals who were back dooring into the cue and coming in through on an insecure page.

And I went and I made a decision despite the fact that I could have told people that you're putting yourself at risk, institutionally I'm not willing to let people who I don't think can assess the risk make that decision, so what I did instead was they had to download the form, print it out and fill it out manually.

Now, I got a lot of people calling me and saying, Hey, I want to be able to fill this in online. And I said, Well, look, you're behind a firewall, you can't get to my secure page, there's a risk of you putting this data and transmitting it over the Internet insecurely and schedule, and that's why I won't let you do this and I understand you're willing to take this risk, but institutionally I don't want to be inviting you take that risk and so I'm going to force you to do it this way.

And you can make that decision as a business to help direct people to better security choices. I

realize that there are downsides. Sometimes consumers get frustrated and I have had that experience, but I do think as somebody who was in a better position to assess

the risk that I also take on a responsibility to educate people about those risks and help direct.

MR. MEDINE: Thanks. Greg?

MR. MILLER: Greg Miller, MedicaLogic. As a side bar, I would move the Commission to consider striking the errant reference to XXXXXX on the record since it is a public record, and everyone is extremely sensitive now about being blamed for things that they didn't do.

MR. WHAM: I think that's an excellent idea.

MR. MILLER: Secondly, with regard to this whole notion of standards, I think the discussion has been moving this way so it may be redundant to just come out and say it, but it seems to me that we need to move to standards of care as opposed to standards of technology or standards of practice.

The problem that we have, and I too referring to Rick's comment earlier, was at the Critical Infrastructure Partnership Summit, and one of the things we were talking about is that liability will come and, Stewart, it's going to happen, and the problem is this. It's going to be standards of care.

At what point does the mom and pop shop who's decided to take their silk flower business and put it online, calls up Dell, orders their first NT server

ever, is totally jazzed and excited about their new DSL connection and, Look, Ma, I can have a phone conversation while being on the computer and this is so cool I'll never shut it off -- how many of those of us out there with DSL connections are leaving our machines on for hours or days at a time and have no idea or knowledge that we currently are parking DEOS code for another denial of service attack on the net because of all of these Window's machines out there on the net with DSL connections.

And you know what? I've got my best friend who works, and MedicaLogic has that, and he doesn't even know what to look for. He wouldn't even know where to start. The first thing he did was he pulled the plug on his DSL collection because he suddenly panicked.

He was reading USAToday, and they say, Hey, liability and negligence is coming, and I think we're well served here to think about you don't know what you don't know, and maybe we should be thinking of standards of care and let other bodies emerge to help understand what the technical aspects of that are, but what's a standard of care for a small shop since small business

runs America?

MR. MEDINE: Good question. Dan?

MR. SCHUTZER: Talking about this standards

stuff and audit and so forth, and I guess it may be strange, but I think you really ought to think about moving in that direction, kind of a tiered kind of service.

I belong to one of the most heavily regulated industries because of the sensitivity of the kinds of data and service we have, so we have internal audits, external audits, and everything else, and it's a cost of doing business I might say, and of course in the web now people recognize that's fuzzy so you may not be a bank, but if you're acting like a bank, you look like a bank, smell like one, you're holding the financial information, providing financial advice, you're offering some kind of payment service, then you probably should be subjected to the same kind of regulation I am.

But on the other hand, let's say I as a bank or you as a company want to go into some other kind of service, let's say I want to throw up some kind of bulletin board service where people can sit around and chat about advice in different sectors and so forth, buying, whatever, then I think -- and I make it clear that all I'm doing is providing a service where people

23 can come and chat and talk and I'm openly not assigning

24 any kind of security officers or any kind of audit

25 processes to this and no security and I'm not going to

be held liable for it, that might be a service that should be answering to a different level of standards perhaps even without order because now I'm trying to do a different kind of business with different kind of data, different kind of sensitivity.

So I'm trying -- sometime in the future we may find that that kind of business exposes us to a different kind of risk, you get concerned and people will then talk at that kind of a business to for a different level of protection, and that seems to be the way we work in the U.S., but when we can recognize that there's a concern where people are at risk, we then put down certain kinds of standards and orders.

But for a small business to get up and get started or even a large business in this other sector, they should be allowed to tell what you they have in disclosure, and it may not be the same level of standard to require audits to the same kind of degree or at all to what you might require in a financial or medical kind of an industry.

MR. MEDINE: Andrew, was your -- John?

MR. KAMP: Yes, I would just like to make a

small--

MR. MEDINE: Can you identify yourself?

MR. KAMP: John Kamp from the AAAA. I want to

associate myself with the notion here that we're talking about a very important reputational value of doing things in secure ways, and in fact my remembrance of the effect of the GeoCities case is very different than Ted's.

I remember it having a very serious effect on the GeoCities, the value of GeoCities, and I think we must remember that in these cases when the FTC or another official body does something that calls into question the security or other reputational value of a company, it has a tremendous effect, and that's a positive thing. That's a positive thing for the value of this agency operating in this space, and in no way do I want to minimize that here today.

MR. MEDINE: Thank you. Jerry.

MR. CERASALE: Jerry Cerasale, DMA. I wanted to agree with Mr. Miller that I think we have to look at some standard of care. From the point of view of security and the DMA guidelines that we have, you have to train people, make sure you have access, certain things of that sort, and I think that's a standard that we say.

I also think however that we have to be careful here with security, and I think that what we're thinking about now is security of the information that we

collect. I don't think it's security of the server that's only been used to go bombard Yahoo or something of that sort. It what we're charged to look at. It's just information that we have.

It's important, it is -- the reputation that John just talked about is very important, and word gets around in this new system of ECommerce.

This Christmas time when there were press stories concerning -- and the FTC knows lots about this -- certain web sites being unable to produce goods at times promised or within the proper rules, and they're doing some looks at that, we found a significant drop off in orders that unfortunately spilled over into the catalog area two weeks before Christmas time.

And so a big boom in our business and then suddenly a stop or virtually a stop right before Christmas two weeks before because of the press reports, so reputation is very important, and I also think that as we go into having -- so it's important for businesses to do that on the -- so they want to make sure they have security.

And the other is I don't think we're ever going

to amiss liability, and I think that from that score as you look at it, liability potential is going to be the major force here to get -- to make sure that ECommerce

businesses take care of the information we have on individuals which is I think what we were talking -- what we're charged with looking at here. Thank.

MR. MEDINE: Thanks. Tom.

MR. WADLOW: A couple of things here.

MR. MEDINE: Identify yourself.

MR. WADLOW: Tom Wadlow, Pilot Network Services. The gentleman over here in the corner, I apologize for not knowing your name, had spoken awhile back about outsourcing security and allowing the small companies to compete on the same basis as larger ones.

I want to thank him because he essentially described my business plan in a nutshell, and we've been doing that for quite awhile. Some interesting experiences to share about that that I think are relevant, some of the things that we do, some of the practices that we follow are in fact that we do have ourselves audited on a regular basis by outside agencies, and I mean mean nasty audits so they really come out good.

We want to get pain so we make sure we're doing it right. We do that. We provide summaries of those to

our customers and to our prospects, and that -- and we also do background checks, and we were asking about that fairly hefty within the limits of the law, of course

background checks on everybody that we hire from the receptionists all the way up to the security officers.

And that has served as very well in terms of getting customers, but it's a very interesting thing to go back to something that Dr. Geer was saying which is that those same customers who work really hard to make sure that we live up to their expectations from a security standpoint are also the same ones that don't want to wait an extra day for example for a code review of their CGI code because it would take too long and it would keep the web site from getting online.

And for those of you who aren't aware of it, any time you've ever seen graffiti on a web site or a web site broken into, there's an excellent chance it came through a hole in their CGI code so it's a matter of that people want this at least in principle, but in fact in practice they are very reluctant to put up with some of the demands that getting those things take.

The other thing I wanted to mention and also talk about something that Dan said is that the fundamental operating principle that we work under is that anybody can break into anything if you have

sufficient skill, motivation and opportunity, and

therefore our goals in everything that we do are to

raise the skill bar very high.

We know you can never max it out. There's always going to be someone that has more skill, but you want to reduce it, require a very, very high level of motivation from the hacker and give them as little opportunity as possible to do that.

The reason why I'm referring to Dan's comment is that if you think about the people that have the highest skill, the highest motivation, the highest opportunity they are in fact the people that work in your company, and those insiders are really, absolutely the most dangerous people around, and that's something that really has to be checked, and it really has to be made certain whenever you think about security for any reason.

MR. MEDINE: Thank you. Given the hour why don't we take a 15-minute break and come back and discuss the security three and then go forward into our wrap up. Thanks.

(A brief recess was taken.)

MR. MEDINE: I understand Ron Plesser would like to make a request.

MR. PLESSER: Out of courtesy to our West Coast

colleagues and out of courtesy to some of us that have work to do at the end of a Friday, I would wonder if the Chair would consider having the committee assignment

discussion now so that we can get that resolved for people who have to leave, and then you can continue on with the public comment.

But it would be helpful if we could do it that way.

MR. MEDINE: Is the committee amenable to shifting things and moving on to assignments? I'm seeing lots of nods. I'll say ayes as opposed to nays and the ayes have it.

(Discussion off the record.)

MS. MULLIGAN: As long as everyone doesn't run out before the public comments happen.

MR. MEDINE: I'll tell you what, let's see if there's any expression in interest in public comment, so we can -- is there anybody present from the public who would like to make a comment? This is it? Then we certainly don't want to shortchange public comment, but I think we've given it sufficient opportunity.

Okay. Then moving on to the suggestion at hand, just to reiterate my comments this morning, what we would suggest to the committee is that it move into the next stage which is the committee has done a suburb job

fleshing out the issues and the outlines and the discussion today, and we would recommend the committee move on to developing specific options with regard to

access and security, and that subgroups be formed to create those options, that those options be circulated to the committee through us and put on the web site as the outlines were for this session, deadline for submission of Friday, March 24 which would give us a chance to have that up on the web site and give the committee a week before the next meeting which is March 31 starting at eight a.m. as a courtesy to our West Coast visitors to review it.

So option papers, March 24, and then we can spend the next meeting on the 31st discussing the variety of options that have emerged.

I guess we are -- your designated federal officer is prepared to suggest some subcommittees and we in light of our experience last time have taken a stand of putting together some subcommittees and subcommittee assignments. If there are others who would rather proceed a different way, it's your committee, but once again we're prepared to serve, if that's the committee's pleasure.

MS. SWIFT: Go for it.

MR. CERASALE: Please serve.

MR. LANE: Wait, wait, hold it. I have a question.

MR. MEDINE: Could you identify yourself?

MR. LANE: Rick Lane. If you are not happy with the pre assigned committees, I would just like to say that you have -- we should have the option to pick the committees that we are interested in and let you know by such and such date, whatever date is determined. That way everyone feels that they're in the appropriate place.

MR. WHAM: My only concern about that is --

MR. MEDINE: Identify yourself.

MR. WHAM: This is Ted Wham -- that my fellow committee members might want to remove me.

MR. LANE: You can't remove someone else. You can only change your own personal identifiable information.

MR. MEDINE: Here's our goal here. We've tried to form these sub groups to have a range of background and experience to bring to the table. I guess what I would propose those who wish to change perhaps could contact the committee, FTC staff serving the committee within the next two or three days to clarify any changes and so that the groups can get working; is that --

MR. LANE: By close of business Monday?

MR. MEDINE: Okay. Jonathan?

MR. JONATHAN SMITH: Jonathan Smith. I just have a procedural question. Will these groups be the

groups that will stay in place until the final report is due May 15? That is, if we are to produce options this will probably be the end grouping?

MR. MEDINE: You're already thinking further ahead than we are. I think we're amenable to going either way on that. Do committee members have feelings one way or the another on the that? Identify yourself.

MR. PLESSER: Ron Plesser. Maybe the way to resolve this is to request that mainly you stay where you assign them, but if somebody wants to double up and go on another committee as well, that that's something you can entertain. I would maintain your balance but then allow people to share.

MR. MEDINE: Share some particular expertise in other areas, that might be an useful.

MR. LANE: Well, that doesn't that -- if I'm not -- Rick Lane U.S. Chamber of Commerce. If I'm not interested in being on a committee and I go on and double up and I just don't participate in the other one, is that just kind of de facto I'm taking myself off of that one and going to another one?

MR. MEDINE: Well, I'm sure everyone has lots to

contribute. Why don't we take those up on a case by case basis preferably by the close of business Monday so again we can get the committees working. At least we'll

have an extra week from last time.

MR. PLESSER: Don't forget Art Sackler. He's not here today but I know he wants to participate.

MR. MEDINE: We assigned everybody prior to this meeting, so why don't I run through our proposed sub groups.

If I can have the order of the committee, we are proposing a slightly different organization. We think that the subcommittee format last time was a useful time to develop certain issues, but I think as we move to options, perhaps a slightly different organization might serve better.

So what we would propose, the same number, that is four subgroups access and three security, and at the suggestion I will go through the titles first and then go back and go through the titles and the committee members.

The first under access is degree of access and terms and conditions of access. The second is entities covered.

The third is ability to correct or edit data, and the forth is authentication and technology issues

related to access.

MR. PLESSER: Three was ability to correct

and --

MR. MEDINE: What we would propose is in terms of relating this structure to the structure of the first processes is access one for this session developed a very extensive list of categories of information, and what we would propose is that each of these four groups in its work among other things consider how those range of categories or range of sensitivity of information fits into the work of each of those groups.

That is more or less sensitive information relate to the ability to correct, more or less sensitive information relate to authentication. Again not to say that you won't project that, but we would urge that that range of responsibilities be at least addressed by each of these groups.

So I guess should I move to our proposed assignments and those people want to discuss the structure?

MR. WHAM: Do you have a three for security?

MR. MEDINE: The three for security are, the first are what we call internal or managerial security issues. The second is external or technical security issues, and the third is disclosure assurance and notice

of security.

Again would people like to discuss the sub groups or should I move to assignments, proposed

assignments?

MR. WHAM: On discussing the sub groups --

MR. MEDINE: Again identify yourself.

MR. WHAM: Ted Wham with Excite@Home. I think even the court reporter knows who I am.

On the security assignments there was a lot of discussion about rulemaking and hitting a certain standard of procedure and appropriateness of care and so forth. I don't know if that's going to be addressable very well in the three groups that you've gotten.

MR. MEDINE: I guess: Why wouldn't it be?

MR. WHAM: I would look at that in terms of you've got disclosure as an area, what you say about it, but I think you need to have some level of do we want to have a bright line rule, do we want to have minimum standards, do we want to have ones that are by third-party, do we want to have government oversight, do we want to create an independent industry report.

I'm not sure if I understand where that fits very well within that scribe.

MR. MEDINE: I guess I would propose that they could fit into either -- to any of the groups but

particularly the first two groups, that is, for instance, the second group would be external security issues. Those could be addressed through standards,

through audits, through any number of means that we're discussing.

MR. WHAM: The very fact that it fits in multiple groups seems odd.

MS. CRANOR: This is Lorrie Cranor. I would suggest there be only one security group that covers all of this, especially given last time that the three security groups spent a lot of time talking to each other, and they were really held to the same thing essentially.

MR. MEDINE: Do people think that's a practical way to proceed, a more efficient way to proceed than last time? I'm seeing some nods.

MR. TORRES: This is Frank Torres. Are you saying combine A, B and C into just the one so we have just the security?

MR. MEDINE: The three security groups is the proposal.

MS. MULLIGAN: I think it would be useful to do so.

MR. MEDINE: Identify self --

MS. MULLIGAN: I but she knows who I am too.

I'm sitting right next to her.

But I think the way that you wrote this out I don't think for me reflects the tone of the focus of the

discussion. The things that seem to come out of the discussion were there was a notion that came out that seems to be very important of auditing and testing, so how do you assure that what you're doing works, a notion of how you establish what it is you should be doing which is the standard of care, how do you assess reasonableness, and then the question of whether or not there are sufficient incentives.

I thought it was very telling that Mr. Geer talked about you weren't sure there was a market failure, but then he said that the only people who really come in dying to have security are people who just had a big public humiliation or people who are highly regulated to me which indicates that there may be a failure.

I'm not sure, but so when I think about technical and managerial, those have to apply both to internal and external. I just wouldn't break them in that way, but I think one group is fine, but I would prefer to have people focus on three different subjects rather than these three subjects.

MR. MEDINE: I think that would certainly be an

appropriate thing for the group to do among themselves is to allocate responsibility for those issues and other issues, and again remember that the goal here is not a

consensus. If anyone has a single view, that ought to be presented as well, and again I will just make it clear, that the subgroup's role is simply to report back to the larger group for consideration.

These are just proposals for options to be considered by the larger group at the next public meeting. So it sounds like -- there seems to be a consensus to have the security three groups merged into one. No, we're having an objection.

MR. KAMP: It was another question.

MR. MEDINE: Yes.

MR. KAMP: I've resolved that and --

MR. MEDINE: Okay. Resolved. Does anybody have any objection to merging? Again it seems as though there's a consensus to merge three in effect. I think that addresses some earlier question is that people had overlapping expertise, and this would create a greater synergy among the levels of expertise in the group, I think that sounds like a reasonable proposal.

John? John Kamp.

MR. KAMP: John Kamp from the AAAA. Mine is a question, and it probably reflects the fact that I work

inside the Beltway, but when I see options, I think what options are there other than policy options, and I thought it might be useful for you at least to discuss

what you were thinking about inside that so that I could get a sense of what our reports would look like.

MR. MEDINE: This is -- the committee has total discretion to submit whatever options it thinks appropriate, whether they're technical options, policy options, options to do nothing, options to do lots of things.

I mean, that's what exactly we're looking to the committee to give us feedback on. Obviously we have an immediate interest in understanding these issues particularly in the context of the web survey that's going on this month, but unless -- I'm not sure if I'm answering your question, but I think that's for the groups to decide, what kind of options they want to lay out and which will benefit the Commission.

Deirdre?

MS. MULLIGAN: Deirdre Mulligan. I have one more. On the access of sub groups, I don't feel like -- and other people of course disagree vehemently if you need to, but the entities subgroup, I feel like we kind of went through that issue very quickly during the general meeting, and I don't know that it would warrant

a full separate sub group.

It seemed to be pretty tightly intertwined into other discussions, and I'm wondering if other people

feel like there needs to be a separate sub topic on the topic of entities.

I think as Lorrie talked about earlier if you're talking about sharing data, absolutely, but when you're talking about access and security I'm not so sure.

MR. KAMP: And John Kamp. Just to sort of respond to that, the way I understand then which I may be again incorrect is that it's the third-party transfer problem. It's the multiple entities that might be involved, and given that I don't think I have Deirdre's problem, but the way Deirdre expresses it I may agree with her.

MR. WHAM: What is it that you have a problem with?

MR. MEDINE: Being from inside the Beltway comment.

MR. WHAM: If you want like me to come closer to tease you personally I'll be more than happy to do it.

MR. JAYE: Don't take this as a volunteer for the entities sub subcommittee, but I do think that there are a few issues there that we didn't talk about today

that probably should be addressed here.

One is onward transfer and where this data control is inside. We about editing at the source,

editing at the target. One issue we didn't talk about today though specifically was actually the issue of jurisdiction, and I know that it comes into a scope issue, but obviously that can be interpreted as sort of from a federal perspective.

But also there's the concern of what about onward transfer to a jurisdiction where the FTC might not have direct recourse under Fair Trade Practices, so it's kind of the inverse of the what the EU has been doing, but I think there are a couple issues like that -- they may only take one minute to address, but there's probably a couple things there that we need to at least check mark.

MR. MEDINE: Okay. Okay.

MR. PLESSER: Maybe if you put entities and sectors in the second one so that we were -- had some of the sensitive sector kind of, Do we deal with everything one way or separate sectors in terms of access, obviously some overlap, but I think that would then give much more meat to the second committee and then splitting it.

MR. MEDINE: We can take comment on that. Even

if we did that, I would urge the other groups to still consider the sensitivity and the range of issues that access one has laid out, but I don't know if that helps

people, but I think certainly the conception about the entities relates to onward transfer sharing, joint efforts, joint ventures, joint marketing, all the various business relationships that data can be subject to.

MR. GAVIS: As a members of the entity group, I think Deborah and I are the only two people here. We had a hard time getting our arms around this, and I kind of second the thought that maybe we want to roll it into maybe even number three, the ability to correct, ability to reach inside the organization and correct from whatever entity it's shared with.

MR. MEDINE: I'm seeing some nods. Are people amenable to merging the entities in the corrections group? You don't have to identify yourself.

MR. WHAM: Actually I have a concern here that this is a relatively large issue that we didn't spend any time talking on, but there's a lot there. If it isn't for access, it isn't for security per se but it is for transfer data to third parties whether that's -- explicitly out there whether it's EBay or whatever it is.

If that's within the mandate of this group, then I for one would participate on a committee like that because I think there's all sorts of detailed

information. Do we have a right to transfer it to a joint venture partner? Do we have a right to transfer to a wholly owned subsidiary? What if we owned 49 percent of that subsidiary?

I think that there are questions -- what if it's a marketing partner? We're doing something with Proctor and Gamble.

MR. GAVIS: This is Alex from Fidelity. I would jump in and say I'm not so sure we want to focus on whether we have rights to transfer from one to the other. The issue is whether the information that gets sent along can be accessed by a consumer or customer.

MR. MEDINE: I think that's consistent with the scope of this group, is assuming information is legally transferred, what are the access consequences in the context of how that information is being transferred?

Lance?

MR. LANCE HOFFMAN: Lance Hoffman. I think we're rapidly nose-diving, and I don't want to do that. I don't want to fly at 500 feet when I think in order to plan for next time we have to stay up at least at 20 or 30,000 feet.

I think Deirdre was on the right track when she said, Look, I think what I've been hearing and the discussion of the committee as a whole day was she said,

they could be different, I had them as standard of care, audit and incentives, but they could be other things.

The point is whatever the subcommittees end up being I would like as a committee member to get not direction but a couple bullets, several bullets from the FTC saying, We think what we heard were these, you might want to consider these to focus your discussion, maybe taking Deirdre's as a starting point.

That way as a process point down the road we can roll some of these things into that and we won't have things all over the map.

MR. MEDINE: We're willing to do that, but again I really and truly don't want to constrain your groups' discussion and the scope of the issues that the groups raise.

MR. LANCE HOFFMAN: One of the --

MS. PIERCE: This is Deborah Pierce from EFF. I just wanted to echo what Alex said. When we were going through our outline, we found ourselves really discussing a lot of scope issues, a lot of ability to correct and edit, and I agree with him. I think that an appropriate place to roll this into would be the third

category or even the first category.

MR. MEDINE: Okay.

MR. GAVIS: Alex Gavis from Fidelity. One thing

that I think maybe that I'm hearing is that if we're going to be an effective advisory to the FTC, I think maybe we need more guidance from you as to whether you want us to focus on policy or you want-- whether you want us to focus on sort of our expertise in industries, and to some extent you may have some ideas and you would like to sort of hear what our expertise and various industries so it comes to bear on these subjects as opposed to what from a policy standpoint we might do.

Or on the flip side you might not care as much about that but really want us to think from a policy perspective, what would we do if we were a policy maker, and I think that's sort of the tension that's going on here.

MR. MEDINE: In some ways we're looking for the intersection of the two because we are looking for your expertise in translating what's going on into operational or implementations approaches to access and security, and again the very specific goal is as we survey web sites right now and discover certain practices on those web sites with regard to access and security, are those consistent with Fair Information

Practices?

So it's a little bit of both. I don't think it's a pure policy, and I don't think it's pure

technical, and I think from the security discussions, certainly we learn that there are some array of technical issues that may force the policy in certain directions.

MR. BAKER: Actually I think we know pretty much what the options are on the security side. It's harder on the other side. I was going to ask a similar question about where this is -- what we should be putting together.

We could write the options in about like a 20 minute phone call is my guess; writing the pros and cons is a more substantial effort, and I'm assuming you want that, but I wasn't sure.

MR. MEDINE: No, I think that's a good question and the answer is yes. I mean, what ultimately will benefit the Commission is not so much six different positions as understanding why those six different positions advance Fair Information Practices and considering the costs and benefits of those various approaches.

So I think certainly identifying the options is obviously the starting point, but then beginning to

flesh those out with pros and cons is exactly what we're looking for.

MR. BAKER: One related point to that. Stewart

Baker again. What should we assume is going to happen with the stuff we've been outlining? Obviously it would require a lot of work to be useful. Is that going to -- are we envisioning that that will be a report, and the options will come at the end? Should we just figure we'll do the options and it was a learning experience to produce the outlines? What do you think our final product is here?

MR. MEDINE: Again that's going to be up to the committee. I guess we viewed the exercise of creating the outline largely to inform the discussion about where to head on options, so I think the body of the report ought to be mostly options rather than spending time writing a treatise on the array of infinite possibilities here.

We want to have a relatively practical guide for the Commission on where do we go from here on these two very important issues.

Richard?

MR. PURCELL: Richard Purcell. As a note of encouragement to whatever subgroup each one of us ends up on, I would like to encourage all of us to be

continually thoughtful about this glossary that I think is going to be very important to our work here and for each of the sub groups to try their best to maintain and

to create some level of consensus around definitions for some of these important terms that we're using and that perhaps we might be understanding but perhaps need to be brought forward in our final report in order to further the understanding beyond the committee itself or the Federal Trade Commission and out into the marketplace itself.

MR. MEDINE: I think that will be a very useful part of the report.

Deirdre?

MS. MULLIGAN: Deirdre Mulligan. As the holder of the categories document, I will actually update it to reflect the discussion and recirculate it. I mean, there was a desire to have of transactional data. There were two or three other things, and I did take detailed note, and I will update it and circulate it because I completely agree with Richard's point that a common taxonomy is really important for anything, so I will circulate this early next week.

MR. MEDINE: Great.

MR. LANE: You have the sweeps going on on access and security starting, probably they've already

started or are starting very soon. Yet we in this room haven't come up with an idea of what exactly is proper access and proper security, so how are you running the

sweeps on an issue that we haven't been able to resolve here? So do you already have what the options are and what the best practices should be?

MR. MEDINE: Well, the question has arisen before. What we're trying to do in the sweeps is to gather as much information as we can about what web sites are doing in fact today and then have the work of this group inform the Commission as to whether what is going on today constitutes sufficient self regulation and meets what are considered Fair Information Practices.

So that's our challenge is to get enough information to give this group flexibility in making recommendations that we can then assess against essentially a snapshot of the world that we find today.

MR. LANE: If we had found on the security discussion which was processed and all you're looking at -- and I'm not sure how you're getting at the process, I mean, I don't know if you're calling the CEOs of the different companies and saying, Please detail us your security process and how many people you have -- there's some comments about numbers and audits and

things of that nature.

Is that what the sweeps are doing, or are they just looking at the web site?

MR. MEDINE: They're looking at the web site. And maybe that's an advertisement for our last discussion which is there's a question that I think this group can be very helpful on to the Commission, and that is do you have to disclose or should disclose your security policies, practices? Should you just have good security?

I think informing us on that issue would be extremely helpful, and then we can read the results of the survey in light of what was discussed here.

MR. LANE: Maybe it will help us in formulating our ideas on the security side. What are you looking at for security -- what are you judging and basing your security sweep on?

MR. MEDINE: Well, we're primarily looking at what sites are saying about their security practices, and certainly to the extent that sites use SSL as part of it as well, but we're looking for this group's guidance as to whether security is something you talk about, is security something you have, if you talk about it to what degree do you talk about it?

We are primarily capturing what sites are saying

at least on that principal limited element of SSL doing in this area.

MR. LANE: So you could actually have a very

secure site that doesn't talk about it, but it could be interpreted just by raw numbers that you actually have a secure that or a site that is not telling you about the security, and that -- my concern is that that could be interpreted as an unsecure site even thought it may be the best security of all the sites, even the ones that are disclosing.

MR. MEDINE: That's where this committee can be very helpful to the Commission in evaluating that information for its release to assess the issue again of whether people should be told about security. Part of the issue of security is do consumers have confidence that their information will be kept securely, and part of the consumer's concerns is will their information in fact be kept securely.

So this group's advice and final report will be helpful in evaluating how the Commission should approach the data that emerges on that issue.

MR. CATE: I'm sorry, could you tell us whether Stewart Baker will be a catering his group and if so which group he'll be on?

MR. MEDINE: That would give his group an unfair

advantage. Stewart?

MR. BAKER: This is Stewart Baker. A couple thoughts on this survey. I certainly agree with Rick,

the fact that you have no security statement at all might not mean you know anything about your security so to the extent you're doing this sweep, there shouldn't be an implication as there might be on the privacy side about the lack of a statement is a fall.

But if you're going to do it, some things that might be useful to know is whether, one, is there a security section; second, does it mention particular technologies, SSL's commonly mentioned; does it mention particular security standards to which it is -- that is adheres to; does it mention an audit or an auditing firm that may have checked their security standards; and how long is it?

Those are all useful pieces of data. I don't think it tells you whether there's good security or bad, but it will it us to figure out does it really matter to have a statement like that.

MR. MEDINE: Let me just say that those are obviously the kinds of options that will -- as you predicted would take a short period of time to start spilling out the options, but those are the kinds of options that would be helpful for the Commission to have

along with pros and cons to evaluate what it's learning in the survey.

This will be useful generally but its most

direct and immediate application will be survey interpretation. Jonathan?

MR. JONATHAN SMITH: This is Jonathan Smith. Why don't you just do something pragmatic? Why don't you just do short scans, go and check their --

MR. BAKER: Buy a war dialer?

MR. JONATHAN SMITH: Go for that.

MR. MEDINE: Okay.

MR. RICHARD SMITH: I think I can answer that.

MR. MEDINE: Richard Smith.

MR. RICHARD SMITH: I was just -- Richard Smith. I was just involved in a project for doing a web sweep for E Health Sites, and we faced the same problem, what do you do about security and pretty much just let it -- take a peak at the privacy policy and what we talked about.

So we made no judgment calls about security, and what I kept telling -- when we got started on this, I don't want to do things like short scans because I don't want to go to jail. If you start testing external security that gets into a real fuzzy legal area, so I don't recommend that.

MR. PLESSER: Point of personal --

MR. RICHARD SMITH: Overall what was interesting is we were still able to find security problems. Like

we found a complete database log in information in HTMO comment so it is possible to find security problems without that, but over all --

MR. MEDINE: Ted?

MR. WHAM: That's not good, is it?

MR. RICHARD SMITH: I don't think so, and were taken off two days after our report back out and still not back online again.

MR. MEDINE: Ron?

MR. PLESSER: I thought we were about to get our assignments, and we went down this road so if we could focus back on the assignments.

MR. MEDINE: If that's a motion to --

MR. PLESSER: I blame the Chamber completely.

MR. MEDINE: I take that as a motion --

MR. LANE: We'll bring our coffee the next time.

MR. MEDINE: Hearing no objection we will proceed.

Starting with new access one which is degree of access and terms and conditions of access, we propose Alex Gavis, Deborah Pierce, Steve Cole, James Allen, James Maxson, Jane Swift, Art Sackler and Richard

Purcell.

For the new combined entities and sectors as well as ability to correct or edit the data all combined

into one we propose Richard Bates, David Ellington, Tatiana Gau, Frank Torres, Fred Cate, Dan Jaye, John Kamp, Deirdre Mulligan, Dan Schutzer, Josh Isay, Ron Plesser, Rick Lane, Rob Goldman and Jim Tierney.

For the access three, the new access three authentication and technology issues related to access, Robert Henderson, Richard Smith, Andrew Shen, Ted Wham, Jerry Cerasale and David Hoffman, and the security group which everybody has left, but I'll read it any way because there is some duplication of people, Deirdre Mulligan, Rebecca Whitener, Larry Ponemon, Dan Geer, Lance Hoffman, Andrew Shen, Tom Wadlow, Greg Miller, Jonathan Smith, Stewart Baker, Steve Casey, Mary Culnan, Stewart Baker, Lorrie Cranor, Paula Bruening and Dan Schutzer.

Let me again just reiterate that while this is a large group, its task is only to develop a set of options to report back to the full committee. Because of the public nature of the advisory committee meetings no decisions will be made at the subgroup level, but the subgroup obviously can be very valuable in developing a series of option for the full group to consider.

Why don't you all --

MS. GAU: Tatiana Gau, when you post this on the site as I imagine you will could you be sure to

include a definition as what you see as the objective of the individual sub groups?

MR. MEDINE: We will do our best to do that, yes. If people don't have further discussion on this issue, perhaps we could move very briefly to the last issue which relates to disclosure. Andrew?

MR. SHEN: Andrew Shen. Just a really quick question. Last time around the authentication group had sort of control over the definition glossary or glossary of terms.

Is that going to continue or is that going to be thrown to a new group?

MR. MEDINE: It's up to the group. Dan?

MR. SCHUTZER: I think the spirit of what was said starting with the glossary, and as we all proceed, we can review that and find any additions to this growing glossary, I would recommend we do it that way.

MR. PURCELL: I agree. I wouldn't characterize our effort as controlled, as rather volunteer effort to just start something up.

MR. MEDINE: Dan?

MR. JAYE: What is the mechanism for providing

feedback on the glossary? I'm not sure this is the

right forum to do that. Is that just E mail to the --

to that subcommittee, the authentication subcommittee in

its new form?

MR. MEDINE: I'll leave -- why don't we have the group decide that.

MR. JAYE: For people in another group though?

MR. WHAM: Why don't we give our --

MS. MULLIGAN: Richard, don't you have the master of that?

MR. PURCELL: Yes, I do, but it's also posted on the web site.

MS. MULLIGAN: Can you edit it?

MR. PURCELL: I can certainly edit it.

MS. MULLIGAN: I was forcing him voluntarily.

MR. PURCELL: Keeping clearly in mind that editing invokes a certain level of control, don't hold me too tightly on that, and if you have any dispute over the editing or that control, please be vocal about that as I know that you probably will.

MR. MEDINE: And as the transparency that we have of posting things and having the next meeting as an opportunity to discuss these raise issues.

MR. ALLEN: James Allen. I thank Richard for volunteering to do this, but I think it would be very

useful if it could be published periodically over the next three or four weeks so that we can see that, and I would hope that the FTC would help Richard in doing

that.

MR. MEDINE: Certainly. We'll be happy to either distribute to the group or post on the web site anything you like.

MR. PURCELL: Tell you what we'll do. This is Richard Purcell. I will do my best on Fridays to post an update to the designated federal officer, and I will leave that officer the accountability for having it available on the web site for the general group's access.

MR. MEDINE: I accept that responsibility.

MR. WHAM: Might there be an alternative for that actually to be posted on a Microsoft site updated as you've got the availability to provide a link off the ACOAS site?

MR. MEDINE: Well, I think it's probably more appropriate to be on the advisory committee site, and you can feel free to link to it from anyplace that you would like. I think it's more appropriate to be on our site.

Any other procedural issues before -- if people can stick around a few minutes for those who can, I

would like just briefly discuss the issue that was just raised a moment ago which is people's views about security, which is do you have to talk about the

security you have, or is it enough to have security in the context of Fair Information Practices?

Again that will be as I said before very helpful and informative for the Commission to evaluate the results of our survey matter. Mary? Why don't we just discuss this for 10 or 15 minutes because I know people look boiling.

MS. CULNAN: One thing I took away from the last discussion is that perhaps disclosures about security itself were pretty meaningless, but people want an assurance that's useful and quick to pick up and understand that this is a safe place to do business in across from the medium, et cetera, so I would say that should be the goal of disclosure is to build trust in the medium and to focus on what's the best way to do it?

Is it through a third-party assurance? Is it through some kind of statement? Those would clearly be options for disclosure.

MR. MEDINE: Lance?

MR. LANCE HOFFMAN: There's this ongoing issue in the security community about full disclosures versus security by obscurity, okay? And it's not going to get

solved by this committee either. I think Mary's on the right track when she says people want assurance.

I would harken back and make a minor

modification to what I said earlier, and I'll make it brief in terms of putting out there we're doing something or we're doing this on the security, and I'm taken on your comments about the small initial -- what's the barrier for a small firm starting up and all that.

In essence again very quickly, an ingredient label kind of thing where it says, Here's what we're doing on security, we're devoting X amount of our resources, our revenues or whatever it could be zero. It could be zero. You could hire it out, contract it out for something, you are taking care of the audit.

We have hired so and so, Pricewaterhouse or whomever to do our -- whoever, to do our audit and here's the -- as I was just talking to Stewart in the hallway conversations, here's the standards they're using whatever they are, could be -- whatever they are, and then finally if you will the liability notice or recourse notice, something like that.

Bang, bang, bang, bang that's it, nothing else, that let's people know without burying them -- once you say SSL 95 percent of the world tunes out, you know?

MR. MEDINE: John?

MR. KAMP: Not to respond to that, but John Kamp from the AAAA, and perhaps at the risk of picking up on what might be a sensitive issue, I do think that this

discussion about what security is and the notification of security might underline an issue that some of us in the business community have said for some time, and that is the FTC web sweeps might be better off done after the report from this committee comes in.

And I would ask the Commissioners and the Commission staff to review the record of this to hear some of the conversation we just missed, that just went on.

MR. MEDINE: Thanks.

MR. PONEMON: May I comment on audit? I think when we say audit --

MR. MEDINE: Can you identify yourself?

MR. PONEMON: Larry Ponemon, Pricewaterhouse Coopers. It's a long name, I'm sorry.

But when we think about auditing, there are different types of audits or different types of assurance services. For example one could argue that TRUSTe and BBB online provide a form of assurance, so I think that when we look at the options each one carries a certain degree of comfort and security to the reader of the disclosure but also carries a cost and so we need

to factor that into the equation as well, so....

MR. MEDINE: Again keep in mind as you formulate

options as to what the disclosure -- there are two

issues, one is what should you be adopting and the other is what should you be telling consumers about what you adopted?

Why don't we just go down the line with Frank and then Jim and then Jonathan Richard?

MR. TORRES: My comment is simply disclosure of the site's security sense is a good idea to establish some consumer confidence and I think it can simply be the truth about what a site feels about its security.

Certainly what I've gotten out of some of this discussion is any site that fully guarantees to the consumer that it's 100 percent secure and under no circumstances will your information ever be broached is just an out and out lie.

But a site that says, Listen, we'll protect your information to the best of our ability and should in the unforeseen circumstance happen, here's what we'll do to protect your information, and I think to the extent that those disclosures are truthful, simple, plain English, it actually provides a good feeling sense for consumers and could be very useful in that sense.

MR. MEDINE: Jim.

MR. TIERNEY: Jim Tierney, I had vowed to try to keep quiet, but John invited the Commissioners to review the transcript about the feeling that this group might

have about the timing of these particular sweeps, and at least as one member of this Commission, I'm delighted that the Commission is doing the sweeps, not only that they're doing it but when they're doing it and that this information will be made available to us and that there are indeed difficulties and problems or defects in the Commission's methodology, that we'll still be sitting as a committee and be able to remedy and point to the public there are defects that the FTC has proceeded but I'm delighted it's being done.

MR. KAMP: Let me respond to that. John Kamp. I'm not sure, Jim, if what you said is correct that this committee will have an opportunity to fully review the results of the study before this committee submits its report. That might change my attitude about this a lot, but I don't have any sense that this committee will be able to have any data available to it before this report comes in.

MR. MEDINE: I think that in fact the current thinking is that the Commission would consider the work of the committee in evaluating the results, but that the results would not be circulated to the committee for

review prior to their public release, and I think we know how quickly things make the right public.

And so I think to give the Commission sort of a

full opportunity to consider both and have a full opportunity for reflection, they will both be issued together in a Commission report, but of course that's not to say that the Commission in considering the results may learn some things from this committee's work that may cause it to reevaluate both the survey, its methodology and what it wants to report in this area.

That is the benefit of linking the two is the Commission has the opportunity to consider the points that you're making in deciding how it wants to proceed with regard to a public release of anything at this stage.

MR. LANE: But I thought originally you said we would have access to this information to help us base our decision --

MS. GAU: Quite the contrary no, no, no.

MS. CRANOR: This is Lorrie Cranor. So I understand that we wouldn't have access to the results because they could be leaked, but could we have access to the methodology?

MR. MEDINE: Let me raise that internally, and I understand the question and I will get back to you on

that. That's a fair question. I can't decide that for the Commission, but I'll get back to you about that.

We were working our way down this line. Richard

and Andrew?

MR. RICHARD SMITH: Richard Smith real quick here. I just wanted to shift gears back to this issue of security disclosures, and I think we'll keep it simple is the real key word because most people don't really care.

The one thing I would say is it's okay to probably brag about your SSL capabilities because sometimes people do understand that, but that's about the limit of jargon they would get into.

Another quick point that I would make is I'm not in the ECommerce business myself, but I suspect there's been some discussion about not hurting small companies by undue security burdens but I believe a lot of companies, small, medium and large actually use hosting services themselves for doing this stuff.

And those are the folks who are providing the security, and that has pluses and minuses, the plus being that they may have the critical mass to provide the security that a large company could even for the smallest group.

On the other hand you have to have then access

to your databases by the company that's off site, and that opens security holes on its own, so it's a more complicated situation in security once you get more

companies mixed into the stew here if you will.

MR. MEDINE: Thanks. Andrew?

MR. SHEN: Andrew Shen. I just want to sort of emphasize something that Frank brought up before. Maybe the most important thing about security in terms of notice is what sort of security you're providing under ideal conditions, but sort of what happens when security breaks down. That's one of the topics we brought up in the security three group because I think that's something very important and I think it goes back to comments that people brought up earlier about market influences, whether there's perfect marketing conditions whether a security breakdown does lead to some tarnishing of reputation.

I think clearly in past security breakdown incidents that has not occurred, particularly the CD Universe case. The break in and CD Universe negotiating with this guy who was holding all the credit card numbers for hostage. None of that was made public to the customers for a couple of months. Now I think you see that same sort of incident repeat itself. Northwest Airlines had a similar incident, Outpost.com.

So I think you clearly can see at least in terms of notice one way you can provide some sort of assurances in terms of dispute resolution.

MR. MEDINE: Richard seems anxious to weigh in on this.

MR. RICHARD SMITH: I am. Richard Smith. A real quick comment about CD Universe. I think it's a little bit premature to judge on that case because it's entirely possible that they didn't go public because they had the FBI involved from day one, and I ended up chatting with a guy, the Maxis guy via E mail, and he just got anxious, and we don't know how it was going but the way it looked to me get they were trying to get this guy to come to the U.S. and then bust him, so they probably handled it okay.

MR. MEDINE: Deirdre?

MS. MULLIGAN: I think most people or many of people in this room are in the business of manipulating data. I know it's quite possible to collect data and analyze it later on, and I think that the only tension between the Commission doing their sweep now and the Commission doing their sweep later is whether or not we would think that you're collecting the wrong data and whether or not we could change your mind.

And my sense is that you are going to collect

notices regardless of what we think, so I don't know that if we came up and said notice means nothing in the security context, which I'm of the general mind to

believe, that it might mean something for your enforcement powers, but I don't think that it means a whole lot as to whether or not the security's good.

So I might suggest that you do something that's much more like Richard Smith did in trying to assess security standards on the web, but I don't have the sense that the Commission would be interested in pursuing such a recommendation so therefore I don't see that there's a harm in you collecting the data now and then using whatever recommendations we come up with to analyze it.

However, I do want to ask a question about the survey. My understanding I think is that you're only looking at a hundred sites? How many?

MR. MEDINE: No.

MS. MULLIGAN: That's what I want to know.

MR. MEDINE: Well, we are looking at two samples. We are looking at the top 100 sites as has been done in the past two years by Professor Culnan in and by us in '98, and we are looking at a sample of an universe of the busiest sites, and I quite honestly don't have a precise number to give you because that's a

number that -- it's a random sample but then sites get kicked in and out.

So I don't want to give you a precise number but

it's a random sample of the busiest sites similar to what Professor Culnan did last year, but as we said in our public statement we're using a different essentially rating service to develop the list but I would say the methodology is in a very rough way similar to what was done last year.

MS. CULNAN: Which was similar to what was done the first time, just more? None of these are reinventing the wheel because otherwise you end up with something that you can't make any comparison to.

MR. MEDINE: That's right. The biggest difference between '98 and '99 just to clarify is in '98 we surveyed the entire body of U.S. commercial web sites. In '99 --

MR. WHAM: Can't do that anymore.

MR. MEDINE: Well, you can't survey it and sample it, but instead we -- Professor Culnan surveyed a weighted sample of the busiest sites, and that's a methodology we are following for this year as well.

MS. CULNAN: So the one thing that will be able to be done legitimately is to this year compare between last year's survey and this year's survey because you're

looking at the same populations pretty much?

MS. MULLIGAN: Except --

MR. MEDINE: Roughly. I don't want to be

absolutely -- it's much closer than between '98 and '99.

MS. MULLIGAN: I just want to voice that last year survey done by Mary Culnan at Georgetown was only at the busiest sites, and the top 100 was not done by Mary and for several very important reasons from at least the consumer and the privacy community.

MR. MEDINE: The FTC in '98 did the top 100 sites so we are again --

MS. MULLIGAN: I know, but the top 100 and the entire universe.

MR. MEDINE: Right. This year we're doing the top 100 and busiest sites, which accounts for I believe on the order of 99 percent of unduplicated reach.

MS. MULLIGAN: I'm just flagging it.

MR. MEDINE: No, no, no. Those are fair. We will be very transparent about our methodology as we were in '98, and people will be free to comment on it.

MR. LANE: Rick Lane, U.S. Chamber of Commerce. The CD Universe comments, can we get that stricken from the record because a lot of it's hearsay about not having the information out and the reasons why? Can we just kind of get that all taken out because it is a

public record?

MS. MULLIGAN: It's a public record?

MR. SHEN: May I respond? I don't think --

Andrew Shen, sorry. I don't think it qualifies as hearsay anymore. I think it's established since it was reported in the press and a lot of people know about it.

MR. LANE: But the reasons why. We heard two different opinions of why something occurred, and that's the problem.

MS. MULLIGAN: They were stated.

MR. SHEN: Like you say its CEO shouldn't have told investors?

MR. MEDINE: Why don't we take that request under advisement as we review the transcript.

Dan?

MR. JAYE: On the issue of security under the review I think one of the key questions is how will the results be applied or interpreted or used. In other words, as you look at the security Fair Information Practices? As you look at disclosure, for what purpose will the information from the survey be used? How will it be interpreted because if you're interpreting is there adequate security, then obviously it's going to drive it versus are you trying to do a survey to see whether policy practices are effective at addressing

consumer competence in which case there have been very

good discussions about the fact that saying something

might be not necessarily meaningful and not as useful as

doing something even if you didn't tell the consumer.

MR. MEDINE: Well, that is the exact subject of the what we're -- merits of this current discussion of that trade-off, and that is what we'll inform the Commission in evaluating results, so I guess it would be helpful to hear again people's views on whether essentially you should have good security and whether you should be disclosing something about security to consumers.

Obviously we're looking at just at what the site says and possibly does with regard to SSL.

MR. JAYE: My question comes back to: To what use will the results be put because that would inform what data we need to collect and how it should be interpreted?

MR. MEDINE: Okay. The results will inform the Commission's observing of web site practices with regard to security. That is on the face of the web site not going behind and pinging the web site or contacting web site officials. It will be simply essentially what is the consumer's experience in dealing with the web site on the issue of security.

MR. JAYE: So from a consumer's experience standpoint and competent standpoint versus is there sufficient security for data protection.

MR. MEDINE: That's right. That's the direct as applied to the survey results of course the committee can be very helpful in educating the Commission and ultimately the public about whether Fair Information Practices call for having certain security measures as we've discussed throughout the afternoon as well as what the web site might disclose to consumers.

MR. JAYE: So the key point I wanted to get to is to the extent that the results are interpreted for example as a basis for -- are interpreted, that's going to be very important that, for example, if the methodology is to look at, Is there sufficient security disclosure, that we want to be very careful that that's not necessarily a statement on whether there is sufficient security and that no conclusions be let to based on that once again as they sometimes are.

MR. MEDINE: That's certainly a fair comment. Rob's been waiting a while.

MR. GOLDMAN: Rob Goldman, a couple small points on this. Appreciate the comment on small businesses outsourcing security to out posting groups and web hosting groups and also the point on, it seems like a curious

thing to look at certainly whether sites say they have security versus whether they deliver it. Certainly it's more relevant -- it would seem to be it would be more

relevant as to whether or not there's actually security, whether or not the site claims there is.

MR. MEDINE: Could I ask, how does the consumer know? How would a consumer know?

MR. WADLOW: That is the point.

MS. MULLIGAN: That's true on privacy also. I would like to highlight the fact.

MR. GOLDMAN: Absolutely. Two small points, I sympathize. It's a hard thing to measure certainly from the outside and than often from the inside as well. I can certainly say we've had issues -- and it may be an issue for an entity's group within the security subcommittee, but issues with out posting groups and who's owning particulars of pieces of software, who's managing switches, who's managing routers, where are there holes and where aren't there holes, and how are those holes measured.

Certainly it would be a much more accurate measurement to have any of the security experts in the room take a look at the site even from the outside, much better from the inside to actually measure whether or not security is there than to read what is or isn't

written on a statement.

MR. MEDINE: All right. Stewart? Okay.

MR. BAKER: I'm not sure this is an initial

committee proposal but it seems to me there's an awful lot of sort of the unhappiness about the idea of doing this because of the security disclosures, but as you say or as Deirdre says you can do what you want.

My thought would be that to suggest that Rick and Deirdre and I just try to write a short letter disassociating the members of the committee who want to sign it from that, saying there a lot of risks in this, this is only one of the options that you might consider in security, and one as to there a lot of doubts and you shouldn't view this as a test of whether there's good security, circulate it around and see if people want to sign it.

I don't know of anyone that wants to participate in that, but I think it might be useful to send the Commission something that says, There's a problem here and you ought to recognize it.

MS. MULLIGAN: Since my name was invoked can I rejoin? Deirdre Mulligan. I would actually like to say I think that would be a good idea except the fact is it extends to privacy also, and that one of the difficulties in assessing privacy is that it's very nice

if a web site says we do X, Y and Z.

We don't transfer your data, we do transfer your data, as a consumer it's very hard for me to assess

whether or not that's happening, and with the FTC without poking around very difficult to assess, the same with security.

MR. BAKER: I'm looking for whether everyone agrees with.

MR. MEDINE: Let me suggest as DFO that if you as private citizens wish to communicate to the FTC outside of the scope of this committee you're certainly free to, and if it's something that you want to put as an option and again as part of your report to help educate the Commission on its interpretation I think it's also appropriate, but I believe we have to separate those two in terms of committee process.

MR. TORRES: Frank Torres. I think we have to recognize that disclosure is only one part of the process here that -- and I echo concerns that other folks raised. I'm very positive about disclosure if it's truthful and meaningful and simple but we do have to get beyond that, and we've said before in the privacy debate disclosure is not protection.

Privacy disclosure is not the same as privacy protection. First of all it can be a lousy best privacy

in the world, but if it's not followed it doesn't do the consumer any good, and the same holds true for the security question.

So I think I'll say something positive about the sweep. I think it's commendable that the Commission is taking a look at this, but you need to take the next step and see what's actually being implemented and whether or not the security protections are real to the extent that they're disclosed or that they even exist.

MR. MEDINE: Again I think the value of this committee is it can educate the Commission on both those questions which is, What is good security or how do you go about providing security on the one hand, and the other is what do you disclose to consumers which may be separate issues, in fact sometimes as we heard earlier may even be in conflict to some extent because you don't want to disclose too much about your security.

But again the question that I posed to the committee for feedback on is a minimum disclosure important for consumers to have at least some sense of confidence in how the web site and companies are handling their information. Jane Swift.

MS. SWIFT: Jane Swift. Now I have two now. I would just say --

MR. WHAM: Does one of those say CBS on it?

MS. SWIFT: I think disclosure is only important when it's accompanied by some sense of verification, and disclosure in and of itself which I'm not sure is

exactly the same as the reality of security.

Verification means is what they're saying they're doing is what they're doing, which I think is the same point Deirdre is making on privacy is it's good to have disclosure. It's good and I think necessary that you have it in terms that folks who -- you all design your software so idiots can use it. You should have that same standard for defining other policies that people can understand, and I include myself in the idiot column, so it's not as insulting.

But verification, I think most consumers believe that verification has to come from a third-party, and that's where I think the conundrum is when you're talking about self regulation.

MR. MEDINE: Again those are useful comments and certainly there are skilled programs and others who do verification. There also is a link between disclosure and what people are doing which is the FTC Act's prohibition on deceptive trade practices. That is if you're saying you're doing something, then there is a legal standard by which you can judge whether someone is actually doing. It you might want to consider that in

the security context as well which is you hold yourself up to a certain standard, then the public is relying on that representation that's being made.

MR. PONEMON: May I emphasize one point? As I said before -- Larry Ponemon, Pricewaterhouse Coopers. The level of verification depends, and I don't want there to be -- consumers misled that because they have seal A, B, C or firm X, Y and Z doing the work that they assume that it is in fact 100 percent or 95 percent level of confidence that everything that is in the system is secure, that privacy is maintained and so forth.

There are different levels of security. There are different levels of assurance and so that has to be factored into the equation as well?

MR. MEDINE: Alex and then Lance happens.

MR. GAVIS: Alex Gavis, Fidelity. I want to go back or move back to 10,000 feet for a second in that brick and mortar companies for a long time have been dealing with information that's been provided to them by their customers, and in fact information security practices and have been around for a long time, and I guess to some extent the case has to be made as to why suddenly in this regime there needs to be a disclosure practice or there needs to be some sort of enhanced

method of disclosing practices.

And I'm not quite sure we made that case. I'm not quite sure where we are. Maybe your survey will

explain at the outset sort of why you're in this space and why you're thinking about it, but I do think companies do and a number of them have had information security practices and quite reasonable ones and don't necessarily disclose them to the public, and there probably hasn't been a need to disclose them to the public.

MR. MEDINE: Just to respond briefly to that point. The Commission since 1996 has laid out what it has viewed as Fair Information Practices, and it arrived at that by examining the work of others in this area including the OECD's 1980 guidelines, the work of the Commerce Department, Ron's Privacy Commission and so forth in reaching those conclusions but viewed these as all interrelated components of Fair Information Practices, that not only does a company treat your data the way it says it does and tells you what it's doing about it but that essentially may not be much comfort if they don't protect it from improper access and improper use.

But I think that's basically what led to the Commission in '96 enunciating what it viewed it's Fair

Information Practices.

MR. LANCE HOFFMAN: Lance Hoffman. Disclosure is important but it does have problems. We all realize

that, and indeed in the security three subgroup I was in, one thing we pointed out we were concerned about the fact that, for example, mandatory check off could serve a disclaimer function for bad actors arguably relieving them of liability, so that's an issue that always comes up with this sort of thing. I want to get that on the record because it is something to look at.

I want to note also that I would suspect that the vast majority not by traffic but by just counting the sites, web sites do zero when it comes to -- I'll lump together Deirdre's do zero in terms of talking about it in terms of disclosing.

The Yahoos and the AOLs and so forth, no problem, but there are a lot of web sites that do nothing, okay. So again this sort of what you do just saying I do anything at all differentiates and I think that's important, but I won't beat that dead horse anymore.

I do want to say something with regard to the sweep since I hadn't focused on it until people started saying Oh, the sweeps, the sweeps are coming, why not do this first and that first. I really disagree I think

it's very important the FTC does the sweeps when they said they were going to do them.

Time marches on. There's always a good reason

for postponing something, new things happening. You know, come on, you have to work on Internet time. Sweeps will happen they'll happen next year or two. We're going to make changes incrementally so I don't think the level of error, if you would, or embarrassment that might come out of the sweeps is going to negate their value relative to the information we get to build a frame to work on.

MR. LANE: Rick Lane, U.S. Chamber. It's not embarrassment. It's more misinterpretation that we're fearful of, and that's in an election year and political ramifications -- maybe I'm too much inside the Beltway, but perception becomes reality in this town very easily, and in a election year it's even more heightened, and the concern is if you have raw data that's not explained or not in context, the perception becomes a reality.

And you have knee jerk reactions that could be a hindrance to the current economic development we have seen in the ECommerce world, so that is the concern that is shared before there's a context put in place, so that is on that issue.

MR. MEDINE: Can I just add to that, that again

this committee is uniquely situated to get the Commission's ear as the Commission considers the raw data and the Commission analyzes the data and the

Commission writes the report that explains the results.

And so this is an opportunity to make your case to the Commission about how the data ought to be interpreted and this committee's work will be the tool the Commission uses in evaluating that information.

MR. LANE: Can Congress get the data before the report is written?

MR. MEDINE: Before the report is written?

MR. LANE: Once the sweeps are done and the data is in place --

MR. MEDINE: Counsel's advised me that I shouldn't answer that questions because that's a loser either way. I don't know.

MR. KAMP: John Kamp from the AAAA. I just wanted to underline the political danger of misinterpretation. In fact in a public meeting this week a member of the White House staff in a meeting by an OPA has already opined that the industry is not going to do well in the study, and that is going to increase the calls from the Congress to have legislation in this area.

So we're talking about a politically very

important, if not volatile, explosive possibility being created here by doing this study I think prematurely.

MR. WHAM: This is Ted Wham from Excite@Home. I

would argue that any organization of any size on the Internet that didn't see this coming and didn't act for it deserves whatever the hell happens to them because exactly the same thing happened last year. Exactly the same thing happened the year before.

The basic fundamentals as I understand them of how the study's being run are very, very close and certainly within the public's eyes are indistinguishable. I think Lance's comments about how time marches on and you do the best could not be more apropos to the situation that's right here.

In 1997 we were an early participant with TRUSTe. TRUSTe hadn't been around that long. They had 20 different people out there, and the FTC is out drumming -- I have to take that back, 1998, they're drumming on the -- their thing and saying, We're going to do a sweep, We're going to do a sweep, and TRUSTe contacted us and said Oh, my God, industry didn't have their act together, can you help us.

And I spearheaded an activity with all of the executives where we wrote letters to the top 100 domains out there and said, You got to have a privacy policy up,

and then I it corralled all of those executives and I got George Bell and Brent Bollington and Joe Kraus to sit down on the telephone, and getting a

slice of their time is no fun.

And we were calling people that didn't want to receive our calls, like CEOs of Lycos that didn't think that highly of us, all sorts of different people saying, You have to have a privacy policy out. This is a year and a half ago. Since then COPA's come out. Since then the first policy sweeps have come out and so forth.

If I'm not incorrect what the FTC is doing out there is taking a review of privacy policies, is taking a top line, saying who has them and we did this three years ago, only 22 percent or whatever the numbers were, and then we did them a year after that and 68 percent of them top out there, but if there's one of the top 100 that doesn't have a privacy policy up, shame on them.

MR. JAYE: Can I just take a comment on that for a second because it's very interesting we looked at the '98 sweeps. I think this actually portrays why interpretation methodology is so important.

When you actually went into the data on the '98 sweeps it was not nearly as bad as it was initially portrayed. On page 1 they talk about 14 percent of

sites that is the general sites of general ECommerce companies which generally were brick and mortar companies that had web sites only had privacy statements.

Ted's exactly right. There was a massive industry effort to try to get the web -- and the focus was completely on web centered companies, and back on page 6 was the first mention of the fact that the web actually didn't do as miserably. Admittedly they should have had 99 percent compliance because of the outreach, I forget whether it was 50 percent or 60 percent, but back on pages 6 was the details that the top 100 sites had actually done significantly better than that 14 percent.

But the front page talked about a set of sites that candidly those of us who were out canvasing and doing outreach weren't even talking to because we had -- basically two years ago they weren't really -- they weren't as important as they are now because the general top large companies weren't really on the web that much back then.

MR. LANE: This was a front page story.

MR. JAYE: The issue was 14 percent, and nobody dug down to page 6 where it talked about what the largest sites which represented the bulk of the percent of time consumers spend browsing so that the bulk of the

23 percent of time consumers spend browsing was being spent

24 on these top sites which related -- which had although

25 not acceptable way below par privacy statements and

coverage, still were significantly north of what primarily got presented or picked up by the media.

So that's one of the reasons why we do have a very -- a great deal of sensitivity about interpretation of the results.

MR. MEDINE: If I could make two points of clarification, and then we can continue for just a little while longer one, is the Commission's report and the survey result will follow this committee's report the Commission will have the opportunity to consider the work of this committee.

Second, if anyone is reporting on the results of our survey, I can assure you we don't know what the results of our survey are going to be, and so I don't know how anyone else could possibly know what the numbers are going to look like because we're in the middle of it and we don't what the numbers are at this stage in the process

Larry?

MR. PONEMON: One thing that I just wanted to mention about based on our experience and looking at privacy policies, we do a lot of privacy risk management

and privacy work and the majority of our clients are not in compliance, are not in compliance with their stated policy.

So the mere fact that you have policies that gives false confidence and false praise in many cases to companies. It's easy to write it but it's a lot harder to walk the talk, and that's what we see. That's across the board, not just in the e-space for all organizations.

MR. MEDINE: I'm attempted to say provide us a list of those companies, Richard and then Stewart.

MR. RICHARD SMITH: I would like to agree with that, also the little bit I've looked at privacy policies and security practices there's a -- and so it's sort of amusing here, this discussion of interpretation of and results I find interesting because if you really get down -- the privacy policy is one aspect. Practices is the more interesting issue.

But one thing that's important to say about disclosure I want to make one small remark about disclosure is privacy policies do have another use beyond consumer confidence and explaining to consumers what's going on which is also it gets into written form for people at the company to understand what their company is committing to, but, yes, they don't always

follow it all, but it is there written, and I think it's an important thing. It's just like a contract. It's there. You make your mark in the sand so I

don't want to discount disclosure totally as another whole aspect because it lets people in the company.

MR. MEDINE: Why don't we, given the hour, take a handful more comments and then we can wrap up for today. Stewart?

MR. BAKER: I tried my hand at a draft while you guys were talking. It doesn't actually say they shouldn't do the survey or they should, but just says there's a problem so I'll read it.

We're all members of the FTC advisory committee writing in our individual capacity. At our last meeting there was extensive discussion of the Commission's plans to do a sweep of major commercial web sites to examine, among other things, the security disclosures provided to the public by those sites.

Disclosure of security practices, however, may have little or nothing to do with the actual security provided for customer data. Equally important, the lack of a statement on security practices does not mean that a site provides inadequate security.

While disclosure of security practices is an option for encouraging good security, it is only one of

many options the committee is evaluating. There is a real risk that a survey limited to the presence or absence of a security statement on a web site will be

misinterpreted.

We urge that the Commission consider these views in deciding whether to conduct such a survey and how to present and interpret any data that may result from such a survey.

That was sort of --

MR. MEDINE: I'm going to terminate discussion of things that the committee members do in their individual capacity, but let me just say that that's the kind of committee report that would be extremely helpful to the Commission in interpreting the results of this information so you might want to consider in the security group addressing that as part of your report in terms of how the Commission ought to evaluate survey results.

Let's take it like one or two comments. Deirdre?

MS. MULLIGAN: Deirdre Mulligan. I fully support that but I think the frustration is that it appears that everyone around this table recognizes that a security statement does not give us adequate information to evaluate security.

Yet people seem to want to hang on to the fact that privacy statement might give us adequate information to evaluate privacy, and I think I would be

overjoyed if the people around this table would like to write a joint letter to the Commission suggesting that rather than doing another sweep, where I completely agree can be wildly misinterpreted, 66 percent increase in a discussion about privacy, it tells us nothing about whether or not people's privacy is being protected or not -- if we would like to suggest that the Commission use its resources in another manner.

For example, I think the survey that Richard Smith did in coordination with the California Health Care Foundation was an incredibly useful detailed survey. It showed both what the policy stated and whether or not there they were being adhered to, and that's the kind of information that I think you can use to do a valid assessment.

And if other people think that would be an useful thing to do I would love to do it. Our public fund should be spent wisely.

MR. MEDINE: Thank you all for a lively, and informing day, and we'll see you on March 31. We're adjourned.

(Time noted: 5:08 p.m.)

- - - - -

C E R T I F I C A T I O N O F R E P O R T E R

DOCKET/FILE NUMBER: P004807

CASE TITLE: ONLINE ACCESS AND SECURITY

HEARING DATE: FEBRUARY 25, 2000

WE HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by us at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of our knowledge and belief.

DATED: FEBRUARY 28, 2000

SUSANNE Q. TATE, RMR

DEBRA L. MAHEUX

C E R T I F I C A T I O N O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and

format.

DIANE QUADE