I N D E X

FEDERAL TRADE COMMISSION

ADVISORY COMMITTEE ON
ONLINE ACCESS AND SECURITY

9:00 A.M.
FEBRUARY 4, 2000
VOLUME 1

FEDERAL TRADE COMMISSION
600 PENNSYLVANIA AVENUE, N.W.
ROOM 432
WASHINGTON, D.C.

REPORTED BY: SUSANNE Q. TATE, RMR

A T T E N D E E S

FEDERAL TRADE COMMISSION:

Robert Pitofsky, Chairman

Jodie Bernstein

David Medine

Jessica Rich

Martha Landesberg

Laura Mazzarella

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.

Steven J. Cole, Council of Better Business Bureaus

Lorrie Faith Cranor, AT&T Laboratories

Mary J. Culnan, Georgetown University

E. David Ellington, NetNoir, Inc.

Tatiana Gau, America Online, Inc.

COMMITTEE MEMBERS:

Alexander Gavis, Fidelity Investments

Rob Goldman, Dash.com, Inc.

Robert D. Henderson, NCR Corporation

David Hoffman, Intel Corporation

Lance J. Hoffman, George Washington University

Josh Isay, DoubleClick, Inc.

Daniel Jaye, Engage Technologies, Inc.

Eric J. Johnson, Columbia University

John Kamp, American Association of Advertising Agencies

Rick Lane, U.S. Chamber of Commerce

James W. Maxson, Delta Air Lines, Inc.

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

Arthur B. Sackler, Time Warner, Inc.

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

Frank C. Torres, III, Consumers Union

COMMITTEE MEMBERS:

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

- - - - -

CHAIRMAN PITOFSKY: Good morning, everyone.

Good morning. I'm Bob Pitofsky, Chairman of the Federal Trade Commission, and I'm certainly delighted to welcome all of you to this first meeting of the FTC's Advisory Committee on Online Access and Security.

On behalf of the Commission, I'd like to thank all of the members of the committee for their willingness to participate, for their commitment. We also received letters in support of almost 190 people to serve on this committee, and I want to emphasize to those who are not formally on the committee that they are welcome to attend all of our proceedings, that they can participate, they can make statements, and they certainly can offer written comments to the Commission, which we will take into account at the conclusion of our process. So, we encourage all interested people to continue to participate in the work of this group.

As you know, this agency has been much involved in issues relating to privacy for five years now. We have held workshops, forums, seminars. We've surveyed the practices of companies on the net. We've offered data and recommendations to Congress, and as many of you know, we are getting ready soon to conduct another

survey of the websites to see what privacy policies look like now.

We pretty much reached a general agreement as to what good information practices ought to be, and they include notice to consumers so that people will know what kind of information is being collected about them and how it's used; choice, so that the consumer is in control of that information and control of where the information is delivered; access by consumers to data, by which I think we all mean reasonable access, and that would take into account the costs and benefits of accumulating the information, making it available, perhaps establishing procedures to correct it; and then security arrangements for the information while it's being held by commercial enterprises.

While I think there's agreement on these general principles looking down from 10,000 feet, when you get down at ground level and you really have to get into the details of what the policy is and what implementation is about, that's when the challenging -- that's when the challenges really begin. And it's for that reason that we turn to you, the members of this advisory committee, a group of 40 experienced, qualified individuals representing the broadest range of interests to help the public, to help government and to help us better

identify and understand relevant implementation issues with respect to two of these good information practices, access and security.

These principles raise technological, policy, management issues, and you are and have been selected because you're the national experts in this area, and we have charged you as a group with considering the access and security questions and coming up with a range of options that the Commission can consider.

I think it will be extremely helpful to the work that we're doing. I think it's critical that consumers have this kind of protection, not just -- well, of course, for the welfare of consumers, but also for the welfare of the internet, since we all agree, I think, it will not grow as it should grow unless consumers are confident about the security of the information that they give over. It remains the number one reservation that consumers have about surfing the net, about purchasing on the net and so forth.

It's an exciting new medium, and we want to see its explosive growth continue, but at the same time, we are absolutely committed to protecting the privacy rights and interests of consumers, and we very much look forward to receiving your advice on these questions.

With that, let me turn this meeting over to

David Medine, who I think most of you know, and I hope you will proceed with a very constructive and useful discussion today.

MR. MEDINE: Thank you, Mr. Chairman.

Good morning. As the designated federal officer for the advisory committee, I'm delighted to welcome the members of the committee to their first meeting. It's a pleasure to welcome back some very familiar faces to the Commission as well as some new faces to the Commission to give us new perspectives on some of these issues.

I'd like to reiterate the Chairman's thanks to the many people who submitted nomination letters and to the people who have traveled both near and far to join us here today. We welcome everyone's participation and are looking forward to a lively and informative discussion.

We turn now to the work of the committee, and I mean work. This committee is expected to produce a thorough and thoughtful written report to the Federal Trade Commission on the important implementation issues presented by the fair information practice principles of access and security. All of your efforts should be devoted and focused on that goal.

I'd like to take a few moments to talk about the process by which the committee will accomplish its

work. First, our goal in setting up an advisory committee, as opposed to simply holding another workshop, was to ensure that the final report would be truly a product of a diverse group of experts in the field, your product. We're asking that you work together to make sure that all relevant views are expressed, discussed, debated and set forth in a public report to the Commission.

Second, I want to emphasize that we're looking to the advisory committee to come up with a range of implementation options for access and security, not a single right answer. I think this will be more useful to the ongoing discussion of these issues, as well as a more feasible way to proceed in light of the many diverse interests represented in the relatively short timetable we have in front of us.

The goal here is not to forge a consensus view on the two major issues before us. The goal is not to convince your colleagues of the correctness of your position, although you may certainly try to do that. The goal is to state and support your views so that the FTC Commissioners and ultimately the public can benefit from your thinking, experience and information.

Third, I want to emphasize the openness of these proceedings. Meetings are open to the public, and we

encourage those attending to address issues during an open mike session scheduled at each meeting; that is, the public will have an opportunity to present their views. Perhaps more importantly, we've set up a process for the public to submit written comments to the advisory committee for its consideration. Again, we believe that having diverse members of the committee consider and discuss these comments from the public will advance the debate on these important issues.

Finally, I want to reiterate the working nature of this committee. As I think you'll agree, it's very important that we have something to show for our efforts at the end of the process, specifically a very useful final report that addresses the relevant options for implementation, as well as their costs and benefits. Therefore, I'm hoping we can use our time here as productively as possible and that the members take full advantage of the time between our meetings to refine their thoughts and put pen to paper.

Yesterday the Commission announced that it would again be conducting a survey of U.S. commercial websites to determine the extent to which the sites are collecting personal information from online consumers and implementing the fair information practices of notice, choice, access and security, as just outlined by

the Chairman. This survey and this committee will proceed on parallel tracks. They are complimentary efforts.

The online survey will provide critical raw data about current industry practices, much of which will likely address issues not immediately before this advisory committee. Detailed substantive analysis of the data will follow later and will be shaped in part by the work of the advisory committee and ultimately its report.

Lastly, I want to thank all the FTC staff members who have worked for months in preparing for this meeting, including Laura Mazzarella, Hannah Stires, Martha Landesberg, Allison Brown and Jessica Rich.

Okay, let's get started. The first item of business is to take a call of the role, and I will go through it.

James Allen, eCustomers.com?

MR. ALLEN: Here.

MR. MEDINE: Stewart Baker, Steptoe & Johnson?

For the purposes of the court reporter, people will have to speak up. This is a little bit like a deposition, where nods won't do it.

MR. BAKER: Here.

MR. MEDINE: Richard Bates, Walt Disney

Company.

MR. BATES: Here.

MR. MEDINE: Paula Bruening, TRUSTe?

MS. BRUENING: Here.

MR. MEDINE: Richard Casey, RSA Security?

MR. CASEY: Here.

MR. MEDINE: Professor Fred Cate, Indiana University School of Law?

MR. CATE: Here.

MR. MEDINE: Jerry Cerasale, Direct Marketing Association?

MR. CERASALE: Here.

MR. MEDINE: Steven Cole, Council of Better Business Bureaus?

MR. COLE: Here.

MR. MEDINE: Lorrie Faith Cranor, AT&T Laboratories?

DR. CRANOR: Here.

MR. MEDINE: Mary Culnan, Georgetown University?

DR. CULNAN: Here.

MR. MEDINE: David Ellington, NetNoir?

(No response.)

MR. MEDINE: Tatiana Gau, America Online?

MS. GAU: Here.

MR. MEDINE: Alexander Gavis, Fidelity Investments?

MR. GAVIS: Here.

MR. MEDINE: Rob Goldman, Dash.com?

(No response.)

MR. MEDINE: Robert Henderson, NCR Corporation?

MR. HENDERSON: Here.

MR. MEDINE: David Hoffman, Intel Corporation?

MR. DAVID HOFFMAN: Here.

MR. MEDINE: Lance Hoffman, George Washington University?

DR. LANCE HOFFMAN: Here.

MR. MEDINE: Josh Isay, DoubleClick?

MR. ISAY: Here.

MR. MEDINE: Daniel Jaye, Engage Technologies?

MR. JAYE: Here.

MR. MEDINE: Eric Johnson, Columbia University?

(No response.)

MR. MEDINE: John Kamp, American Association of Advertising Agencies?

DR. KAMP: Here.

MR. MEDINE: Rick Lane, U.S. Chamber of Commerce?

MR. LANE: Here.

MR. MEDINE: James Maxson, Delta Air Lines?

MR. MAXSON: Here.

MR. MEDINE: Michael McFarren, Bellerophon?

(No response.)

MR. MEDINE: Gregory Miller, MedicaLogic?

MR. MILLER: Here.

MR. MEDINE: Deirdre Mulligan, Center for Democracy and Technology?

MS. MULLIGAN: Here.

MR. MEDINE: Deborah Pierce, Electronic Frontier Foundation?

MS. PIERCE: Here.

MR. MEDINE: Ron Plesser, Piper, Marbury, Rudnick & Wolfe?

MR. PLESSER: Here.

MR. MEDINE: Lawrence Ponemon, PricewaterhouseCoopers?

DR. PONEMON: Here.

MR. MEDINE: Richard Purcell, Microsoft Corporation?

MR. PURCELL: Here.

MR. MEDINE: Art Sackler, Time Warner?

MR. SACKLER: Here.

MR. MEDINE: Dan Schutzer, Citigroup?

DR. SCHUTZER: Here.

MR. MEDINE: Andrew Shen, Electronic Privacy

Information Center?

MR. SHEN: Here.

MR. MEDINE: Richard M. Smith, internet security consultant?

MR. RICHARD SMITH: Here.

MR. MEDINE: Jonathan Smith, University of Pennsylvania?

DR. JONATHAN SMITH: Here.

MR. MEDINE: Lieutenant Governor Jane Swift, Commonwealth of Massachusetts?

MS. SWIFT: Here.

MR. MEDINE: Frank Torres, Consumers Union?

MR. TORRES: Here.

MR. MEDINE: Thomas Wadlow, Pilot Network Services?

MR. WADLOW: Here.

MR. MEDINE: Ted Wham, Excite@Home Network?

MR. WHAM: Here.

MR. MEDINE: Rebecca Whitener, IBM Corporation?

MS. WHITENER: Here.

MR. MEDINE: Okay, thank you all. We certainly have a quorum. I think we can proceed with our business.

As a working group, I'm going to have to go through some administrative matters just to get

ourselves on a firm footing as part of a formal federal advisory committee.

First, the court reporter sitting to my left, this meeting will be transcribed, and transcripts of all of the sessions will be put on the FTC's website. This is a major challenge for a court reporter having a table of over 40 people, all of whom are talking, so I would ask that before each of you speak, you identify yourself every time that you speak so that the court reporter can keep a proper record. Also, for the benefit of the court reporter, let's have only one person talking at a time so that she can keep a comprehensible record of these proceedings. Thank you.

Turning to the webpage, the advisory committee has a webpage. It's on www.ftc.gov/acoas, or there's also a link from the FTC's home page, ftc.gov. This is an important place for members of the committee to check for information, submissions, agendas and other items relating to the work of the advisory committee. We will post all relevant documents relating to the committee, and, of course, this page is also fully accessible to the public, as well.

We will be sending committee members e-mails to alert you to any new materials on the website so that you don't have to constantly check it first thing in the

morning. We will let you know when new and important items have been added to the website. We'll also ask that you print out items from the website for your consideration. If that presents a problem, Hannah Stires, who will become very familiar to all of you as your technical support person, will be happy to assist you in printing out materials.

Moving on to submissions of materials at future meetings, if you intend to distribute documents at meetings, please make them available to members of the committee, if possible, in advance of the meeting, and again, Hannah Stires can receive your e-mails and post these items to our website and distribute them. If you bring hard copies of materials to meetings, please bring 44 copies for consideration by all your fellow committee members, as well as an electronic version that we can post to the website. If that presents, again, hurdles for you in terms of copying it, again, please contact Hannah Stires, preferably five days in advance of the meeting, so that she can get those materials copied and distributed.

The public may submit comments or questions for the advisory committee's consideration at any time up until April 28th, and the comments can be submitted to advisorycommittee@ftc.gov, that's the e-mail address.

Again, we will post all the public comments on the website and alert you to their receipt. These are comments that are not being made to the FTC. These are comments that are being made to the advisory committee for its consideration and review.

Members of the advisory committee who want to communicate among themselves can e-mail to advisorycommittee@ftc.gov, and we will transmit information to the committee members.

Later in this meeting, there will be an opportunity for the public to raise comments and questions, and we'll invite people in the overflow room who do wish to participate in the public comment period to come to Room 432 to address their comments directly to the committee members.

I now want to turn to the bylaws of the committee. I'm aware that because of some recent snow that not all of the committee members received their bylaws in the mail in advance, although I hope by now all the committee members have received the bylaws either by fax or e-mail. If people need a moment to review the bylaws, we can certainly take some time to do that. I would like to touch on some of the high points of the bylaws before we move to a vote of the committee to consider accepting the bylaws.

First, in terms of membership in the committee, if a member cannot attend a meeting and wants to send a substitute, under the bylaws, they must obtain a written agreement from the designated federal officer. The Commission may replace any member of the advisory committee who is unable to fully participate in the committee's meetings.

Our meetings must proceed with a quorum of 21 members present to have a meeting. A summary of the agenda for each meeting will appear on the Federal Register 15 days before each meeting, so we will shortly be publishing the agenda for the next meeting because of the short time period between the first two meetings. And again, this will be -- the agenda will be posted on the website.

As I mentioned before, all meetings will be transcribed, and within one to two weeks, the transcripts will be on the website. Materials brought before or presented to the advisory committee will be made part of the transcript, and again, posted on the website.

Later in the session today, we are looking to form some subgroups to conduct some of the work of the advisory committee between meetings. Subgroups cannot technically have more than 19 members; otherwise, there

would be such a quorum in the meeting of the committee that it would have to be public. The subgroups will report only to the full committee, and we look forward to much of the work of this group being conducted in those subgroups between meetings.

Voting, the designated federal officer will request a motion for a vote, but any member may make a motion for a vote at any time. Decisions by the group are made by a simple majority, and if all members are present, again, that would be 21.

In terms of support, the Commission, as part of the Federal Advisory Committee Act, has agreed to provide the necessary support for the operations of this committee; however, we are unable by law to compensate the committee members for travel-related expenses.

Those are some highlights of the bylaws, and I guess does anyone have any questions or issues they want to raise before we move to a vote on the bylaws?

Yes?

MR. SACKLER: Art Sackler.

I have a couple of questions about the voting. I think you just implied when you said everybody is here that the majority would be 21. Does that mean that any majority vote is a majority of whoever shows up, as long as we have a quorum?

MR. MEDINE: Yes, exactly, so long as there is a quorum present, it would be a majority of those present. That would constitute an affirmative vote of the committee.

MR. SACKLER: Okay. Are proxies allowed?

MR. MEDINE: No. That is, the requirements of the committee are that people attend the meetings. There is a procedure, as I mentioned earlier, if you are unable to attend a meeting to get written approval from the designated federal officer to have somebody appear in your stead, and so if for some reason one of the committee members cannot be here, they could have essentially a representative appear for them.

MR. SACKLER: Okay. And are the same voting rules applicable to the subcommittee or subgroups or whatever you're going to be having?

MR. MEDINE: No, the subgroups will operate essentially on their own and report back, and again, the key point here is that you're all essentially individual members of this group. You have the right to express your views in the committee, and you have ultimately the right to express your views in the final report to the Commission. So, again, there's no requirement for consensus, and therefore, there is no need to take a vote at the subgroup level, because you essentially have

a right to express your views even as an individual to the larger group. Again, I anticipate probably the next major vote, if not only final vote, would be on sending the report of the committee to the Commission at the end of the process.

MR. SACKLER: Okay, thank you.

MR. LANE: I have two amendments, proposed amendments for the bylaws. How do we move forward to offer those?

MR. MEDINE: Why don't you offer them right now. You have to identify yourself.

MR. LANE: Sure, this is Rick Lane from the U.S. Chamber of Commerce.

The first amendment that I would like to offer is basically based on the fact -- and I think everyone around this table agrees -- that the internet cannot grow without consumer trust. So, in the Purposes section of the bylaws, I would just like to add at the end of the first sentence, to make it even longer, is to add, "in order to optimize the value of the internet and to build consumer confidence." So, should I read the whole sentence --

MR. MEDINE: Sure, why don't you do that.

MR. LANE: -- with that so people can follow along?

"The purpose of the advisory committee is to provide advice and recommendations to the FTC regarding implementation of certain fair information practices by domestic commercial websites, specifically providing online consumers reasonable access to personal information collected from and about them and maintaining adequate security for that information," and where I would like to add, "in order to optimize the value of the internet and to build consumer confidence."

MR. MEDINE: Okay, why don't we take them one at a time.

Is there any discussion on that proposed amendment to the bylaws?

DR. KAMP: John Kamp from AAAA.

I'd like to speak in favor of that, most importantly because I think the consumer confidence reason is the primary reason for all of what we do here in this matter, and I think it's one that essentially is uncontroversial here but an important message that I think that we remind ourselves of as we go forward here and remind -- and make sure that the public is not in any way confused about what it is that we're doing.

MR. MEDINE: Other comments or questions? I was going to wait for a motion, yes.

Yes?

DR. JONATHAN SMITH: Yes, I'm Jonathan Smith.

How do you measure the value of the internet? I mean, that's an imprecise statement.

MR. LANE: What we want to ensure is that --

MR. MEDINE: I'm sorry to burden the discussion, but for the benefit of the reporter, every time you speak, you need to identify yourself.

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

What we want to ensure is we do not diminish the value of the internet to both consumers and businesses by placing unreasonable restraints or requirements on either side.

MR. TORRES: Frank Torres from Consumers Union.

I don't have any objection to this provision, but I do agree with some of the impreciseness of it. I think that --

MR. LANE: If you would like to qualify it, then -- I'm sorry.

MR. TORRES: -- I think that it's a given, you know, that a part of our function is to see what we can do to build consumer confidence and trust in the internet or we wouldn't be here. So, I don't object to the statement in principle. I guess maybe what I'm trying to say is the necessity to have something like

this in here where it's kind of implicit that that's what we're all about.

MR. LANE: Just clarifying.

MR. MEDINE: Okay.

MR. LANE: Should I make a motion to --

MR. MEDINE: Any further discussion?

Certainly.

MR. LANE: Motion to accept this amendment.

MR. MEDINE: Is there a second?

DR. KAMP: Second by Kamp.

MR. MEDINE: All in favor -- why don't we try to proceed by oral vote, if we can, and then a recorded vote, if necessary.

All in favor, say aye.

All opposed, nay.

Well, maybe we should have a recorded vote, I guess. Can we take -- do we take the majority rules? Does everyone agree there is a majority in favor of that?

COMMITTEE: Yes.

MR. MEDINE: Okay, that's adopted.

Okay, second motion.

MR. LANE: One of the reasons for the success of the internet as a business tool is low barriers to entry, especially for small businesses. The question of

what constitutes reasonable access and adequate security are intimately tied to the state of technology. What is doable with relative ease at reasonable cost today is not the same as what might be doable down the road.

Put another way, what is theoretical or cost-prohibitive today might be reasonably accomplished in the future. So, in fact, the state of technology ought to be considered as part of our purposes. So, therefore, I would like to add an amendment, a second sentence after the first sentence, that reads as follows:

"In developing its recommendations, the advisory committee will take into account the state of today's technology so that the recommendations are within the bounds of both what is technically feasible and economically reasonable."

MR. MEDINE: Any discussion?

MR. LANE: I do have copies of this. I think I do have -- I might have 40 copies of this if people are interested in actually reading them.

MR. MEDINE: Lance?

DR. LANCE HOFFMAN: Lance Hoffman, George Washington University.

I am a professor of computer science at GW. This could lead us down a slippery slope where I don't

think we would want to go. We are, in essence, dealing with values and what balances we want to strike to in some sense wire in the technology, to do this is a bad idea. Technology is going to change too fast, and you'll have numerous conflicts of technology getting ahead of the law. I don't think it's wise for that reason.

MR. LANE: Yeah, well, that's what we agree with, but what we don't want is actually the opposite of that, where recommendations are made for certain security measures that change so quickly that we are locked in in one way as a recommendation. So, it's actually getting to your point more so than trying to lock in -- obviously from the U.S. Chamber's perspective, we never want to have any type of technological standard or mandate -- I'm sorry, this is Rick Lane again from the U.S. Chamber -- but on the same side, we don't want to have walls put up and saying you need to have this type of security mechanism in place, because as we all know, there are hackers out there constantly able to circumvent certain technologies. So, what we say is reasonable now and protects now may not be reasonable in the future. So, it addresses your point.

MR. MEDINE: Okay, Mary.

DR. CULNAN: Mary Culnan, Georgetown University.

I think this is more of an operational statement, and this is something that we would clearly consider in our discussions, because every discussion of security is a balance between what's technologically feasible and costs, and I just don't think it's appropriate to put it in the purpose. We're already heading towards recommendations when we have barely begun our work.

DR. JONATHAN SMITH: Jonathan Smith, U-Penn.

I'm curious as to what "economically reasonable" means. I mean, who decides? That's the problem.

MR. LANE: Well, again, like -- Rick Lane from the U.S. Chamber -- like all judgment calls, you know, you don't want to ask companies to put Fort Knox around a piggy bank. I mean, there is some type of levels that we need to look at. Again, this is just a clarifying -- what is reasonable is what we're going to have the other meetings about, and again, this is just a clarifying amendment of our purpose.

MR. MEDINE: Could I -- for the discussion, just a technical matter, could people please speak into the microphones for the benefit of those in the overflow rooms.

MS. MULLIGAN: Deirdre Mulligan.

I'd like to second Mary's comments that I believe the statement that this is about reasonable access and adequate security already encompass both of the sentiments in here, and, in fact, I think part of our job here is to help identify what technologies would be appropriate and to actually stimulate their development and hopefully their deployment in a more cost-effective manner, and I wouldn't want to presume at the outset that we have to take the bounds of current economic conditions, et cetera, as limiting factors at the beginning of the discussion.

MR. MEDINE: Okay.

MR. HENDERSON: Bob Henderson.

I guess I'm uncomfortable with this statement when it talks about the state of today's technology. The technology moves so fast that making a decision today, based on the state of that technology, especially looking at the technically feasible and economically reasonable state of that technology, I don't think this committee's going to be in a position to make that type of judgment, and I think we have to look at the issues surrounding the consumers' concern in terms of access and privacy and let the technology and the businesses decide how to execute that. So, I think this is an

inappropriate statement as part of the bylaws.

MR. MEDINE: Okay.

MR. TORRES: Frank Torres, Consumers Union.

I would agree with those comments, as well as the sentiments expressed by Dr. Culnan. At the git-go, we're already going to limit ourselves if this is adopted, and I don't think that is appropriate.

MR. BAKER: Stewart Baker from Steptoe.

I think it's a perfectly reasonable statement of purpose, but it's going to distract us to debate it here. We'd be better off just moving on to the main business.

MR. MEDINE: Again, let me just reiterate that the committee will have the freedom to consider what it wants to consider and to develop its recommendations, and so I suspect this is an issue that will certainly play an important role for many of the committee if not all of the committee participants, but I guess the question is whether it unduly constrains some of the discussion. So, I guess if you want to --

MR. LANE: Since there seems to be some confusion, because I agree with the gentleman from NCR that we're not trying to pick technologies now. The purpose of it was to make sure that we didn't do that, but since there is some confusion, I'd be happy to

withdraw it and consider it as part of our debate in the broader scope of things.

MR. MEDINE: Thank you.

Are there other -- we're moving on to other issues relating to the bylaws.

MR. COLE: I have a request for a clarification. I don't have any motion or anything. It's about the purpose of the advisory committee. The last sentence says, "We will consider the parameters of reasonable access --" this is Steve Cole "-- reasonable access to personal information and adequate security and will present options --" it doesn't say to whom "-- for implementation of these information practices as well as the costs and benefits of each option in a written report to the Commission."

Is the function of our final report an educational report to the business community and the public about options that are available and the cost-effective way to provide reasonable access, or is it recommendations to the Commission for action that the Commission may or may not be taking in the next few months?

MR. MEDINE: The purpose is not quite either of those.

MR. COLE: Okay.

MR. MEDINE: That is, the purpose is to make a recommendation to the Commission for its consideration of these issues and how the issues of access and security are to be implemented in general and, of course, as I mentioned earlier, particularly with regard to assessing the state of self-regulation and the survey of websites that will be conducted this month.

MR. COLE: Well, that's a very different -- that's a very legitimate purpose, but I hear that as a very different purpose from what's stated here, and if one of the functions of the advisory committee is to be assessing on these two issues the success or lack of success of self-regulation, maybe we ought to be saying that. I guess I'm confused.

MR. MEDINE: Then let me clarify. The point is not for the committee to assess self-regulation. It's for the committee to state what it views as a -- as what -- how access ought to be implemented as far as fair information practices go, and then the Commission will receive a range of views about how access should be implemented, and then the Commission will adopt as its own view which particular view or some combination of views is appropriate for access in terms of providing fair information practices to consumers online.

MR. COLE: This is Steve Cole again.

I'm so clearly supportive of everything the Commission has done over the last few years on this issue that it's awkward for me making these comments, but for what purpose is the Commission going to be stating its views? I mean, this is very important in terms of the nature of the recommendation. You don't have any present statutory responsibility. You may or may not in the future have one. You may or may not make a recommendation in the future.

Is the committee's report designed to help you make a determination of whether you should adopt a legislative or regulatory position?

MR. MEDINE: No, the direct purpose of the committee -- again, maybe I didn't say it as artfully as I should -- is to evaluate the state of self-regulation based on what it learns in its survey of websites. That is, it will learn in its survey of websites, and it will do both a quantitative and qualitative analysis of privacy policies, what access is being provided and what security is being provided on websites or at least what websites are saying they're doing, and this committee's work will essentially give the Commission, whether it's a benchmark or a metric or a means of better understanding, what it finds in the marketplace in terms of assessing whether self-regulation has met fair

information practices.

MR. COLE: Thank you, that's helpful.

MR. MEDINE: Richard?

MR. PURCELL: Richard Purcell from Microsoft.

David, I'm concerned about the last statement in that what we're saying is that this committee's charter is to create criteria by which the Commission may be able to evaluate the compliance with fair information practices of websites.

At the same time, prior to the completion of that work, the FTC will be doing a web sweep, which as you've just stated contains qualitative analysis of the fair information practices as it's currently implemented. I'm confused as to how that criteria that is going to be delivered after the fact will be used within that sweeps ratings.

MR. MEDINE: Well, again, the sweep will assess factually what is going on today, and obviously this committee will in part enrich the Commission's ability to analyze the results of that survey. So, I don't know what more to say other than obviously what people have chosen to do in terms of their fair information practices today is out on the web, and that's what we will be gathering in our survey. That is essentially a fact.

This group will also provide both facts in terms of costs and benefits as well as opinions in terms of the policy of access and security, and then the Commission can essentially evaluate the facts it learns from the survey with the work of this committee.

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

Can you identify past advisory committees that have functioned in this way that we can take a look at in terms of bylaws or reports? I think this is a new process to many of us. Is there a precedent or an example that the Trade Commission can point to that we can kind of look at as an historical precedent for not only consideration of bylaws but in carrying out the work, or is this brand new?

MR. MEDINE: The Commission staff have certainly examined other federal advisory committees' work, bylaws, charters in developing the work of this group. On the other hand, this group does have a unique mission in the sense that it's a relatively short, compressed effort to focus on two very specific issues, but we would be happy to provide you with other agencies' work that. Again, I don't think there's anything --

MR. PLESSER: Is there any Trade Commission precedent?

MR. MEDINE: I believe this may be the first federal --

MR. COLE: I was on a Federal Trade Commission advisory committee in the early eighties -- this is Steve Cole -- and the advisory committee there was looking at possible recommendations for rules to implement or to improve the regulations under the Magnuson Moss Warranty Act, and you have already done a wonderful analysis of different things that are needed, because you've defined consensus here in a way that may work. In the first advisory committee, you defined it as unanimity. So, I know that I don't need to tell everyone that there was no conclusion of that advisory committee.

MR. MEDINE: Well, this is certainly in dramatic contrast to a negotiated rulemaking, for instance, where the goal is for the group to reach a consensus. Really, the goal of this committee is to enrich the Commission's understanding of these issues through a variety of views, and that's honestly why we picked a diverse group of participants in this committee to express their views and to draw on their experience and knowledge and to give the Commission a much deeper understanding of some of the subtleties and complexities of these issues.

MR. TORRES: It's my understanding that the real

purpose of this Commission is really to provide some guidance, and I've worked with some people around the table, and I don't think anyone here is shy about expressing their views, and I think at the end of the day, as long as everyone's views are able to be expressed in the document going to the Commission, it's most helpful for our separate constituencies, as well as to the Commission, to be able to do that.

So, you know, maybe we're focusing too much on -- I think that the purpose needs to be, when it comes to access and security, a little bit broad. I come at it from, you know, my experience on kind of privacy issues, it's been in the financial arena, and that's the view that I hope to express before the Commission, and I'm sure everybody is coming at it from a little bit differently, but as long as we can be assured that those views will be reflected in the final document, I think that might help allev -- I mean, that will alleviate some of my concerns about reaching consensus and doing all these things that consumers in the financial arena would be included in the report.

MR. MEDINE: I can assure you that all committee members' views will be represented in the final report to the Commission.

MS. MULLIGAN: Deirdre Mulligan.

I have a question similar to Ron Plesser's question about just process and previous experiences, and I noted that the subgroups are not subject to FACA, although you indicated that much of the work will go on in those subgroups, and to the extent -- you know, it says that documents should be available, and do those documents include, for example, a responsibility to take notes and make meeting minutes available at meetings?

To what extent -- I mean, as a committee member, I'm not sure whether or not I can serve on every subcommittee, I'm not sure whether even if I could I would have the time to do so, but I'm clearly interested in all of these issues, and I do want to be able to understand the thinking that's behind different recommendations from different subgroups.

MR. MEDINE: Under FACA, the subcommittees are not covered, as you say, and their meetings are not public. What is public, and I think that's where the accountability comes in, is what the subcommittee comes back to the committee with, and the committee will then have an opportunity to fully consider, debate and discuss and do further work on the subcommittee's efforts.

Just a review of what the subcommittees will do after this session is to go back on the issues that we

identify and work out a detailed outline of matters to be considered, but that detailed outline will then be presented to this committee, and if people feel that it's deficient or things should be added or taken off, then the committee will have a full opportunity and the public to consider those views, but just as a practical matter, because so much work is to be done, the subcommittee structure seems to work best.

MR. BATES: Richard Bates, Walt Disney.

First, I want to thank the Chairman and Commissioners for allowing me to be here. I appreciate that very much.

I don't want to dwell on this too much, but the timing of the survey and our recommendations troubles me a little bit, and I'm trying to understand why -- I mean, how that's going to work. Are you going to release the results of the survey on access and security after we make our recommendations, or are they going to be released at the same time? It seems to me you might want the benefit of our recommendations with respect to what the survey is going to say. I don't want to dwell on that, but if you could just spend a few minutes talking about that, I'd appreciate it.

MR. MEDINE: Well, as I said, and it was announced publicly yesterday, the survey will be

conducted this month, that being the actual work that Professor Culnan is intimately familiar with some of the challenges of conducting a survey.

We will then have to analyze the data and present the results to the Commission, and it will be really up to the Commission as to how it deals with the data that the staff produces and how it evaluates that data and when it chooses to release that data. So, I don't think we can say at this point when that will be done other than obviously to the extent that the data's interpreted that the committee will provide a valuable instrument to the Commission in evaluating the results of the survey.

MS. GAU: Tatiana Gau from AOL.

Will there be any opportunity where we will have the analysis shared with us while this commission is still active, this committee?

MR. MEDINE: The results of the survey?

MS. GAU: Yes.

MR. MEDINE: Certainly typically in the past the Commission has publicly released the survey results, and so certainly to the extent that it's publicly released, the committee will have an opportunity to review them. Of course, the committee's proceedings are public anyway, so that would be the equivalent to a public

release. So, that will certainly be in the hands of the Commission, once we complete the survey and have the final numbers, as to how the Commission chooses to deal with that information.

MR. PURCELL: Richard Purcell from Microsoft.

I'm going to raise the horrifying specter of scope creep. I'm concerned about the purpose of the committee being limited to the internet and online data collection. On the flight out here from the West Coast, the inflight magazine provided me with nine opportunities to provide personally identifiable information, none of which are internet based, none of which promise any kind of access or security.

However, what we find in the real world these days is that a lot of offline data gathering is now being commingled with data that's gathered online. I don't understand quite how the committee can define access to data in the online environment in order to make the internet safer when it's unknown whether the data that's being accessed by the data subject has been gathered online or offline.

If I provide my name and address in an offline manner and an online manner and those two records are commingled into an online database, am I equally able to access that information that I provided offline as well

as that information that I provided online? And if you think about the technologies that are available there, if a record is merged and the same data element is provided in the two different records, then edit precedence has to take control of which of the two sources are trusted for the updated information.

If I provide my name as Richard Purcell online and I provide my name as R. Purcell offline and those are commingled and the R of my first name is preferred because of better precedence, do I have access to correct my first name or how is that displayed?

There are some pretty gnarley questions about how the internet will commingle and become the central data store regardless of the collection methodology. If we limit ourselves here to an online environment only, we run the risk of terrific data clashes in terms of policy and ambiguity as to how these rules or these principles that we will define here will actually work in the real world of large technical databases.

MR. MEDINE: Go ahead.

MS. BRUENING: This is Paula Bruening from TRUSTe.

I'd like to second what Richard Purcell has said and give you the perspective just of a privacy seal program on this particular issue.

What we find that companies are looking for in terms of meeting our core tenets of fair information practices is clarity and predictability and some clear guidance on how to implement these practices, and I think that if we limit ourselves in the way that potentially we're limiting ourselves in the bylaws, I think from a seal program's point of view, we're going to find ourselves having to revisit these issues over and over again.

We are looking to expand our program beyond just information collected through a website. We plan to do that in our software program that we're working on right now. And over and over we're finding that these lines are becoming more and more blurred, and what is offline and what is online is very, very difficult to distinguish.

We'd like to come up with some guidelines that we can take into the future and that will serve us and our consumers and our companies as the internet continues to change and evolve over time.

MR. MEDINE: Thanks.

Other comments? John?

DR. KAMP: This is John Kamp.

I'm sort of putting myself out here for the moment, I'm a former member of the FCC, and I'm sort of

putting myself in the position of -- well, the ideas here expressed by the last two speakers are very interesting, and I think they bring up important points, but that it's really not scope expansion. That would be scope explosion, I think, for this committee, and I think the issues are just way outside of where I think the agency intended to go and essentially outside of even why the rest of us came to the table today, and I just don't think we can go there.

MR. JAYE: Daniel Jaye, Engage.

I'd just like to comment that I actually agree with the colleague from Microsoft that it's very hard to separate out this issue of commingling of offline data with online data. I think that there's a lot of concern about that currently and that if we don't at least consider some of those implications as part of our process, then we may miss addressing one of the fundamental issues that will affect consumer trust.

DR. PONEMON: Larry Ponemon, PricewaterhouseCoopers.

Again, Richard, I agree completely, and I think if we don't look at the issue, we are short-changing the consumer. In my experience, we do a lot of audits, a lot of privacy audits, and a big problem is commingling. It's the appending and reverse-appending

problem. So, if we don't deal with that issue here, we're not going to add any value in my opinion.

MR. MILLER: Greg Miller, MedicaLogic.

We are dealing with a very similar problem over at HHS right now dealing with privacy and regulations for health care data, and I think we have to balance, Richard, the issue of scope creep with what we're trying to accomplish here, and the way we're dealing with it over there is that if data ever ends up online, then it becomes protected health care information.

We may want to consider an analogous approach here that our focus is on the data that ultimately ends online. How it gets there is another matter, but once it gets online, that's when we want to make sure that we have the mechanisms in place.

DR. LANCE HOFFMAN: Lance Hoffman, George Washington University.

I don't think it's scope creep at all. I think we have to deal with it. Most of the previous speakers, not all, have agreed with this. It is not appropriate to not deal with it. Even better, the purpose -- we don't have to change the wording. If it isn't broke, don't fix it. It says, "providing online consumers reasonable access to personal information collected from and about them." It doesn't say how or where. So, this

wording is not broke and needs nothing fixed.

MR. MEDINE: I guess from the point of view of your designated federal officer, I would agree with that in that that's, of course, one of the advantages of having you come in and tell us what's on your mind and what your concerns are, is that if you think there's an important nexus between online and offline, then that's an appropriate matter for this committee if it chooses to discuss it. Obviously there's a nexus to online or we wouldn't be here, but if you think it's a broader issue, I think it's certainly within the committee's purview to address that or have particular members address that issue.

So, I don't know if there are any further comments on that particular matter, but I think it's clearly within -- that's why we have the advantage of seeking outside views and a variety of views as people will express their views on this subject as something that only the to I think what clearly is within the scope of this group.

MR. PURCELL: Richard Purcell.

Just to close out, my concern in the last two comments would simply be that we have to be cautious not to provide a safe harbor for companies to exhibit bad behavior around protecting personal information by not

putting it in an online environment. I agree, Gregory, with your statement, that it's great when we commingle it, then it becomes subject to online rules, but if I want to not play according to the rules and the rules are that tightly constrained, then I simply don't commingle the data, and that data that I have, which may be duplicative of what I have online, I may be able to play with that data in a way that's not specific to the purposes for which we're gathered here.

MR. MEDINE: Can I just maybe phrase that another way, which is for purposes of this group, one of the issues that we'll address -- and we are going to turn to this fairly soon -- is setting up what issues under access that you want to consider. One issue that the group may well want to put on this list is whether when you get access to online information, you also are entitled to access to offline information, as well, as part of the question of the scope of access, which is a central issue for this group's consideration.

MR. COLE: Steve Cole.

I thought I was going to say that I was really surprised to hear this described as scope explosion, and the reason I was going to say that is because when we developed our policies with the 25 or 26 industry representatives, many of whom are in the room, we came

out with the answer that if the data is commingled, that it's available for access.

But now, having Richard raising the legitimate concern about what happens when it's not commingled and there's data collected offline, that seems like scope explosion. If we're going to talk about access and any other privacy protection practices on purely offline collected data, it's probably very worthy of the Commission to do that, but it's a very different task than talking about data that may be commingled where separation is impossible. So, I would be cautious about opening up too far.

MS. MULLIGAN: Deirdre Mulligan.

I wanted to build on a comment made by Greg Miller. I think perhaps what -- at least part of what Richard is getting to is the storage component, and while information may not be collected online, it may be stored in a system that looks identical, and actually at HHS it's not online, it's electronic.

MR. MILLER: Electronic, correct.

MS. MULLIGAN: And, in fact, it would warrant changing the wording a little bit, but it would get at the intent of what was said on this side of the table and to what Richard was reaching for. I don't know if there's responses to that.

MR. MILLER: Greg Miller, MedicaLogic.

Deirdre, you're correct, I wanted to make a modification. Actually what we did over there is we said electronic so that we could cover the situation where protected health care information would just be taken offline and gathered another way, basically relying on paper records, and I think Deirdre will agree with me that what we have over there is a situation whereby if anything is even faxed or ever created in electronic medium, then it is construed to be part of that domain. So, I agree that we probably can take this up as we get into considerations of access means.

MR. PURCELL: Richard Purcell.

And you're right, this may require some follow-up, and we may be in a stepped process here. I think that the reason we're here today is because of electronic data storage. The best protection information can have is to keep it on paper, because it's so dang hard to do anything with it at that point, but very little information is not stored electronically, and that that is not stored electronically I'll grant may be outside the scope of the Commission, because I don't want to think about that stuff.

But what I'm worried about is the retail

information that has to do with purchases. That's all stored electronically, it's -- your records are updated electronically in realtime often, the databases that are kept electronically, again, within, you know, major corporations that have affiliates and all that data becomes commingled in some way or other in order to develop, you know, meaningful, beneficial customer relationships. If we simply say that this is about access to data that's stored and security to data that's stored electronically, well, a scope explosion has occurred at that point.

MR. WADLOW: Tom Wadlow, Pilot Network Services.

I want to expand on that just a little bit. I mean, I think really the essence of this is that there is no real qualitative difference between online and offline data. The qualitative difference is that online data is so much more easily abused, but offline data can be abused, too, just it's a lot more difficult, and I think that's a -- you know, they really are the same thing, and it's very important to keep that in mind.

DR. SCHUTZER: Dan Schutzer, Citigroup.

I don't think that's quite accurate. We keep everything electronic, but when we say electronic, I mean, word processors, correspondence with individuals

that you don't maintain in a database. I think what we're talking about is addressing the commingling of information, the information that we have on online databases which are practical for us in an online manner to provide access to, not necessarily everything that is, quote, "electronic" on Palm Pilots, on digital recordings of voice, for purposes not for storage or use or database marketing or electronic word processing, correspondence. You can consider that, but it does enlarge the scope significantly.

MR. WADLOW: Tom Wadlow.

I agree it does enlarge the scope. I do want to make a comment, though, that one of the common things that happens on the internet right now is a lot of what you might term data mining, where people go off and look through documents for e-mail addresses and things like that to use for various purposes that were not the intention of the original document. So, I mean, yes, online data has a number of different forms, and it certainly has a number of different intentions for original use, but, in fact, once it's there, it's relatively easy to grovel through it and extract the information that can be used in ways very different than was intended.

MR. WHAM: Ted Wham from Excite@Home.

I've been a database marketer for many, many years. I actually know Mr. Purcell from Microsoft from a prior life. When I entered the internet space about four years ago, I was struck by the fact that there's two sets of rules, and I think that we should, you know, kind of take that out of the closet and put it right up on the table.

A lot of the information practices that happen within the internet space are not dissimilar to the information practices that happen within the direct marketing world, but there's a higher standard, and it's not a higher standard that necessarily you look at it and you go, this is what I would choose to do as a logical step, but it is a higher standard which is being required by the public at large.

There is not generally a requirement in the direct marketing world for consent. I don't sit down and say, you may take my warranty information for product X and share that with company Y, but it happens all the time. I don't say I would like to receive information from cataloger Z, but it happens all the time.

In the online world, I simply don't have that freedom. I have a situation where there's a higher standard, and I think we should look at what the

committee's responsibilities are. We are the online committee on -- we are the advisory committee on online access and security. That online word is critical to it.

One of the key things that we can do here as an advisory committee is help point out to the FTC in that role how the offline activities are really making a difference in the online world and how the government is looking at, you know, implications of that and is missing the big guy underneath the closet, the online activities, and how they're impinging on both of those.

But I think that to look at all electronic information storage would be well, well beyond the scope of this group, well beyond the expertise of many of the members here and beyond what -- you know, I'm terrified as I look at my watch and see that it's 10:00 that, you know, we have four meetings, and if each one ends at 1:30, you know, we're not going to get done what we have on our plate, let alone expanding to this very, very broad definition.

MR. MEDINE: I don't know if it's any comfort, but the future meetings will be day-long meetings, but I'm not sure that does solve the problem you present.

I would like to address some of these issues, but I'll let Ron Plesser go next.

MR. PLESSER: Maybe in an effort to move things along, I just want to get back to where Lance was, because I think what he said was exactly right. I think this is a conversation on the bylaws, and I think the bylaws adequately describe the purpose. So, I think that all of this discussion is very important, but this agenda item is the adequacy of the bylaws, and when everybody's complete and ready, I'd be happy to move, you know, for the adoption of bylaws so that we can go forward, but I think that I agree with Lance that I think the bylaws, as you drafted them, adequately gives us the scope to discuss or not to discuss some of these elements. So, I think it's a very worthwhile conversation, but I think the bylaws are --

MR. MEDINE: Yes, I would agree, and I would even state further that the charter of this group, which has been approved by the administrator, General Services, as well as the Federal Trade Commission, which we cannot change here, is focused on the online context, but obviously the nexus between online and offline, if the group chooses to find it relevant, would be an appropriate matter for the group to consider. So, I guess I would be happy to entertain a motion for approval of the bylaws as modified by the first motion that was made.

MR. CATE: So moved.

MR. PLESSER: Second.

MR. MEDINE: All in favor, say aye.

All opposed, nay.

Remarkable unanimity. Let's hope we can keep it up as we move forward. Thank you.

Let me just -- a few more housekeeping matters before we I guess resume the discussion of some of the issues for us. The --

MS. BERNSTEIN: And there are no amendments to the housekeeping rules, right?

MR. MEDINE: None will be entertained.

Okay, well, further housekeeping, just again to keep the group focused is the report to the Commission is due May 15th, and again, I really want to emphasize that unlike a workshop where you get to say your piece and go home, the real work is done after the meetings in terms of actual drafting of documents. So, we should really always be moving toward the goal of preparing a final written report by May 15th.

MR. PLESSER: Ron Plesser.

Technical question. The written materials and the report, is there any restriction on the federal side, on the federal officer and his staff writing, or does it all have to come from the advisory committee

side? Is there any guidance on that? No, no, no, of who writes the draft? Because somebody told me there was a limitation, and I'm not sure that I think there is.

MR. MEDINE: Well, first of all, I'm pretty confident there is not a legal limitation, and secondly, the whole point of this exercise is for this group to express its views to the Federal Trade Commission. So, I don't think it would be appropriate for the staff to essentially edit or craft your views. We'd like your views to come from you.

Again, to emphasize the point made earlier, we're not seeking unanimity, and that is, there could be 40 different statements on each of these issues, and that's fine, but the writing should be done exclusively by this group. Again, we will provide the support staff to get things copied and prepared and collated and finally printed, but we are really looking for the input of the members of this group.

MS. MULLIGAN: Deirdre Mulligan.

I just wanted to make clear, so, the responsibility for writing this report rests on the shoulders of the people on the committee.

MR. MEDINE: Absolutely.

MS. MULLIGAN: I'm the person who raised the

concern that Ron was talking about, but that was my understanding.

MR. MEDINE: No, the report writing absolutely rests on the committee's shoulders, and we will give you encouragement in that effort. There's no extensions.

MS. MULLIGAN: In case you didn't know what you signed up for.

MR. MEDINE: That's right. No, this is very much of a working group.

MS. BERNSTEIN: Can we give them a page limit at least?

MR. TORRES: Absolutely not.

MR. MEDINE: With this group, we would have to specify font size and margins.

Okay, I would like to note for the record that David Ellington and Rob Goldman are here. Do they acknowledge their presence?

MR. ELLINGTON: Here.

MR. GOLDMAN: Here.

MR. MEDINE: Okay, thank you. Thank you very much.

Again, really just to reiterate that the report is going to identify key issues regarding access and security. It should reflect options. What we hope to do, again, by the conclusion of this meeting is really

start the drafting of the outline for the report. We're back in college again and we're starting with outlines, but I think the outline process will be helpful in really laying out the issues for the group so the group can consider whether they're heading in the right direction and whether all appropriate matters are being considered.

Again, I would encourage the group as it moves forward in its drafting to consider the comments that are made by the public to the committee as well as the committee's own deliberations.

We're ready to move on to access unless people feel a need for a break, but I'm ready to jump in if you are to -- okay, why don't we -- what I propose to do in the next -- an hour for access and roughly an hour for security is to do essentially issue spotting, to try to elicit from this group what are the key issues you see with regard to each of these issues.

This is not necessarily the time to debate those issues, but it's mostly what does this group want on the table for its consideration, and then we will conclude by creating subgroups around the general issues that are formed so that subgroups can then flush out these issues in more detail.

So, if that's acceptable to the group, Hannah,

our able staffer, will be taking notes of your thoughts, but I would really open it to the group, starting first on the question of access.

What matters ought we be considering or ought you be considering when it comes to access issues?

MR. PURCELL: Richard Purcell, Microsoft.

We've done a bit of thinking on data access issues, and we have quite an extensive list, but first of all, I want to clarify that this is really hard work. This is really difficult stuff, because what we find is that there is layer upon layer of granularity and difficulty that becomes intermeshed one with the other, not only within the question of access, as an example, but across all the principles, and we'll find that or we do find that notice and consent are tied into this, and we can't ignore the intermeshing and the layering of this.

With that said, the first question about access that comes to mind is, of course, to what? What are we talking about accessing? What we don't have as an industry standard but what we have been able to construct within some of our different businesses are definitions and categories of data, from personally identifiable to nonpersonally identifiable to behavioral, transactional, inferred, derived, and I'm

sure others, other categories. Those are examples of it.

We also, of course, have to look at the issue of commingling from multiple sources, whether online or offline, and it increases the rules. It becomes difficult. When we get into access, we have to actually get into some database systems administration issues on the business rules that control that. So, if you're guaranteed access to information and the system has essentially obliterated some of your information because it's commingled it, and I've said, you know, I've said essentially, to use an example, I say if I work in a business of, you know, one to five people on one online forum and one to nineteen on another forum, only one of those values is going to survive. So, the question is I don't have access to both of my data points that I've provided. One's been eliminated in favor of another.

We also, of course, have to address methods of access in addition to these data definitions, but again, getting back to certain categories of data, methodology matters. The ability to correct or edit, again, applies to data categories. We're not going to allow somebody to alter the credit card number that they used in a transaction. That's a fact. That's a record that we can't corrupt, and it almost -- and here we start

layering with some security issues, as well.

We can't let a customer say, you know, I want to look at my order, and no, I didn't order three of those, I only ordered one. No, you ordered three and we delivered them and that's how it is. So, there are things that are alterable, but there are other categories of data that may not be.

There is also, you know, again, what rights does somebody have, what special rights to editing against these different data categories? Certainly some can be flexible. I can change my personalization data. I've said I want the color blue and certain stock quotes and da-da-da-da-da, those personalize my page and provide me a benefit of the web experience, and those certainly are, you know, can be editable, I would think.

MR. MEDINE: If I could at least summarize where we are so we have some of these categories in mind, access to what information, which would include transactional information, behavioral information, methods of access, and I think we may want to flush out some more categories of information, and you raised the issue which we discussed earlier, commingled data, and then ability to edit and correct, just so that the group can follow along. Is there other --

MR. PURCELL: One last point, if I could, and

I'm sorry, it's a list, we've got a list here, but authentication becomes an access and a security issue. So, it's not just access to what, but access by whom, and if we commingle data, which means we didn't necessarily gather it online on a primary basis, we gathered it offline, how do you identify the individual who submitted that data if they didn't use an online password and ID pair to get access to that?

And worse, if you have public data that you didn't gather from your data subject at all, that you got from a third party in some way or another, how do you not intrude on their privacy and yet still authenticate them?

MR. MEDINE: Okay, thank you very much.

DR. CULNAN: Mary Culnan.

Two issues, I want to first second the issue that Richard raised in terms of looking at the relationship between access and notice, because I still believe some of the access issues can be resolved by -- or concerns, I would say, by much better notice.

Another issue which I think is very important is what data at what cost, how much do you have to pay for access. I don't think there's necessarily a guarantee that access is always going to be free.

MR. MEDINE: Okay, thanks.

MR. PLESSER: Well, I think one issue that fits in with that is -- I guess from my past experience at the Commission -- Ron Plesser from Piper & Marbury -- that we should put in is essentially a sliding scale concept, which is, you know, is all access of sensitive data, nonsensitive data, different types of data, do the relative requirements and burdens of access shift as to the nature of the data, not just the costs alone, but, you know, is there some data where access is more -- some relationships where access is more important or would justify more cost than others?

So, I don't know how you want to summarize it on the list, but sliding scale is not a bad way.

MR. MEDINE: Okay, again, without necessarily getting into it right now, what I hear you proposing is one of the things that the group consider is are there certain categories of sensitive information, for instance, or decisional information that there might be greater access to as opposed to other kinds of information?

MR. PLESSER: Right.

DR. SCHUTZER: Dan Schutzer.

I'd like to second the categories, although I have to give some thought to what is really computed and combined and how it's derived and it's stored.

I also emphasize or will second the idea of the authentication. If anything, you might even want to consider the need for stronger authentication/ authorization to have access to information that would be much more comprehensive than the individual items you would have in the transaction. You want to safeguard that a lot more.

In fact, you would have to be concerned about the authorization, because sometimes the data's combined in ways which an individual might not be authorized to see it all, perhaps storing a transaction which consists of both parties' account numbers. I certainly don't want one party to see the other party's account number, and information private to that other party, they wouldn't be allowed to see that, even though it's stored online as a complete transaction history.

MR. MEDINE: Just again maybe to clarify it, authentication goes to a couple of issues. One is are you who you say you are. The second is the data that you seek access to data that relates to you. And third is are you entitled to see all of the data that may be part of your transactional record.

DR. SCHUTZER: Yes, and the other concept of the transaction, if I'm collecting data but I'm combining it in ways that some of that data is destroyed, it's the

data that I've combined that's relevant, not the data that I've collected on a temporary basis in cache and no longer maintain.

MR. WHAM: Ted Wham from Excite@Home.

Two issues that come up is, first of all, validation for an anonymous issue, so providing access to information that you've computed about individuals.

The second issue that I would bring up is in terms of the categorization of data, as you come through some of that data, if you get it wrong, so, for instance, the example that was brought up before, if an individual says they bought one and you know they bought three but you're wrong, what rights and what responsibilities does the customer have or does the company have to correct that type of information?

MR. MEDINE: Art?

MR. SACKLER: Yes, Art Sackler of Time Warner.

I think we have to take a look at frequency of requests, should there be any limitation. Getting back to Rick Lane's point from before, if we're looking at technology, it should be technically feasible and economically reasonable to be able to respond to access requests.

And on commingling, if we do go that way, I mean, what actually constitutes commingling? I mean, is

it merely the merging of the data, or is it the situation as happens in marketing situations, where you take some online data and then you take a slice of what you've taken from offline, marry it up and then do the marketing? I mean, is that commingling, as well, and how would we handle that?

MR. MEDINE: Can you flush out what you're referencing in terms of technical feasibility? What kinds of issues do you see arising in that context?

MR. SACKLER: Well, I think we have a lot of technology experts around the table, and all the rest of us have access to them --

MR. MEDINE: Maybe I should pose it to the larger group, then, in terms of technological issues, are there subsets of that that we ought to be explicitly considering?

MR. HENDERSON: Yeah, that was one of the comments I was going to make where I want to second the comment that -- oh, Bob Henderson from NCR.

MR. MEDINE: Thanks.

MR. HENDERSON: I want to second the comment that the whole relationship of access is directly correlated to the issue of notice and choice, and then looking at the technology issues, I think it has to do with time of response by the businesses back to the

consumer, because we have to address the issue that being an online advisory committee, you could get into the issue of characterizing the issue of giving instant response because of the online capabilities, but that may not be prudent because of the cost implications to businesses. So, I think you've got some technology issues in how you manage the response, and the time period of the response back to the consumer is very critical.

I think there's been a mention of the derived, but I think that's a separate category in itself, in the derived data, for the simple fact that you've got a lot of businesses that are going to have third-party relationships, and data is going to come about from third parties where the consumers won't have any indication of what data is being accumulated to calculate the derived model on them. So, that gives you complexities of access. So, I think the derived issue has to be addressed.

MR. MEDINE: Would you agree that put another way, the derived information is what information did you get from a consumer and what information do you have about a consumer as two potential issues to consider?

MR. HENDERSON: I think that gets closer to the issue of addressing derived data, yes.

MR. MEDINE: And whether you should have access only to the from data or the about data, as well.

MR. HENDERSON: But there is also the issue of who owns the result of the derived data. Does the business own the result because they put forth the effort, even though it came from multiple sources, the consumer and other third parties, or does the consumer have rights to see that result because it is about the consumer? So, I think that's another issue.

MR. MEDINE: Okay.

MR. GOLDMAN: Rob Goldman.

I think you have to be careful when you talk about derived data, because there is data that is, as you say, about. There's also data that is just simply aggregation. That is also a way of deriving data. I suppose it's a subset of the categorization issue, but we have to talk about at what level of detail do we provide access to data?

Several of the companies here collect vast amounts of high-volume data, clickstream data, other huge volumes of data, and it's very expensive and difficult often to provide access to the detailed information but much more reasonable to provide access to aggregated information, which is another form of derived data. So, it's an issue.

MR. MEDINE: Again, just to clarify that point, if a consumer's information is captured in some fashion and that information is made part of a larger set of aggregate data, should the consumer have access to aggregate data of which their data became a part?

MR. GOLDMAN: It's also -- and maybe this gets back to the sliding scale and sensitivity issue, at what level is it reasonable to provide access at the detailed level? At what levels are aggregated access acceptable?

MR. MEDINE: Okay.

MR. DAVID HOFFMAN: David Hoffman, Intel Corporation.

Fearing scope creep, I think we are going to have to discuss the user's perception when we talk about access here.

MR. MEDINE: So, how long is the data kept, so if I seek access to information, will you still have it on file when I seek that access?

UNIDENTIFIED SPEAKER: And also how long the user would expect that information would be retained.

DR. JONATHAN SMITH: Yes, Jonathan Smith.

I want to emphasize that issue. I think that's one of the most important issues here. I mean, I think we've all seen examples of cases where information has

surfaced, you know, from unexpected -- from unexpected corners, and I think that expectation is a really key issue here, because I don't think people fully understand that once something's on disk, it's there forever, and they don't understand that it's easy to move, and, you know, so you give away something at one transaction, you think it's over when the transaction's over, but it's not, and I think that expectation issue is absolutely key to what we're trying to address.

MS. WHITENER: Rebecca Whitener with IBM.

I just want to also agree with that statement about data retention. I think it ties in also to some of the comments that have been made about the association between the notice and the access issue, so that there is an awareness of what -- about these retention policies and what we're talking about.

I also believe that as -- and I agree with many of the issues that are being raised here as issues that we should look at for access and what -- after we look at the full exhaustive list of actually what types of information can be accessed, and then applying that reasonable type of definition around that full list.

And then, of course, as we go from there, looking at our charge, to also consider in light of the reasonable access, to then evaluate the costs and

benefits of each of the issues that we are looking at.

MR. MEDINE: Ron?

MR. PLESSER: Ron Plesser, two quick points.

One is I think availability from other sources. The debate that we find ourselves often in in the public record and the IRSG is if information is available from another source, does that in any way lessen the database requirement?

And just a word to put up on the list, which I think has kind of been covered but which is a consideration of the proprietary nature of the information. I think it's been referred to in different ways, but it's easier to talk about at least on the checklist of what's the proprietary value and how do you separate that from the information that is valued by the information.

MS. MULLIGAN: I want to highlight three things, Deirdre Mulligan.

First, when we talk about access, people very frequently just jump into what should you have access to, and I think it's really important to understand that there are reasons for access, that information is being used to make decisions about individuals, whether it's what they see -- that this is not a superfluous thing, that individuals really do have an interest in what's

going on behind the scenes, why they might be getting certain things and other people are getting other things, is that limiting their opportunities, and so that, you know, there are real due process type concerns here, that this is not something that privacy advocates just demand and there's absolutely no reason behind it; that there are, in fact, reasons.

MR. MEDINE: Just to clarify that point and something that only the to a point that was made earlier, and this could be part of the work of the group, but consider whether the statement you made in terms of the need for access depends on what kind of information you're seeking access to and how that ought to be played out in terms of evaluating when and where you get access.

MS. MULLIGAN: Um-hum, I think there are many considerations, but to understand that access is the -- that there are purposes behind access, that there are, you know, that there are reasons for it. You know, somebody didn't just make it up one day.

And the second being that in the costs and benefits area, that I think people generally are thinking about the costs to businesses and the benefits to consumers, and I really want to push on that notion and say that there are direct benefits to businesses in

allowing customers to access information. There is nothing worse for you than having inaccurate data that isn't particularly useful or outdated data, and that to consumers, you know, there are real costs sometimes to accessing data, and we know in certain areas it costs money and that we do need to make sure that if there are costs associated, that they're not prohibitive, that accessing your information shouldn't be something that only the wealthy have access to.

MR. MEDINE: Thanks.

MR. TORRES: Frank Torres, Consumers Union.

I'd like to reiterate some of Deirdre's comments and to add upon them. I mean, what -- from the consumer perspective, you know, it's how do consumers make decisions about who they do business with, so notice becomes important, as some people have said, but access becomes important, too, and the ease of access for consumers to get in.

In the offline world, we've got the Fair Credit Reporting Act, which gives consumers access to the information that credit bureaus have about them, and it requires that, you know, that there's a system put in place that makes it easy for consumers to get in or it's supposed to make it easy for consumers to get in and to correct that information. Why? Because that

information is used to make decisions about them.

I'd recommend that some of us take a look at the recent privacy -- direct privacy rules in the financial setting that were just published yesterday by the OCC and the Federal Reserve Board that talk a little bit about the scope of information. Of course, that really doesn't get into the access, but at least you're supposed to be told that the categories of information that are collected about you and the categories of people that that information gets shared -- that that information gets shared with.

I think ultimately we will get to the access question in that sense, because decisions are being made that affect your creditworthiness, the availability of products to you. So, it's important for consumers to have an ease of getting to it to correct it, and I think when the internet first became real popular, I heard some stories about people actually providing false information, which, you know, if you're a marketer and you're gathering this false information, I doubt that that would help you very much, but to give consumers the ability to correct the information in an easy way.

MR. MEDINE: And just to clarify one of the points you made in terms of notice, I assume what you're referencing in part is that what you have access to, it

would be helpful to essentially have notice of what was collected so you know essentially what you're seeking access to and what you have access to.

MR. TORRES: And what's the purpose of the information.

MR. MEDINE: So that the two fair information practices are something that only the in that way.

Dan?

DR. SCHUTZER: Dan Schutzer.

I think one of the things we might want to discuss is the whole concept of agent technologies, aggregation technologies, and when you provide access to those technologies, what happens to your relative liability and so forth as they pass from different parties, who are you required to send the information to, whether you have any kind of responsibility as to whether you send it to another software program or agent. I think that would be worthwhile discussing.

MR. MEDINE: Just to clarify, are you talking about agents, A G E N T?

DR. SCHUTZER: Software agents and services.

MR. MEDINE: Could you clarify?

DR. SCHUTZER: Since the last time we met, technology is making it more possible for me to have an agent that can store my various PINs, that can go to my

various sites, extract information from multiple financial sites or medical sites or somewhere else and provide as a service better comprehensive views for the consumer. So, I think what we need to discuss is the advantages of that, the risks of that, the responsibility of somebody that's maintaining that information and providing it not directly to the customer. Do they even know if they are providing it directly to a customer or if they are sending it to an agent? And what happens to the liability if I'm releasing that information through a software agent?

MR. MEDINE: Does this include -- in the software areas things like scrapers?

DR. SCHUTZER: Screen scrapers, that whole category. It's worthwhile discussing and elaborating on.

MR. LANE: Rick Lane with the U.S. Chamber.

I agree, Frank, that ease of access is critical, even from a business side, in terms of having your customers happy. You don't want to get a lot of complaints, but at the same time, where the concern is is when you have ease of access, sometimes you have less security, and so there's a balancing there. What's the liability a company faces where there's ease of access, someone breaks into someone's home computer,

gets the codes and the information? They know everything about it not from the individual, not from the business, but from their own home computer, and then they access it.

The company authenticates it, because we're trying to keep the barriers low to accessing, and all of a sudden the customer sues the company because of information that was gathered from other sources to break into that company. So, there's a balancing act there. So, we have to make sure that we're looking closely at ease of access but also maintaining security that will protect the customer's information at the same time.

MR. MEDINE: Okay.

MS. SWIFT: Jane Swift.

I think to build on the user expectation of storage as well as how the utilization of the information goes, I think it's going to be important for us as we discuss access to address what consumer understanding is or technological sophistication of consumers are, because while this group may have a great deal of knowledge about what agent aggregate technologies are and how you're utilizing the information, I'll speak for the "internet for dummies" group that can say that it is hard to have informed

consent, notice or access if you have absolutely no comprehension of the capabilities of the technology, and it is hard, for example, to opt out of something that you don't know exists.

MR. JAYE: Two points. One is that it relates to definitions, but we talk about personal information and a definition of personal information. What constitutes personal information is going to be very important to this discussion and probably will inform it.

The second thing is, we actually talk about this in the bylaws, about collection of information, and I'd actually like to point out that that may not be a serious issue. My analogy is somebody throws me a baseball. If I don't raise my hand, it hits me on the chest and falls on the ground. Did I collect that information? I think we would agree no, but there are scenarios like that on the internet where you get IP addresses as part of the way in which the web works, but if I never touch it, and perhaps it's by using a third-party proxy server in the middle, I never even see it, the question is did I collect it.

Then we go to receipt. There's a number of stages. There's receipt, there is collection, there is storage, maintenance, and that we really need to look at

how data is handled as we look at this issue, because, for example, if I don't have the data anymore, then I can't provide access, and that does relate to the retention issue, as well.

MR. MEDINE: It sounds like we'll be delving into some philosophical issues, as well.

UNIDENTIFIED SPEAKER: If a database falls in the forest, does --

(Laughter.)

MR. COLE: Steve Cole.

I think there are two bullets we have that I would like to see refined a little. One of the very earliest ones was data at what cost on one of the first sheets. There's cost to the business, and that raises a lot of the questions we have been discussing in terms of the cost-benefit balancing, but there is also the question, can fees be charged for the access, and if so, how do you determine what they can be? And I think you should have that as a separate -- it's kind of -- there's a whole collection of issues of terms and conditions. We mentioned frequency, fees and others, and there may be still others.

The second one that I think needs clarification comes from the good point Deirdre made earlier. It wasn't so much as a question, she was saying that we

ought to all remember that there are good reasons for access, and I think the question that comes to my mind that needs to be asked and answered is could the consumer's reason for access be a basis for granting or denying access? I have my own answer to that, others may have theirs, but there was a lively discussion in our steering committee on that, and I think this group should consider it.

MR. MEDINE: Just to clarify, you mean the --

MR. COLE: Well, can you only get access to correct data, and if that's true, do you have to show any reasonable basis to show there's an error, or can you have access for access sake, because that may promote other values and other benefits? We are not going to debate that now, but I think that's the point I'm raising. Can your reasons for access be a limiting factor in whether or not you get access?

DR. PONEMON: Larry Ponemon, PricewaterhouseCoopers.

Going back to what you said, Jane, I really commend you. I think there's something real basic here. There are three ethical principles on the table concerning access, at least in my mind. One is awareness. I mean, I think consumers are complacent. They don't realize how big the problem can be, and not

where it is today, but where it can be, so I think awareness is very important, and that concerns awareness to access and awareness of the type of information that's used.

The second ethical issue is just accountability. What kind of accountability do we want to impose on business, and what kind of accountability do we want to impose on consumers? It's a two-way street, and I think we need to remember that.

And the third issue I think was addressed, is the whole issue of accuracy. Unfortunately, accuracy is not a zero-one game. We see this in the credit world. You know, sometimes something that is -- looks like a -- looks like a mouse may be an elephant, and the bottom line is we might not be able to find, at least within this group, whether something is defined -- within a degree of reasonableness whether something can be defined as accurate.

So, I'd like to get to the ethical tenets, and I think awareness, accountability and accuracy will be fundamental to the access question.

MR. MEDINE: Lance and then Deirdre.

DR. LANCE HOFFMAN: Lance Hoffman, three points.

First, following up your point on

accountability, I think it's important to examine all sort of transaction logging and a, quote unquote, secure evidence chain. Two examples of this: One is when a consumer or somebody makes a request for access, respond to this in tracking, how do we know what went on and when, so tracking. The same thing is with agent logging, same thing, what were the agents doing? To the extent we can have a reasonable flight recording of what went on, we'll be in a lot better shape in terms of having the appropriate balance struck.

Two other points. One is on identification and authentication, I think we want to be careful that we keep in mind the implications of this for anonymity dilution. The tighter we get in terms of ID'g people, whether there are passwords or biometrics or whatever, we get more and more towards the fish bowl society, and again it's a balance striking there.

Third, Ron raised the issue of a sliding scale, perhaps. I think it's important to not necessarily -- to understand -- we may or may not go to something like that. We may have to suggest a top-down solution in many cases. On the other hand, there may well be in many cases individual definitions. Right now, the user, do you want a blue screen or a green screen? No problem. In many cases the user can decide. It is not

guaranteed that some other organization has to decide. We have that capability.

MR. MEDINE: Deirdre?

MS. MULLIGAN: Deirdre Mulligan.

I actually wanted to add onto Paul's point that I think when you look at access, particularly in our current environment, it does play a very important accountability role, that it is a check on are people actually abiding by their notices, you know, is what's in their database actually what they said they were collecting? So, that's why I think it's important to look at the reasons behind providing access.

And I also wanted to raise the comment that was made by Mr. Hoffman about authentication in that I think authentication is a critically important issue here, but in our, you know, seek to have perfect authentication, we don't want to have perfect annihilation of anonymity, and figuring out how we thread through that is going to be tricky, but it does go very much to the notion of what is personal information and ensuring that personal information -- what's required to make decisions about people in the offline world is not the same thing that's required about people to make decisions about things in the online world.

We have things like unique identifiers. They

substitute for names and addresses. So, thinking about how we ensure the same principle, which is information that's used to make decisions about people. We have to not necessarily get stuck in these definitional barriers, carrying offline processes into the online world. It's important to use them as barometers, but I think we have to look at the environment in which we're dealing with it.

MR. MEDINE: I think you raise a good point, among many interesting issues, the balance between authentication and access. If you set the authentication standard too high, you may not get access to your own information, which is interesting.

We have got a lot of folks over there. Let's start with Lorrie.

DR. CRANOR: Hi, Lorrie Cranor.

Following up on what Deirdre just said, I think there's a big question as to when data becomes applied to an individual, and there has been many debates as to whether say an IP address is personally identifiable information, and I think we need to look at that as a specific example. There are a number of specific examples and also more general cases as to when you should be provided access to that data.

Another point had to do with what sort of access

should you have when data is shared. If I make an online purchase, I should have access to the data that company has, but what about the delivery service that also has my data now, should I have access to the data they hold on me? As we're talking about the online versus offline, the delivery service may not have the online data, but I think that is perhaps something that I might want to have access to.

MR. MEDINE: Andrew?

MR. SHEN: Andrew Shen from EPIC.

To return to an earlier point, I think it's important to highlight the points of accountability, because I think one thing we're wondering is whether there should be legally enforceable standards on the information you should have access to. I think returning to a point that Lieutenant Governor Swift made before, I think this would help consumer awareness if they were assured that there was a baseline standard for what they can expect out of the internet companies they deal with, and that if such standards are in place, what processes should be put to oversee that standard, to perhaps levy penalties on companies that violate it?

MR. GOLDMAN: Rob Goldman, Dash.com.

Just two points that are subtleties on the agent issue, which has come up a couple times right now.

Dash.com makes -- actually, our product is an embellishing agent, and one of the issues is we allow that agent to make decisions on behalf of the customer. So, getting back to the point that was made earlier about decisions are being made on behalf of the customer, based on information, the specific information is the webpage that we're visiting at the time, that we as a company and certainly our database knows nothing about. So, how do we provide access to information on which we made a decision that doesn't exist anywhere in our controllable realm?

And a point that was made earlier is this question of agent logging, whether or not it's important to keep track of all of that information, sort of requiring collection in a way, and if we do such a thing, in what time frame is it reasonable to offer access? Since this is all digital and on the internet and electronic, it seems as though everyone assumes access should be immediate, and I think that's an assumption that's very difficult to deliver in practice. So, the time frames in which we must offer access, at least, is a major issue that we're trying to work out. So, I imagine we're not the only ones.

MR. MEDINE: I know there's been a number of comments about consumer understanding and notice, and

maybe those all relate to giving notice when there isn't information collection so that there's not a false expectation of access in that situation.

Josh?

MR. ISAY: Josh Isay with DoubleClick.

I want to go back to a point that Ron Plesser made earlier about a sliding scale, which is that the type of information we're dealing with, it's sensitive information, calls into question all of the other issues that have been brought up. A cost-benefit analysis for sensitive information could be very different, access could be very different, retention could be very different. So, I just think it's important to try to draw the distinction between what is considered sensitive information and what is considered by many people nonsensitive.

MR. MEDINE: Rick?

MR. LANE: Yeah, someone mentioned about consumer awareness and educating consumers, and I just want to mention about, you know, internet for dummies. From the business side, and we saw this with some of the early adopters of having a webpage that wasn't collecting information but not having privacy statements, and the reason that they didn't have privacy statements is they just didn't think about it. They

didn't know the advantages and disadvantages.

So, when we talk about education and consumer education and consumer awareness, it's also incumbent and one of the things that the Chamber is doing and implementing is business awareness of what are their responsibilities and what they should be or -- we would probably disagree that we should have legal requirements, but I think a business awareness is critical to this. So, we're all on the same page. So, consumers know what they're expecting and businesses are knowing what the consumers are expecting from them.

MR. MEDINE: Thanks.

MR. GAVIS: Alex Gavis from Fidelity.

I think one thing that may be a little bit more mundane to think about is the format of access. When you think about format from the customer's standpoint, it's got to be clear, has to be understandable, and to Jane's point that the customers need to know what the technology is. Format also from the company or the corporation side in terms of if it's narrative or if it's in data format. If it's narrative, it may be very difficult for the company to actually develop a standard that would make sense for the customer or that could describe what derived data is or what the derived data about the customer is. So, I think format is an

important point.

MR. MEDINE: I think there's been a useful evolution in the credit report format over time from a code sheet to plain language, explanations, and so that might be a useful lesson to learn, at least the group might want to consider looking to that model, where there was a desire to put everything on one page, but it meant everything had to be a variety of codes and that you had to code them, to now a little bit longer narrative where consumers might easily understand what was going on, so that you might want to consider that as a possible model.

MR. WHAM: We have got issues on access on three different fronts. First of all, as a business -- I'm sorry, Ted Wham with Excite@Home.

We would have enormous benefit from more explicit definitions of what exactly is personally identifiable information. There are contexts, for instance, where a first name is not PII but where a first name combined with a last name, suddenly the first name does become PII. There is issue also around if you can identify somebody down to the household level but you don't know which individual it is within the household, have you gotten down to PII or not? Is a cookie PII?

The second question I've got regards appended or overlay data. That's the process of taking, you know, what you know about a customer, combining it with a third-party data set to know more about that customer, what is going to be the responsibilities of the businesses that are the purchasers and users of that appended data to make that appended data available to the consumer, and secondarily, what are going to be the responsibilities to allow, you know, a mechanism for correction of that appended data where the business is the consumer of that information as opposed to the originator of that information?

And finally, kind of touching on the points raised here by my colleague from Fidelity, and that is the narrative information. Narrative can take a couple of forms. It can take the form of what the company takes and writes about the customer and says, you know, this is an individual that perhaps in Fidelity's case seems to have some upcoming needs for perhaps trust development, but it can also take the form of all of the information that the consumer has put in nonfielded data entries, such as chat conversations, bulletin board entries, you know, e-mail, et cetera, which the websites, such as Excite@Home, is going to be the conduit for the provision of that information, maybe

because of backup purposes have that information long-term, but for God's sake, we don't want to have to provide it, because we don't use it, we don't field it, we don't use it in that way. So, is there a requirement for us to provide, for instance, a transcript of every chat conversation over the last three years?

MR. MEDINE: And also I guess more broadly information that you have and may not be easily associated with an individual but could be associated with an individual?

MR. WHAM: Very, very good point. So, if we have a need, it would be potentially possible to do a lot of things that the data volumes themselves don't generate a business rationale for doing them, so we don't have that information available, but do we have a requirement to provide a level of access greater than our own level of access within the business itself?

MR. MEDINE: And also, you know, I'm interested in -- an interest to us would be the cost issue surrounding the compilation of information for a consumer, and that may depend on whether it's an old database system which is indexed in certain ways or a new database system, but the cost structure and whether that cost structure is something that's likely to change over time I think would be very beneficial to hear some

comment on in terms of whether access is feasible and at what cost.

MR. MAXSON: Well, Jim Maxson, and this is really following up on these last few points that were made. I think what we're talking about is meaningful, reasonable access. Reasonable access is not useful if it's not meaningful, if the data cannot be understood by the consumer.

MR. MEDINE: All right.

MR. PURCELL: Richard Purcell, Microsoft.

Further to the list, one of the -- despite the best efforts of Mr. Henderson of NCR, not all of our companies have created single data warehouse solutions where access can be granted from a single point, and we have to be careful, because what this brings up is the conundrum of practices that are designed to protect people's privacy that follow onto results that are singularly considered intrusive of privacy.

In other words, if I gather all of my customer information into a single data storage device, I've done more to enable privacy intrusion as well as to enable privacy protection, and there's a real problem that we have to address there.

So, further to that, though, a lot of our companies do not store customer data in a single point.

One of our access questions will be access to all data storage devices in which that customer information is uniquely held. That becomes a very much more difficult problem as the company, like my own, has a very extensive set of different business and consumer services and may maintain the relationship with those customers in that service in a discrete database and may not commingle and combine that into a single source.

Additionally, the source of the data may be an access attribute that is important. Where did you get that may be a legitimate question that we need to address in terms of providing access.

Further to that, where did it go may also be a legitimate question. We may follow the notification and consent around distribution to third parties. Does the individual then have a follow-on right in the access principle to know to whom you distributed that information?

And supporting Lorrie's earlier point, this has to do, of course, with transactional stuff. I am a vendor. When you order, I ship that order off, the vendor fulfills that order, fine, that's done, that's one part of it, but there are other marketing partners. You may have -- I may have notified you adequately, you may have consented to the distribution of your name to

marketing partners, but the question is, do you have access to know where that distribution has occurred?

MR. MEDINE: Thanks.

Tom, then Frank.

MR. WADLOW: Tom Wadlow, Pilot Network Services, several points.

One thing I think that's interesting to talk about here is we've talked about, for example, informed consent, and one way to sort of shorthand that informed consent is some sort of a grading system to know how well an organization applies an information security policy, how well they manage privacy information and things like that, and discussing something like that might be interesting.

Another thing that I think becomes interesting in this regard, and people touched on it in terms of derived information in a number of ways, is the implicit assumption in derived information in some of the discussions that's been going on here is that there's a buyer and a seller or two people in a transaction. There's also a lot of people in the middle of a transaction. A good example of that would be an organizational firewall and having traffic analysis of information passing back and forth across that. You could derive a great deal of interesting information

about a person, what their buying habits are, things like that, and what are the responsibilities of people who maintain those things?

A third point that I wanted to raise and my final one is there's a difference I think that becomes interesting in terms of information that a consumer asserts in that they buy a book from Amazon, for example, and they have made an assertion, this is my credit card number and I want this book, versus information that other folks were discussing earlier that happens in a much less formal, much more conversational fashion, like I might say in a chat room that I like a particular book. That is one sort of information, and it may or may not be as true. I may have said it just to stimulate conversation, whereas if I buy a book from Amazon or whoever, then that's a much more tangible assertion.

MR. MEDINE: Okay.

MR. TORRES: Frank Torres, Consumers Union.

What's really eye-opening from this discussion is how widely consumer information is collected, used, stored, manipulated, sliced, diced, kept for your own purpose, just stored, maybe other people can access it, and so in that sense I think it's been really fruitful.

But to get back to some earlier points that have

been made, I understand the complexity and the technological questions that are involved here and the points made about, you know, how to get access and yet keeping the site secure. Again, I'd like to just raise the point, we don't want to create or get into a world where we're protecting the consumer from himself or herself. You know, you call up the bank and you say I want to access my information to see if it's right, what have you collected on me, you know, what are you using, how are you using it, and you're told, well, we'd love to give it to you, but it's kind of scattered about for your own protection, and I'd hate to see us kind of go in that area, that consumers don't have access for those reasons.

MR. MEDINE: Okay, and those are useful contrasting views as to whether aggregating data is more privacy protective or more privacy invasive and it facilitates access or it makes access more difficult, again, I think those are very useful considerations.

Mary, then Ron, then folks off to the left.

DR. CULNAN: Mary Culnan.

This sort of relates to the issues of sliding scale and type of data and sensitivity and whatever, but I think it's also important to at least think about are there contextual issues something that only matter to

the different industries or different business practices. This may not be an issue, but it may be, and we wouldn't want to come out at the end and have something that just goes -- and go, whoops, it's just a show-stopper for a particular group that's not represented at the table because we just didn't think about it.

MR. MEDINE: Again, we tried to pick as diverse a representation from those who were nominated, but again, that's the advantage of the public comment process, is that those who are interested in the process have the opportunity to submit comments for the committee's consideration in terms of drawing lines if they choose to.

Ron?

MR. PLESSER: Just to underscore I think what somebody said about the communications part, I'm now representing a client where we're trying to get information about what information -- who called in to a cell phone voicemail account, and the Bell company won't -- the particular Bell company won't give it to us not because of access principles, but they're worried about the privacy of the people who call in and whether or not that's required or not and those issues. So, I think that very much is the issue of almost a minimization or

the access to what information and how it impacts the privacy expectations of others. That may be less so involved in a merchant or a direct marketing thing, but when we start talking about chat rooms and access and communications access, I think those issues are very critical and probably need to be looked at.

The other issue I think is you know, the liability issue, which we did look at in the Children's Online Rule. You've got to be very careful that you're not giving out the information to the wrong person. I think that's been discussed here, but I -- you know, it is an area that the Commission has looked at. I think there needs to be reasonable rules. Access sounds great, but we all know that e-mail authentication is not really perfected yet, and so how that's done and who that's done with and what's your liability if you give the information out to the wrong person. I think what are the standards of care, and I think those are very serious issues that the credit industry has -- credit reporting industry has faced, and they are very difficult and important issues here.

MR. MEDINE: Right, and I would like the committee to look at the Fair Credit Reporting Act, for example, that requires proper identification for access to a credit report, and you also raised an issue which

was raised earlier, just to repeat, which is if there are multiple people involved in a transaction, access by one may have privacy implications for others, whether it's a joint account, joint internet service provider account. There may be information where people are involved where access by one may have privacy implications for others.

MR. PLESSER: And the word is minimization, if we can look at the wire tap statutes, but I think the question is really what's the requirement to minimize so that you're giving data only on the particular person who's making the request.

MR. MEDINE: It may also turn on expectations as well as -- in the notice context of what people expect is going to be accessible by others.

Rick?

MR. LANE: We focused on the collection of information from businesses, but there are other entities that collect information. I don't know if Consumers Union has a website and they collect information, what currently their access and security mechanisms that are in place. Governments collect information, other nonprofits. You have local homeowners' associations now putting up websites and collecting information. So, you know, when we're

looking at these issues, you know, let's not just focus on business. We're talking about consumer access and security, because information is all over the place. So, you know, let's make sure we have our own houses in order, as well, before we start --

MR. MEDINE: Okay, I will I guess, going back to my legal role here, remind the group that this group has a charter that was approved by GSA and the FTC, which had focused on commercial websites, and so while there may be --

MR. LANE: Some of them -- yes.

MR. MEDINE: -- there may be matters of interest that go beyond commercial website activities, that this group's charter does limit its focus to that particular context.

MR. WHAM: Ted Wham from Excite@Home.

It's interesting, the gentleman from Consumers Union made the point earlier about the bank, because you call up and you can't get information about yourself because the bank has put up such a high barrier to entry for the access. I'd like to point out that a lot of our discussions about the type of access we'd like to be able to provide is information that I absolutely cannot get by calling my bank, and I would suggest that most of us in this room wouldn't be able to get by calling their

bank, as well.

So, while I can access information about my bank account and my transaction history at the bank, I can't get information about the overlay activities that they've done on me. I can't get information about what type of marketing campaigns they've targeted to me. I can't get information about why I'd be targeted for some of those or not targeted for others. So, I think part of our work here should be -- you know, I can't get any information about where they've shared that information with. They might be able to tell me on a binary basis where they do or do not share that information. In most cases, the information that that bank holds about me is a lot more near and dear to my heart than many of the businesses here.

So, I think part of the things that we should include in terms of access is making a compare and contrast to what's available in an offline world and to what degree is a standard of access for the online world that is higher than an offline world, is that a reasonable position for the FTC to be, you know, building in and making into their recommendations.

MR. MEDINE: And of course, you're free to make whatever recommendations you deem appropriate.

Fred, Dan, Tatiana, Art.

MR. CATE: Okay, thank you, this is Fred Cate.

I think we should also be specific about thinking about affiliate and subsidiary issues, because I expect that most consumers would want to think that they can go to a single entity, even though that entity might be providing services or collecting information through numerous affiliates.

On the other hand, it would be somewhat ironic in light of the current debate if we were to make a recommendation or if the Commission were to adopt a rule that were to require affiliate sharing of information in order to provide access.

MR. MEDINE: Dan?

MR. JAYE: Dan Jaye, Engage.

Two points as we -- two issues to consider. As we talked about reasonableness, one of the things that we should talk about is what implications some of our decisions have on the general economic models of the internet. So, for example, if to provide access we suddenly said every site, in order to do any personalization, had to now have explicit user name and sign-in, then certainly that would impact the ability of -- first of all the accessibility of the internet to many people. It also I think would arguably reduce privacy on the internet.

And then finally, the economic models of the internet do not currently make most websites that provide free services and content profitable. Marketing and advertising services are what pay for the internet, and it's very important that we consider our decisions in terms of reasonableness so that they don't adversely impact the benefits the consumer receives from the free internet.

And then the second issue that we need to consider, and bearing in mind this is a domestic committee, but there are domestic commercial interests about being able to support our customers and our businesses that are multinational, and to the extent that we know, for example, that an access requirement or an access recommendation is going to cause issues in other jurisdictions that we have to interoperate with, I think we need to at least address that very briefly, because it does affect U.S. commercial interests.

MS. GAU: Tatiana Gau, AOL.

I would like to concur with the majority of the comments that have been made with regard to looking at the different categories of data, particularly in the context of access and security to protect such data as it's stored.

I would like to also concur with Mr. Purcell on

the issue of data being stored in separate databases where companies do not have a file on a user, how can they be expected to create a file, within what parameters and within what logical time frame, you know, the reasonable issue that we've been talking about.

I would like to comment on the issue regarding chat sessions and public message boards and other types of public displays made by individual users on the internet at large. I think that you need to take into account category of data in a somewhat, you know, different room so to speak and look at that separately, because when a user is actually interacting on the internet and is posting to a message board, there is no expectation of privacy at that level, and I don't think that we should lump it in with some of the other things that we've been talking about so far.

A final point I'd like to make is with regard to personally identifiable and nonpersonally identifiable data. To the extent that a company is not tracking any kind of data and, in theory, could be maintaining it at the nonpersonally identifiable level, I think we really need to consider what would be legitimate reasons for a consumer to have access to that data if it is not tracked nor used in any kind of personally identifiable form.

MR. MEDINE: Thank you.

Art?

MR. SACKLER: Art Sackler.

David, just going back to your point about the charter confining us to just looking at commercial entities, I assume, though, you are not saying that we can't look to the practices that are taking place in other places, the nonprofit world, to see what they do for comparison, number one. And number two, there may be situations where nonprofit data and data collected by commercial entities are gathered in the same place, commingled, whatever you want to call it, and then used for a variety of purposes, and we'd want to look I think at how we might want to address that particular situation.

MR. MEDINE: Just let me comment on that. The charter and the report should be focused on commercial websites. Obviously, as we discussed during this conversation, there may be examples, models, lessons to be learned from other contexts, and, of course, those could include nonprofits or others, but the focus of the Commission's work in the area of online privacy has been with regard to commercial websites, and that's the charter of this group, as well.

MR. SACKLER: Right. Then one other point, and

we're talking about third parties, if businesses are in joint ventures of one sort or another and there's information being collected on both sides of the joint venture, I think we should look closely at how limited the access requests and responsibilities should be in that circumstance. If the other party is doing something with the data that you have absolutely no idea they're doing, it should not be your responsibility.

MR. MEDINE: Okay, that's a little bit -- also relates to the affiliate-sharing/third-party issue, as well, that as information flows through a variety of companies, at what points in the process should there be access.

MR. SACKLER: Right, it does mostly fall under there, but I'm thinking about going beyond the outright affiliation within a company to two distinct companies working together, that kind of thing.

MR. MEDINE: Steve?

MR. COLE: Two points, Steve Cole.

This issue, we have been talking about commercial entities versus nonprofits. I don't remember what the charter says, but the bylaws we approved talk about commercial websites, and that's very different in my mind than commercial entities. A nonprofit may be selling goods and services online, and I would consider

that a commercial website even though it's a nonprofit, and I assume we're referring to commercial websites, not the legal corporate organization of the entity.

MR. MEDINE: The charter refers to commercial websites.

MR. COLE: Okay. So, Consumers Union, for example, has a very fine commercial website.

MR. LANE: And that was my point.

MR. COLE: Okay, the other point I wanted to make is someone mentioned COPPA earlier, and it reminded me that the question of who gets access to information goes beyond the authentication issue we've been talking about. For example, in the children's area, a parent may need access and will need access, and there are issues something that only the to that. If I'm a gift recipient, I didn't provide the information, but I'm a prospect in your database, perhaps, then I may need access to that information.

So, we should look beyond the person who gave the information to see whether there are other categories of information, other categories of persons who also deserve access.

MR. MEDINE: We'll take a few more comments, we are going to try to wrap up in the next few minutes, but Larry.

DR. PONEMON: Larry Ponemon, PricewaterhouseCoopers.

Here's an interesting real life case study, and I'd like to pose it to the table. One of my clients, a financial service organization, it's a bank, and they are required by law to have a program called Know Your Customer, KYC, which means that when you're, you know, getting a loan in Mexico, whatever, you're giving out money, you're receiving money, you need to know who you're dealing with.

This organization got into big trouble, I'm not going to mention their name, but the bottom line is now they are required to do profiling of their customers, and so they have a rating. It's called a likelihood of money laundering risk. In other words, we want to let people know -- good and not so good people know what that rating is. So, if we're thinking about access as always being good, we have to think about the flip side.

MR. MEDINE: Deirdre?

MS. MULLIGAN: I wanted to reiterate a comment about -- Deirdre Mulligan, sorry -- by AOL that I think when we're talking about access, it's very tightly tied to retention, and it's also hopefully something that we can separate from when people are acting as conduits,

but I think, for example, when you're providing chat or allowing people to e-mail, that by minimizing retention of data, you can both limit access concerns, because you're not maintaining records of what people said, and you can also limit the privacy impact.

Well, I think our focus here is the uses. You spoke about you may have the data, but you're not using it in an identifiable form. You're not using it to target people, you're not using it to profile them. It's in your database, you have no interest in it, but the fact of the matter is somebody with a subpoena or a warrant could come in and ask you to produce that data, and my guess is that with a reasonable effort you could.

So that while the privacy impact might not be apparent at the front end, the risk of retaining the data may become quite significant. And that also ties into what's being retained, that when you're looking at data, if it says, Deirdre's a sports enthusiast, that's very different than saying Deirdre went to, you know, the NCAA football page and -- is that right -- football, yeah, and then she went to the Division I soccer page and then she went to, you know, the sports zone.

One of them allows you to track my actions as though you were following me around. Another provides a

very generalized concept about, you know, what I might be interested in, and if you think about how those are different from the individual's perspective, from how they could be misused, I think that could be quite significant, and you could imagine having a much lower standard for access to data that merely said, you know, user 982 is a sports enthusiast and, you know, likes books versus an entire transactional history of what I've done, where you might need to have very serious authentication methods that said this is Deirdre Mulligan.

MR. MEDINE: Dan?

DR. SCHUTZER: I think we're just dismissing the chat aspect a little too fast, too soon. I mean, it all depends what I'm correlating it with and what I'm using it for, and it's not just a question of retention. I think I do have an expectation when I'm in chat that there is some privacy aspects to it. I don't think you're going to want -- I'm not going to expect you to correlate it with my home address or my credit card number or necessary to pop up an intrusive advertisement based on something I said because of word spotting. I think you dismiss it a little too lightly when you look at what can be done in today's technology. It can be just as intrusive, maybe perhaps more intrusive, than

some of the examples we're giving in the financial services industry.

MS. MULLIGAN: Deirdre Mulligan, I just want to respond.

What I'm suggesting is where somebody is merely acting as a conduit and, in fact, isn't doing anything else with that data, are merely providing a service where other people can communicate, which I believe is what both AOL was talking about and what was being talked about over here, that that's very different than actually collecting and retaining data for the purposes of using it in a way that relates to a specific issue.

DR. SCHUTZER: Yes, for the use, but we have to be aware that there are some types that doesn't have anything to do with retention, but it's realtime use.

MR. MEDINE: It sounds again from the number of comments about the chat issue that this group may well want to take that up as one of the issues.

MR. WHAM: I think Dr. Schutzer was talking about chat just because he doesn't offer chat, so --

MR. MEDINE: Maybe he's thinking about it.

MR. ALLEN: This is James Allen.

There has been a number of comments made about referring to information like marketing campaigns or the likelihood that somebody might launder money, and those

are really actions and conclusions that are based on opinions that are derived from factual information. It seems to me like we're really talking about giving consumers access to the factual information about themselves, not to the opinions or conclusions or actions that businesses may draw from that factual information, and I think we should try to differentiate those two things.

MR. MEDINE: Okay, for time purposes, we are going to take four more comments, Tom, Ron, Lance and Tatiana.

Tom?

MR. WADLOW: Tom Wadlow, Pilot Network Services.

One thing I wanted to mention that somebody had brought up earlier about the advertising model of the internet and how a lot of services are provided for free to various people and we didn't want to impact that. I think it's important to note, though, that those services are not free. What those services are doing is essentially in many cases trading privacy for service, and where we could make some efforts to make that more explicit, so that someone would have an ability to know what privacy they're trading for services, I think that's very important.

MR. MEDINE: Ron?

MR. PLESSER: Just talking about the cost-benefit element, there's one thing that I don't think has come into the conversation on cost-benefit, is whether or not consumers really use access, and I think that's something, while we talk about creating structures and centralization, the experience in Europe is, where they do have access requirements, is that there's extremely little consumer request for access.

In the United States, I have had experience both with the cable industry, and I would suspect it is under mandatory access under the Cable Act, I would suspect that there's more subpoenas over the years and warrants in the cable industry than there have been individual requests. That's just anecdotal, but I think that's probably true.

And under the IRSG, which has an access requirement for nonpublic information, and I think we did present some statistics to the Commission and we will be happy when the time comes up to do it, it's astoundingly low. I'm not saying that that's good or bad, but when you look at cost-benefit analysis, when you look at the privacy dangers, when you look at some of the other issues, I think you've got to take a look at whether or not these systems are really going to be

used by consumers and look at other experience.

Fair Credit Reporting Act I think is different. When somebody gets a notice that they've been turned down, then they go to the -- then the request for access is fairly high. I think there is a dynamic there, but I think that should be on the list, because I think it's important.

MR. MEDINE: Again, I think that's where this group can be very helpful in providing information about levels of access on the one hand versus the values that Deirdre outlined earlier of the benefits of access and striking that balance -- providing good information base for the Commission to strike that balance would be extraordinarily helpful and I think enrich the debate considerably.

Lance?

DR. LANCE HOFFMAN: Lance Hoffman.

I think as we pursue these discussions further we ought to keep in mind the increasing advent of the wired world, rather the wireless world, because, in fact, we're seeing just now for the first time, you're more and more able to store a lot of your information, chat and other information, not only communications, but storage, as well, offline. Both consumers and businesses may wish to store their information offline,

because it's cheaper. There are services and businesses coming up to do this, and it raises a whole different dynamic to the way we're used to thinking about this.

So, I think as we consider this, we have to consider these vast repositories, and that would have to necessarily include chat at least to examine it before we decide what to do, because it's not the usual paradigm we're using. It's changing.

MR. MEDINE: Thank you.

Tatiana, last word?

MS. GAU: Tatiana Gau, AOL.

I think we all agree that online access is necessary in order to help improve the online experience, to build confidence in the medium, but also really to address consumer perception, and I think awareness is a key component there, but to go back to the point that Deirdre made earlier with her example about clickstream tracking and navigational data, that's a particularly sensitive area right now, and I believe that that needs to be addressed in terms of indeed what kind of navigational data is being collected on users by certain companies, how are they notifying users that this is happening, what are the choices, and, of course, as we're here to discuss, the access and security to said data.

MR. MEDINE: I thank you all for a very lively discussion. I think we have set forward a very impressive agenda of things for this group to consider. Let's try to take a 15-minute break and then return to discuss security issues.

Thank you.

(A brief recess was taken.)

MR. MEDINE: We are going to now turn to the question of security, if people can take their seats.

Okay, we have a few -- we will give a few people a minute or two to get back to the table again.

Okay, we want to turn now, now that we have resolved the question of access, we can turn our attention to the issue of security, and we'd like to basically have a similar conversation about the range of issues that the committee will consider in the area of the fair information principle of security, and again geared towards developing some working groups to follow up on this meeting and to report back at the next meeting.

So, I guess starting off with the brainstorming on security, is there anyone who would like to volunteer to begin?

Yes?

MR. HENDERSON: Bob Henderson from NCR.

I'd like to first establish a point of reference, a potential discussion point. Security and privacy are separate, they're different, very much co-related, have a dependency on each other, but I argue that you can have privacy and not have security, you can have security and not have privacy, but if you're going to build trust with the consumers, you have to manage both, and so I just want to be sure and put that up as an issue, that we understand the relationship of security to privacy and vice versa.

DR. CULNAN: I'll build on that --

MR. MEDINE: Again, let me just remind people as we return, two points. One is to identify yourself at every opportunity, and also, for the benefit of those in the overflow rooms, to speak into the microphones.

DR. CULNAN: Mary Culnan.

I agree and I think often privacy and security get mushed together, and they are very much separate, but this is also one of the areas where poor security leads to enormous privacy violations, so they are clearly linked.

I think one issue, and this is where I sort of bail out of knowing anything about security at all, it's security information in transit versus security information in storage, and a lot of stuff is encrypted

while it's traveling, but then it's stored in a database that's accessible online or whatever proper protections are put in place. So, we need to look at both of those issues.

MR. MEDINE: I guess one thing that would be helpful, at least to benefit the Commission's knowledge base on that question, is to what extent can a website have influence over the transmission process. Obviously they have a lot to say about the storage process, but what role is appropriate for a website to play in the transmission when obviously it is being transmitted over lines and communication mechanisms that are not in control of the website.

MR. PURCELL: Richard Purcell from Microsoft.

There are specific responsibilities and functions that a website can provide in terms of transmission through encryption technologies that they do control, and they can enable SSL or other encryption devices in order to make sure that transmission over wires is kept -- is kept in -- there are varying levels of security, so we have to be really careful here when we talk about, okay, secure transmission.

Well, that's -- there's a lot more to securing a transmission than just stating that as a fact. There are multiple means of doing that, there's point-to-point

issues, there are firewall issues, there are a number of different layers involved in that.

Additionally, the question becomes, do you pass -- if we get to -- if we are able to categorize data that -- defined data, first of all, and then categorize data, are there categories that are subject to a higher level of security and other categories that are subject to either a low level of security or, as is often the case perhaps unfortunately today, data that's passed in free space.

Transmission is one of the security concepts or aspects that we have to be concerned about. Transit is another one, as Dr. Culnan has mentioned. Data is not always passed over wires. It is often passed over some other media, as well, could be a magnetic medium, could be optical. There are lots of ways to store data for transfer, and again, the securing of that is necessary.

One of the -- probably arguably the largest data transit company in the United States is probably Federal Express. They probably or arguably handle more personally identifiable data than this room combined, because they essentially ship this data from point to point physically and not often securely.

Storage is a major issue, again, encryption, permissions, physical access, backups, archives,

purging. There's a whole host of layered information or issues that we have to be cautious about. Distribution, as I said, in transit, and then, of course, monitoring security of all of these different areas is incredibly important, too. So, there has to be some mechanisms both internal, perhaps external, and there have to be a set of standards, which some of our colleagues from RSA certainly can help us to explain, against which then that monitoring is conducted.

MR. MEDINE: Okay, just I guess to add on to what was talked about, media, and we had talked about wireless earlier, and there are I guess a number of communication mechanisms. We also -- the sliding scale may be returning, as well, in terms of the level of security being very closely something that only the perhaps to the nature of the information, but that would again be something that would be very useful to hear from the group about.

Yes?

MS. PIERCE: Deborah Pierce from the Electronic Frontier Foundation.

It's not just the technology that's involved but also training people who are handling that data, because a lot of times what we see happening is people who have a lot of information in databases, they accidentally do

something because they don't understand the technology or they haven't constructed their database securely enough, and data gets out, and it's released to the public. So, I think, you know, like HHS has in their proposed regs for the health information, maybe one possibility would be to have, you know, a privacy officer, you know, on site, but that's an issue we should look at.

MR. HENDERSON: Bob Henderson from NCR.

I think another issue for us to consider is levels of security. You have the emergence of biometrics. I was dealing with some European government registers, and we were talking about fingerprinting recognition, and their view was that that's a very cost-effective capability, and they wanted to implement that as a standard, because it was only $200 in terms of having the PC. And I said, well, what about those businesses that have millions of customers, have hundreds of thousands of stations, and would have to have literally several hundred thousand of these terminals? Now you're talking about a big ticket item, even though it's only $200 apiece.

So, there are needs for the businesses to have the ability to have levels of security based on their business and the environment that they're in. The

Social Security and PIN or Social Security and mother's maiden name type of thing is the simplest form, then you get to levels of encryption, then you get to levels of biometric.

I think as a committee we want to look at these and maybe set some parameters, but there have to be some people looking at security to define the levels that should be necessary. Obviously government has a higher level than a retail in terms of controlling security. So, I think levels of security and how we recognize that and identify that is very critical.

MR. MEDINE: And obviously reasonable security turns to a fair extent on cost-benefits, and I think your point about costs, it's important as both the costs to businesses and the costs to consumers, is to take advantage of some security mechanisms, and that may raise some issues, as well.

David?

MR. DAVID HOFFMAN: David Hoffman from Intel Corporation.

To borrow from Mr. Purcell's methodology on access, I think our efforts will be aided by being able to subcategorize storage and transmission, and I think the question on storage is a question of where is it stored, and I think that should include, for purposes of

our discussion, the end user appliance that they are using to enter that data into transmission, also includes third parties where it might be originating and intermediaries that have access to that information.

For transmission, I think the key question to subcategorize is who's the transmission between? Is it just the transmission from the user to the person -- the entity that they believe that they are giving the data to, or is it onward transfer? Is it intermediaries that are transferring, is it subsidiaries and affiliates, and are there vendors involved who could be handling the data?

MR. MEDINE: Okay, Rebecca?

MS. WHITENER: Okay, Rebecca Whitener, IBM.

I want to basically agree with the kinds of things we're coming up with with regards to the mechanisms and also with what Mr. Henderson said about information classification and then bring also into focus that all of the kinds of things that have been brought up with monitoring, they really tie into a security organization. So, as we examine and look at the mechanisms that might be in place for encryption or in the transmission, as we relate to specifically personally identifiable information and online, we would want to take into consideration, again, the things that

have been mentioned as training, incident management, the organization of the security within the organization, how they classify information.

All the kinds of things that are being discussed are really part of a larger security management program, so that it can't be really isolated to one specific element. It is really part of the whole. And it actually does go back to access control, what or how are employees given information within the organization, clean disk, password administration, a whole elaborate program.

MR. MEDINE: Would you include audit procedures?

MS. WHITENER: Yes, audit, monitoring, training, that was mentioned earlier.

MR. BAKER: Yes, Stewart Baker, Steptoe & Johnson.

I thought I'd try to unpack some of these issues from the point of view of what we might ultimately recommend. The first and most fundamental rule of government policy in security maintenance and in security is the government always wants more security than anybody wants to pay for, and so the question of how much security you want to pay for is a fundamental question, and I think the first question we ought to ask

in this context is would we want to not simply rely on the cost-benefit analysis that the company that's protecting the data uses, that is to say, the company decides how much it's going to spend on people to do web security or not. It does, after all, collect this data and thinks it has value. The question is why shouldn't you rely on them to make the decision. I think that's one question.

There's a separate, second question which is are there market failures that would lead you to think, well, maybe this data's more valuable to the consumer or more risky to the consumer if compromised than to the site that gathered this. They don't really care that I looked up gallstones, but I might be embarrassed by the fact that it was disclosed.

And if you're going to pursue the question of market failures and decide that someone else should be deciding how much should be spent on security or raising the amount that's spent on security, you come to the question of how you set the standards, the security standards. This is a field where standards are not well defined in my view, and there's an enormous amount of debate about them.

If you talk to people who do computer security for companies and ask them what their graduate or

undergraduate degree is, you will find people who have nursing degrees and law enforcement degrees and computer science degrees. You cannot predict who will end up in this field, and their expertise and the standards that they apply are very fluid. So, finding those standards and deciding what is appropriate I think is a tough issue.

On the question of data in transit versus data at risk, I think we see an example, if you had read the papers, you would have said the one thing that websites have to do is put SSL in place and have a longer key than 40 bits to protect that data while it's in transit across the internet. The fact is I would bet that 60 percent of the credit card numbers that have been transmitted over the last five years on the internet were either in the clear or protected with a 40-bit key, there's not one known compromise of those keys.

It turns out that where we should have spent our money is in protecting the databases that we built afterwards. So, it's very difficult to predict what is good security here and define it, and I think the question of how we're going to get to that is a tough question we have to put on the agenda.

MR. MEDINE: Thank you. I guess going back to your first comment, cost-benefit or who's protected, I

think it sounds like it's an important point of view from a public policy perspective, from a consumers' perspective, from the businesses' perspective.

MR. BAKER: Yeah, I would unpack that to say why not start with business since they provide a consumer cost-benefit analysis for all of their other data, and the question that then arises is are there circumstances where they're not measuring the cost properly because the consumer has a bigger cost.

MS. GAU: Tatiana Gau.

To the point of storage of data, which I think is something that is separate from transmission of data, when speaking of unauthorized access, and if you take a look at hackers, hackers are always going to choose the path of least resistance, and in most cases it's much easier for them to target an existing database or a website that has become e-commerce enabled and hasn't taken the proper steps with its technology to actually protect the data, and they will go after such things as credit card numbers and post them on the internet, in some cases to illustrate certain vulnerabilities, but you do not hear of as many incidents, nor do I know of just from my experience as well as colleagues of mine in the industry, that hackers are going after the databases. They are not going after data in

transmission. So, I would just like to emphasize that as a particular issue something that only the to storage.

MR. CASEY: Steve Casey, RSA Security.

There is a third bucket I think I'd like to add in relation to storage is authentication, and to build on I think Tatiana's point, one of the weakest points I think is the password. So, we have talked about biometrics, but I think we need to expand that discussion into two-factor identification, in that it's often the initial entry point.

MR. MEDINE: Was that two factor, could you explain that?

MR. CASEY: Yes, two factor, so that it's not only -- it's typically something you have and something you know. An ATM is a good example. You have a card with data on it, but you also have a PIN in your head, and unless you have both elements, you can't gain access to that data.

MR. MEDINE: Do I see another hand back there?

MR. SHEN: Andrew Shen from EPIC.

Building on something Stewart said, I think here it's important to point out that breakdowns in security are an important issue and include the effect. I think the customers really bear the brunt of the unfortunate

consequences that may result. So, we have to really investigate where the liability of security breakdowns should lie, because I think such security breakdowns are inevitable. While they may not be that often, they may not occur on a regular basis, they are inevitable, I think, in today's world. So, whether, you know, companies that are negligent in implementing a security policy should be liable for not doing so and rules implemented for companies that don't take their responsibility seriously should be considered.

MR. MEDINE: Well, Frank, why don't you go ahead.

MR. TORRES: Frank Torres from Consumers Union.

A couple of comments, first of all, to follow on what Andrew just said, you know, what happens when security is breached? For a consumer, it could mean a couple of different things. If it's just simply somebody got your name and e-mail address and sends you a bunch of SPAM, that's one thing. It gets into identity theft where they have stolen some account information, then it becomes a little bit more problematic. If it's a credit card number, then you've got some liability as limit -- your liability is limited by law. If we get into other payment forms, like debit cards or check forms where it's a little bit more

questionable whether or not some voluntary limits on liability will actually withstand if there's a lot of fraud going on, that's another issue altogether.

So, I think that's important, what are the consequences, and as Andrew said, the consumer feels the brunt, especially in the area of bank accounts and checking accounts and savings accounts.

What is the responsibility of sites here? Again, in the financial setting, there was -- part of the pretext calling rule, making an illegal practice of pretext calling, kind of more illegal, if you will, but the banks didn't want to bear any responsibility for giving the information over in the first place, which kind of gets to I think the authentication question, you know, who's responsible for authenticating, and isn't that a good first step to look at.

And then we have the question of responsibility for downstream use. What's the responsibility for the person who's the primary collector of the information, who then sends it to somebody else, who that second party might have another secondary use, and, you know, where can the consumer go? I hear the industry side raising it, well, the consumer's -- you know, where should consumers go? I think that's a good question to ask.

Then finally we have the types of data, which kind of, you know, we've got, you know, credit data and bank account data and health information, and some of these, you know, consumers are very much concerned about keeping and protecting, which raises the importance of the issue, which, you know, might be on a -- where it hits the consumer in the pocketbook might be a little bit different than an e-mail address that gets out. So, those are the issues that I wanted to mention.

MR. MEDINE: So, again, consider that there are costs on the business side, but obviously consumers bear costs, as well, and that may to some extent relate to the market -- the question of whether the market adequately factors in the costs to consumers of identity theft or other concerns.

MR. TORRES: Or just to follow up, I had a side bar discussion with somebody a little earlier, is it a question of -- say in the payment system, do we look at -- you know, should we be looking as part of the security debate or the security discussion, looking at, you know, if it's a question of somebody, you know, stealing someone's identity or taking somebody's check card number, should we -- is it appropriate -- maybe not to say, you know, you need to have insurance liability protection, and any entities doing business on site --

online have to do that, or we should -- maybe, you know, a more fundamental approach is looking at the payment system mechanisms, and maybe that might be an adequate way of dealing with at least some of the payment security questions.

MR. MEDINE: Deirdre?

DR. SCHUTZER: Dan Schutzer --

MR. MEDINE: I'll get down to you, Dan. Thanks.

MS. MULLIGAN: Deirdre Mulligan.

I'm not a security expert, but generally, even when I look at things from a legal perspective, usually identifying what it is we're trying to address, and so far I have heard most of the conversation focus around unauthorized access, primarily hacking, whether it's into databases, and when I think about risk assessment and threats to data, I think there is several boxes.

One, we have unauthorized access from outside parties, so the hacker. We have misuse by authorized parties, which is kind of getting into the auditing issue and the logging. And then third, which is a -- I think an access issue or risk, security threat that is often overlooked, because it does dovetail into law, is the fact that the further data gets from the individual, the less legal protection it has, as in the more people

who are authorized or at least not limited in their access to that data.

So, for example, my bank book under my bed, Fourth Amendment, government can't come in, you as a private party can't get it without my knowledge, unless you come and break into my house. If that information is on a third-party server, if it's Monica Lewinsky's book purchases at Kramer Books, okay, the Fourth Amendment doesn't necessarily follow us out into the network world.

So, when you think about risk, you have to think about the different risks that are caused by different decisions about where to store data, and I want to suggest that in assessing risk, client side applications versus service side applications, we've talked about -- there's a reason that people are targeting databases. If I'm a hacker, if I can get access to 3000 credit card numbers, it's much more attractive than getting access to Deirdre's computer where you have access to one or if I'm a big spender four.

So, I think in thinking about risk, you really have to think about some of the risks that are created by your decisions about where to store data, because I think otherwise we're going to focus on hacking, and I think hacking is a tiny slice of the risk. Certainly in

many other industries, unauthorized use by people with permission to access data has frequently been the most atrocious cases of abuse.

MR. MEDINE: Lance?

DR. LANCE HOFFMAN: Lance Hoffman.

Well, Deirdre gave me a lead-in here, because I also want to talk briefly about risk analysis. I think we have to understand there is a -- there's always a tension between usability and security, and the issue is striking the balance. The first question there is who decides, okay? But in terms of risk analysis, I will expand that to include cost-benefit analysis, including the social costs.

This is something that is hard to do, and so there are not a lot of computer security products or services in risk analysis as well developed as in some other areas, like firewalls or intrusion protection or things like that. The reason is it's hard, and it also gets into religious arguments at times, what is the best religious -- what is the best risk analysis, what is the methodology you should use.

To give a simple example, are we considering the expected values or the worst case? And whose expected value or whose worst case, okay? We really ought to -- and over what time period? So, I would urge that when

we look at the security issue to look at the specific technologies, for sure we ought to do that, but in addition, look at the big picture, look at the risk analyses and see, following up on what Deirdre said, what fits for the consumer and for the business.

To compound things, this gets tied in with architectural problems. We build computers today in some sense like Henry Ford built cars, you know, he didn't put in seatbelts or air bags or things like that. Things are going to get better over time, but, you know, we're not there yet. So, when we look at what security is built in and in particular where the defaults are set, the defaults in some sense for security are set in just the wrong places. If you look at logging, well, turn logging off, it generates too much information. In terms of cookies, well, it's very useful, so we will leave cookies in, so that sort of thing. So, we have to look at all of these things when we look at security.

MR. WADLOW: Tom Wadlow, Pilot Network Services.

I wanted to echo some of the things other folks are saying and perhaps expand on them a little bit, and there really are two categories of abuses, as Deirdre was pointing out, people who are actually authorized to

use the information, who have access to it, and then the abuse of people who are basically getting access to it through some unintentional means, which I think leads to a point of general system security.

You can have a web server that's very well designed, perhaps uses SSL, perhaps has wonderful authentication, but if the entire system that is used to implement that web server is not as equally well secured, if there's maintenance access to it, for example, that's not correctly authenticated or things that are in the clear that shouldn't be in the clear, you can have a number of problems that -- people getting access to that machine not through the expected channels but rather through some unexpected ones.

Another issue I wanted to raise is that we talked about the two issues of data in use on a machine and data in flight. There's also a number of subsidiary maintenance issues that come with that, also. For example, I don't have to break into a computer to get access to data if I can manage to stick one version of the backup tape in my pocket and walk away with it. That contains the sum total of everything that's on that machine if it's not properly stored, if it's not properly encrypted. So, having sort of a minimum window of visibility for data, such that it's encrypted except

when it's actually used at this precise moment, is a very important principle for keeping the system security.

DR. SCHUTZER: I just wanted to give one point of clarity and then go on to something else.

There aren't really any laws that protect people with credit cards. That's voluntary on the part of the associations that provide those type of limits on the exposure, and that also includes the debit card world.

MR. MEDINE: Point of clarification, the Fair Credit Billing Act does limit liability of unauthorized use to a maximum of $50 for credit cards, and there's also --

DR. SCHUTZER: Voluntary, also, though.

MR. MEDINE: No, mandatory, and there are debit card limitations, although the associations have gone beyond the legal requirements in terms of debit card liability, but credit card liability is mandated by law, just to clarify.

DR. SCHUTZER: Right, but there is this voluntary on the debit card.

MR. MEDINE: Right, right.

DR. SCHUTZER: I think we all agree that security is not going to be perfect and that authentication is one of the weak links, not the only

weak link, hacking is another weak link. In fact, if you look at hacking, it might mean that websites that just have limited information can be taken from some other sites, combined in ways to make them just as potent as sites that have more information. So, I think you have to look for ways to protect consumers that create a tension between the privacy and the protection. That's to say that a lot of information that we will collect on consumers to learn patterns of shopping are there to allow us to detect anomalies that will allow us to come back and contact consumers and alert them to suspicious activities and also to allow us to in many cases, with their permission, revoke the card number and provide new card numbers.

So, I think there's this tension we have to look at, that if you assume that security is not going to be perfect, now or for the foreseeable future, then there will be this tension in terms of usage of what information you might want to collect and not want to share in terms of protecting your customers and protecting foul play.

MR. MEDINE: Larry?

DR. PONEMON: Like everyone else it seems, I'm not a gear head, I admit it, I'm an auditor, an accountant. Don't hold that against me, though, but

there's two issues. First, one thing I realize -- well, let me just start by telling you where I work in the New York City office of PricewaterhouseCoopers, right across the hallway is our hacker lab. It's really a cool place. I mean, we have these people who are professional hackers, and their whole job is to break into our clients' systems and test the infrastructure, and, you know, and then they brag, and they're very loud, so I hear their stories, and it's great. I can't get any work done, but it's great.

They talk about all the systems they break into in a day, and some of the systems they break into are folks in companies that are represented here. But the moral of the story -- don't worry, don't worry -- but the moral of the story is that I think that if you think that there's a level of security that would be acceptable today, I don't think -- I don't think a company would be able to spend that much money, okay, without going bankrupt. So, I think that the second best solution is disclosure. Let people know, as we let them know with the privacy statement, let them know what level of security exists.

Now, of course, there is going to be tension between the issue of, you know, your intellectual capital in terms of how you do security, and, of course,

you don't want the bad guys to know how you do it, right? That would be bad news. But I think there's a way of disclosing a level of security.

Now, there's the flip side. As the user of technology, security is impressive, right? Do you ever forget your password or, you know, it's always your mother's maiden name when you have to call in for, you know -- you always forget that special code, and it takes like five hours for you to get another password, and you can't do your business. I think most consumers today would actually forego a level of security in order to get the job done, but that's today. I think if people start experiencing -- see the universe of experience, and it happens in many places, I think there's going to be a much more serious and greater appreciation for security.

MR. WADLOW: I'm sorry, I have to leap right in, I have to strongly disagree with one thing you said. Tom Wadlow, Pilot Network Services.

You said the level of security to keep things safe is something that would be oppressively expensive. In fact, I am a gear head, I actually do this for a living, and most of the things that people find about security when you do audits, what you discover is that mostly it's the very simple things that haven't been

done right, cheap, inexpensive things, but I think it's very important to remember that security really isn't the level. It's not a place; it's a process. It's a crank you have to keep turning, and it's not so much how you've done it but measuring how often you're turning that crank that really determines the level of security.

DR. PONEMON: May I respond? Larry Ponemon again.

The bottom line is you can measure it, you can disclose it, there is no question about it, because it's been done. There's a lack of consistency, however, and I think that needs to be established first. The point I was trying to make is a fail-safe system is impossible, but there are levels of security. Going from zero to 95 percent is relatively inexpensive; going from 95 percent to 99.9 percent is prohibitively expensive.

MR. WADLOW: Completely agree, but most people are at 2 percent, which is --

DR. PONEMON: I hope not.

MR. WADLOW: It's true, they are at 2 percent.

MR. MEDINE: Just to add on, from the Commission -- this is very useful, as the whole discussion is, but one particular point that's been raised here that I think would be useful for this committee to give some

views on is the level of notice to consumers about security, because really there are two issues here. One is should you have security as part of fair information practices, and the second is should you disclose to consumers that you have security, and I think the committee's views on the relationship between those two would be extremely helpful.

Ron?

MR. PLESSER: Well, that was a good segue to my comment, because I was going to talk about, you know, wearing the emperor's clothes here, but why are we discussing this? I know security is an FIP and something that you want some input on, but there's a lot of law on security. I mean, public companies have an ongoing requirement to keep their property protected. The SEC has rules. We have an electronic communications Privacy Act, we have computer fraud and abuse, we have a lot of statutes and a lot of law that requires security.

So, I guess the question -- or the law allows, I guess, somebody to protect themselves, but the question I'm really asking is what's the goal of this conversation in connection with the Federal Trade Commission? And maybe, you know, this last little concern is that it defines notice, how much security

should be in a web notice, but I mean I don't -- just I sit here and I'm kind of scratching my head.

The Federal Trade Commission is not going to set, it would seem to me, security standards for the web or for the net or for communications, or are they? I mean, this is very helpful conversation, but in the end of the day, we're supposed to advise you about things that are really within the scope of and things that the Federal Trade Commission is going to do, and I think it would be helpful to me and maybe to others -- I understand access, and I -- but on security, it's really a different issue.

What is -- what is the -- where is the Commission going? Where do you -- I mean, what is the question? Security is not a good enough question. It's like what security or why security? What is it that we're supposed to come up with a recommendation on? Certainly not setting up technical standards on the level of security or when security -- you know, what bit lengths are appropriate. Clearly that's not where the Federal Trade Commission is going. Where is it going and what is the advice that -- maybe the consumer notice is one area, but I'm a little confused about why we're having this conversation and where we're going.

MR. MEDINE: Let me just respond in part to

that.

Security is a fair information practice. One of the main reasons for having this advisory committee is to have just the discussion that you just posed, which is what does that mean out there in terms of -- and we are, again, not in the context of setting standards but in the context of looking at what self-regulation has done with regard to this particular fair information practice, and the question is, should it be a notice standard, should it be a performance standard?

I don't think anyone is into setting technical standards and specifying one technology over another, but should there be a notion that consumers' data that they give to a website, it's fine to have notice and choice, but if the data is freely accessible to anybody, is that really the kind of privacy that people expect online?

So, the question is what security should sites be offering to the data that's in their databases, what security should be offered in transmission, and then something that only the to that, what level of notice, and are those two something that only the. They are all points that exactly -- if we had easy answers to those, we wouldn't need the advisory committee. We have the advisory committee to help us flush those out, which is

why we're all here today.

MR. PLESSER: One response to that, it's not quite security to me if you go on the usegroup or usenet, dejavu.com or whatever it is, there will be a public record. That's not really a security issue. That's understanding the nature of what you're transacting. That is a notice. I mean, people should know that when they go into those sites.

I think security is really a different issue, which is more, you know, is the -- the thing Stewart was talking about, but the question is, you know, how deep is the Commission likely to get into that level of the conversation?

MR. MEDINE: Well, again, we are looking to you to direct us on that, but getting back to the sliding scale concept, which is there may be at the extreme of the sliding scale is a product group or a use group where there may not be an expectation of privacy and providing your credit card number and personal information where there may be a high expectation of privacy, and the question is what security should be associated with that information?

Let me -- did you have a brief comment?

DR. CULNAN: One real quick. I mean, I think our focus could be to get away from the technical issue

would be it's an issue of creating consumer confidence, but if consumers are not confident that their information is secure, they -- e-commerce won't grow, and so I think that's the response.

MR. MILLER: Greg Miller, MedicaLogic. I too am a gear head, those rusty as they may be, sometimes I wonder if I'm becoming a flight wheel, but two of the comments I made earlier, I think that security issues need to be considered in light of three elements, and this may foster discussion later that's been raised, and security is really about people, process and technology.

There are three elements there in our minds, at least in MedicaLogic, and it's probably worth remembering that the single greatest threat to data integrity is social engineering. Something on the order of 80 percent of all security breaches or compromises come from within an organization, and it's probably already been mentioned but I think it's worth revisiting that policies and procedures need to be factored in here.

I'm a gear head, so naturally I probably want to migrate to technology, let's talk about the sufficiency of two-factor authentication, but that's only a piece of it. Really what I think we can do here is remember that

privacy is the foundation, and security becomes a compliant -- a privacy-compliance matter, and security comes about by thinking about all three of those things, the three strands of a rope that create security.

So, I don't think we need to go down the rat hole of security details. There's plenty of people capable of doing that. But I think it is probably very worth us considering what do companies do in terms of policies, in terms of people and processes, as well? I think there's a balance there between those three.

MR. MEDINE: Jonathan?

DR. JONATHAN SMITH: Jonathan Smith.

I think the key question is -- in my mind is allocation of responsibility, okay, and what I mean by that is that there's kind of a tuning rod here between what the user does. So, truly paranoid users can be very, very secure if they choose to.

Allocation of responsibility has gotten a bit more complex because of the complexity of the systems we've built. So, for example, in, you know, days gone by, there was a reasonable expectation with the monolithic telephone company, which I used to work for many, many years ago that nobody is going to listen to your telephone call. That was an expectation that you had as a consumer, and it was, in fact, a monolithic

organization that owned all the facilities that, you know, in fact, the phone system was very secure as security goes, and any dents against that security usually had to be done with legal means, so the government would say authorize a wire tap. That was sort of the counter of the security provided by regular wired technology.

So, the responsibility has, in fact, changed on issues like transport and storage, okay, and it's changed in very deep ways. I mean, one of the things that was commented is there are pairing relationships. Many companies now carry your traffic rather than Ma Bell, okay, and so, you know, the issue here is that, you know, you have some allocation of responsibility, and I don't -- I'm not trying to profess anything, but I'm saying that this is really an issue we should consider, is who's responsible for the security?

MR. MEDINE: Dan?

MR. JAYE: Thank you. Three points I want to make. The first is I think that there's actually a great level of security that's relatively easy to accomplish on the grand scale of things that is insulated for some of the employee issues and other issues that are brought up, which is something that only the to data minimalization. If you don't have the data,

it's very hard for an employee to misuse it or abscond with it, and I think that there are techniques such as anonymization of data, hashing and encryption of data, so that you can still meet your business needs, such as analyzing customer behavior, analyzing trends and patterns, without necessarily having to maintain it in identifiable form or even in reversible form, and there are challenges, such as avoiding a level of detail that allows triangulation, but once again, some of these techniques, and these are techniques that I've used as a database marketer even before I started Engage, can really enhance security.

The second point is making sure that the reasonableness test still allows for the entrepreneurial spirit of the internet, and I know it's very hard to say that we shouldn't have a minimum level of security for an e-commerce startup, but what we don't want to do is create a stacked deck so that only the ten largest e-commerce vendors have an opportunity to innovate and create businesses. And so we need to make sure, for example, that if we have a requirement for a certain level of security, it's okay, for example, for a third party to provide outsourced services to be able to allow a small player to provide the same level of security as a large player, which would intentionally mean that, for

example, some level of security would have to be delegated to a third party.

And then the third point is that there is a tension between -- or not a tension between security, but as we look at security and access and authentication, is that there may be contractual requirements and restrictions that require strong authentication, and so as we balance the levels of authentication needed for access to different data, it's not just the sensitivity of the data, but, for example, if you have made a representation that you will not share data with third parties, even if the data's relatively innocuous, the question is if you don't have sufficient security and a third party can get access to that data, have you breached your either -- your responsibility under deceptive trade practices if you've made a privacy statement on your site saying you don't allow third-party access or contractual requirements with your partners? So, those are the three points I'd bring up.

MR. MEDINE: Thanks. Let me just -- a couple of things, that was Dan Jaye for the record.

We have about five more minutes for this discussion, so we can take a few more comments. Second, for those in the overflow rooms who want to participate

in the public comment session that follows, please come to Room 432, because we will be -- invite people to present their views in person to the room.

Stewart, did you have -- Stewart?

MR. BAKER: Just three or four things that I would like to get on the list. First, on the question of relevance, actually, I think if you're subject to the new financial privacy requirements, you've already got all of these obligations with respect to security as legal obligations, and we'd better -- I think the FTC has some enforcement authority. So, it would be useful to assist the Commission in that regard.

Things that I think that belong on the list, costs of security in terms of technology impairment. The Federal Government is famous for buying secure products that are two years out of date, if that's the best you can do if you want a secure product, at costs to consumers. There are real costs to consumers if you're -- if it takes ten minutes extra to double-check whether the state trooper who's calling in from an accident scene has authority to get your medical records, you're going to be a pretty unhappy consumer.

Authentication versus anonymity, I think there's a fundamental tension, we've talked about that in the context of privacy, but I think it's a particularly

serious problem here. We've seen privacy groups prevent the deployment of authentication technology that would have actually assisted in security, and we ought to address that issue.

And finally, on security disclosures, I think the question is is it possible to write a requirement for a security disclosure that will produce meaningful information, and my guess is not. I think that's the real question. My guess is that by the time you factor in the abstraction difficulties plus the ability of people to claim a lot of stuff about their security that doesn't really tell you anything, that disclosure isn't going to help consumers.

MR. MEDINE: We have time for four more quick comments, and then the -- that's the bad news. The good news is we all get to see each other again soon and can continue this discussion. So, don't feel that you don't have another chance, but I have Deirdre, James, Rick and Lorrie, the final commenters, and again, I'm sorry with the time, but again, we will be exchanging views in subgroups, electronically, and I think personally here again in a few weeks.

Deirdre?

MS. MULLIGAN: Deirdre Mulligan.

I actually wanted to concur with the point made

by Mr. Baker and also take issue with him. I want to concur on the question of market failure, and I think authentication technologies are an area where we're very likely to see a market failure from this perspective: The people who are deploying the technology, if there are not appropriate liability rules, are not the ones who bear the ultimate risk of harm, and I think that's something that we've seen in the credit card industry, where there are liability rules, because, in fact, credit cards are not all that secure, and therefore, because consumers are the ones who would bear the cost, as in the financial cost or the bill, the liabilities -- the liability rules were set so that we could have a probably less secure technology than the marketplace would otherwise stand, because the liabilities were structured in a way that appropriately balanced security and liability from the consumer perspective. So, I do think that there are issues about how when one party bears the risk and the other designs the technology, whether or not you have a market failure, and I think it's likely that there may be areas where we do.

On the question of stopping the deployment of authentication technologies, I really do feel a need to respond. Authentication technologies can be useful for security. They can also be designed in ways that are

not useful from a security perspective or a privacy perspective. I'm sure we agree upon that. I think the question of how you design authentication devices that serve all those interests really deserve very particular attention, and there are very specific reasons why we have challenged the deployment of certain technologies. We don't think that a single key for every door is good for security or privacy, and I think that's probably a value we share.

MR. BAKER: That's why this is going to be so much fun in the next few sessions.

MR. MEDINE: And remember, you don't have to reach agreement.

James, very quick comments, if we could wrap up the session.

MR. ALLEN: This is James Allen.

The problem of authentication for us I think is very gnarley, I don't know how else to put it. The classic authentication systems that people have been referring to are designed to answer the question are you the person who was granted authority to access this account? And what we're trying to do is give consumers or talk about how to give consumers access to information that's been collected about them from a variety of sources.

So, we have to answer the question are you the person that this information is about, and that's a very, very different question, and it's a very difficult question to answer, because we all are known by many aliases, initials, different names, different addresses we've lived at and so forth. And furthermore, in many cases, the people we want to protect that information against being accessed inappropriately by are the people who know all of our aliases, because they are our ex-wives or ex-husbands or employers or et cetera.

So, I don't claim to have any answer to this problem, but I think the authentication problem is particularly gnarley in this space.

MR. MEDINE: And it sounds as though that's the advantage of having these two groups together, access and security, because that seems to be the cross-over point, authentication, so it would be useful to hear the two groups' views on that.

Rick?

MR. LANE: In terms of market forces, and we heard a lot about CD Universe, I don't think a company out there ran to see what CD Universe's security was to go buy it. I'm sure CD Universe was not advertising, and look at the impact on us. The interest was on CD Universe and their customers, but there was also a heavy

toll paid by the business that allows for the security breach. So, there are already in the marketplace ramifications for unsecure data. So, we should make sure we balance that.

In terms of liabilities and having something -- standards written or some type of notification, again, from the market standpoint, I would think that most businesses would want to tout when they have strong security, and a customer would feel comfortable with that. Just like privacy statements, it's good business to have a strong privacy statement, because you want businesses to go there. It doesn't have to be mandated or put into regulations, but businesses are going that way, like AOL and Microsoft and others, because it's good business sense, because their customers are happy, and that gets to consumer confidence.

MR. MEDINE: Thanks.

A final comment from Lorrie?

DR. CRANOR: Hi, Lorrie Cranor, I'm in the secure system research group at AT&T.

I have two quick points, one to put on the table a question which I think has been raised by some of the recent security breaches, and that is what responsibility, if any, does a company that has had a security breach have to notify their customers that

their data may be at risk? And that's just a question.

The other is to bring up the user interface issue of security. As we have more and more websites that consumers are interacting with and they're getting passwords and they have to authenticate themselves, people are getting 20, 30, 40 passwords. We give people advice that they should pick strong passwords, they should pick different passwords. The reality is the average person cannot remember more than four passwords, and so when --

MR. MEDINE: If that.

DR. CRANOR: -- and so what happens is that people write their passwords on yellow sticky notes and stick them to their monitors, and this is very -- this is not good. I'm not expecting this committee to solve this problem, but I think highlighting that there's a big user interface problem with security I think would be a good thing for us to do.

MR. MEDINE: Thank you all again for a very lively discussion, and I think we'll have plenty of things to talk about over the coming weeks. We will return to both of these issues in terms of going forward, but this is an opportunity for the public to present its views, again, because this advisory committee is very much an open process, and so if there

are individuals who would like to come forward, there's a microphone here, and present their views to the committee, this would be the chance to do so. There's people standing there. I don't know if they're here to observe or speak, but anyone who would like to give their comments is welcome to do so.

Well, the public is still pondering these issues, I think. Okay, I see a familiar member of the public. If you could identify yourself, that would be helpful.

MR. HENDRICKS: Evan Hendricks, Privacy Times.

The Privacy Act requires federal agencies to take reasonable steps to guard against anticipated threats. That is a very vague standard, but it is a standard which to me means that you have to do something as opposed to doing nothing, and I think it's a good standard to start from.

Now, what I think is you take that standard and you take the work of Richard Smith, and every time he scratches around or 'Smiths' a company, he's finding you serious security problems, because their systems are configured to capture data in ways that aren't transparent to the user. So, I would like, you know, to raise that that standard, coupled with the realities of what Richard is turning up, shows that there's serious

work that needs to be done in this area.

MR. MEDINE: Any response or any other public comments?

MR. MCNULTY: I've got one.

MR. MEDINE: Okay.

MR. MCNULTY: My name is Len McNulty, I'm with RSA Security, and in a prior life, I was a manager with several large firms, ADP Security for example, and I was struck by kind of the disclosure focus in the discussion on security, and I'm sure that in Dr. Hoffman's computer security 101 class that the computer security also looks at the availability and integrity of information, and that's usually the way it's defined in the Computer Security Act for federal agencies, and I think that this group ought to least make a conscious decision whether you are going to include those issues or not in your discussion on security.

MR. PURCELL: Richard Purcell, Microsoft.

One of the issues that hasn't been brought up around security, we have talked about unauthorized access, internal and external, we have talked about unauthorized transmission, that type of thing. One of the underpinnings I want to reinforce here, security involves the security against the loss or corruption of data, as well, and that's an important point. It's not

-- it's one thing to lock it up and make sure it's used properly and accessed properly. It's a whole another thing when it's encrypted well to be able to encrypt it equally well, and so the data doesn't suffer severe corruption or even loss.

DR. LANCE HOFFMAN: Lance Hoffman.

I think in response to what Mr. McNulty was saying, there's a good acronym you might want to use, CIA, cover all the aspects of security, confidentiality, integrity and availability, because availability goes directly to consumer confidence.

MR. MEDINE: Any other comments? Rick?

MR. LANE: Just to make a plug -- this is Rick Lane, U.S. Chamber. Just to make a plug, the chamber, as part of our educational efforts, we are hosting a conference at the end of March on the issue of network security, so we invite you all to attend and listen.

MR. MEDINE: As long as it doesn't conflict with one of our meetings.

MR. LANE: No, it doesn't.

MR. MEDINE: Any other members of the public like to make any comments?

Okay, if there aren't any, I would propose again a five or ten-minute break so that we can put our thoughts together and then propose a subcommittee

structure for your consideration. Thank you.

(A brief recess was taken.)

MR. MEDINE: Okay, thank you, let's get started again.

Okay, thank you for coming back. The next item of business is where we go from here, which according to our plan is to create some subgroups, to go off and create detailed outlines based on the issues that were raised during these two discussions, and then to circulate those outlines two weeks from today, so February 18th by close of business, send to advisorycommittee@ftc.gov. Each person obviously can designate a person to forward those to us, but to send us the detailed outlines flushing out the issues that we've discussed today. Those outlines will be posted on the website, the advisory committee's section of the website, and will serve as a basis for the discussion at our next meeting, which will be the week following the 25th.

So, we would like to move now to assignments. We've divided this up into eight subgroups based on the discussion so far, and if you do the math, that means roughly four to five people on each group.

Now, there may be people who are dying to be on more than one group, there may be people dying to not be

on any groups. Let's see how it sorts out. Let's try sort of one person per group, but if there is something that you have tremendous expertise or interest in, we can have maybe one or two assignments per person, but let's try to spread the wealth a little bit.

Again, remember, this is only a two-week assignment, and in the sense that you'll have an opportunity to group differently or work on different issues after the next meeting, this is really to help the group flush out these issues so that we can have -- I can't say a richer discussion, because we had such a tremendously rich discussion today, but to continue the discussion and bore down on some of these issues.

So, on the issue -- on access, the staff of the committee -- of your committee are proposing I guess the following four groups, and obviously if there's strong opposition to these breakdowns, I'm sure we'll be hearing from you now.

The first is -- relates to the scope and categories of the types of information involved, that is, that you would want access to, and we heard a number of issues relating to whether -- from or about consumers, what sources of information commingling, clickstream, aggregate, anonymous, all sort of issues in the same general category of scope and categories of

information.

The second relates to entities, and that involves, as was discussed earlier, affiliates, third parties, joint ventures, single and multiple data sources, chat rooms, the sort of broad categories of entities dealing with information.

The third relates to costs and benefits, to try to quantify those both for business, in providing access and benefiting from access, and to consumers, likewise, and the cost of not having access to their own information.

And then lastly, authentication and technology, and we heard about the tremendous importance in the access area of making sure you're giving access to the right person, so ensure you're giving access, what steps to take to ensure you're providing access to the right person and so forth.

Those being the four groups, unless I hear a strong objection, obviously within those groups you're free to cross group lines if you feel it's appropriate to your group in terms of the discussion, because again, this will all be coming back to this larger group.

I propose, though, and I guess I would propose people -- yes? If you could identify yourself?

MR. WHAM: Ted Wham from Excite@Home.

Those are very good breakouts from those. I have a fear that number one is going to be swamped by interested parties and will be very, very large, and it might need to be broken down further.

MR. MEDINE: Okay, well, let's try and see how -- if people will want to -- we will take one first, and maybe people will -- oh, okay, good point.

Just so you can do comparison shopping, we thought it only fair that you consider your alternatives in security so you can put your efforts in the right places. The four subcommittees we would propose in the security area are standards, and we heard a lot about how -- should there be standards, how should we set the standards, do market forces help set the standards, what are the social costs and sliding scales and so forth, as one sort of general category of standards.

The second is managerial steps to protect data, and we have heard about access control, monitoring access and so forth.

Technical steps to protect data, and we have heard about encryption and firewalls and so forth.

And lastly, appropriate disclosures to consumers, and we've heard about the interplay between what you do and what you say you do and how that relates to fair information practices and privacy.

So, again, we propose standards, managerial steps, technical steps and appropriate disclosures in the security area.

MR. PLESSER: Ron Plesser.

It seems to me that there's at least some basis here of a fifth committee, which is existing legal structure and where does the security kind of fit in. As Stewart pointed out, there's sections of the Financial Act that has it, there's a lot of requirements sitting around, and it seems to me that particularly in security, without looking at it in the context of other laws and requirements is difficult, but that would be my suggestion.

MR. MEDINE: I guess we had envisioned that as being part of the standards discussion, and I guess the question is just in terms of management, if we could fold that in -- I think it's an appropriate consideration, if we could fold that into the standards group as one of their considerations.

Also, I guess I should also add that cost-benefit is probably a critical component of all of these groups in security, and I hope that all the groups consider cost-benefit issues in evaluating standards, managerial steps, technical steps and disclosures.

DR. PONEMON: Larry Ponemon,

PricewaterhouseCoopers.

I suggest on the disclosure we also add the word assurance, disclosure and assurance.

MR. MEDINE: Okay, that's done.

DR. PONEMON: Thank you.

MR. MULLIGAN: Deirdre Mulligan.

I second the concern that many people will want to be in the first access panel, but I think it's because in looking at either access or security, the first thing that we need to do is figure out access to what, security of what, and I'd like to suggest that perhaps that the definitional issue of what it is that we're talking about, while I think that there could be a small group to take a first crack at it, that you might even want to separate that out into scope and categories.

MR. MEDINE: Okay, the question is -- remember, these are first cuts for the group to come back to the group to consider, and there's some concern about managing too many subgroups, but why don't we see how that number sort of -- maybe we should start with security first and get some -- peel off some people and go from there, but we -- you know, obviously, again, you're free to talk to people in the subgroups, you're free -- you will all have a chance at the next session

to discuss the subgroups' work.

DR. LANCE HOFFMAN: Lance Hoffman,.

I want to make sure I understand the process.

So, you're suggesting that we now volunteer for one of these eight groups?

MR. MEDINE: Yes.

DR. LANCE HOFFMAN: And then you're stuck with dealing with what's left.

MR. MEDINE: Well, let's see what happens. We want volunteers, and again, just for the purpose of the next two weeks. You are free to regroup as we move forward. Really just to go back and help this group develop in more detail some of these concepts in the form of a detailed outline for consideration at the next meeting.

MR. WHAM: Ted Wham from Excite@Home.

Just as a suggestion for process, why don't we just do a straw poll on how people are playing out amongst the eight different groups and see whether breakup is required.

MR. MEDINE: Okay, fine.

Well, do you want to start with --

MR. DAVID HOFFMAN: David -- can I make a comment first?

MR. MEDINE: Sure.

MR. DAVID HOFFMAN: David Hoffman.

My concern is how we have split this up, how we have the hard split between security and access, we will duplicate a lot of work on key definitions, like the definition of personally identifiable information and some of the general work that would be done on the framework and the background. So, I would suggest that there be some sort of a committee that would pull together their recommendations for the key definitions that will apply to all of the work.

MR. MEDINE: Well, again, the question is whether as a management issue that's doable. Again, I don't think there's any harm in some of the groups' efforts overlapping, because again, it will all be compiled again in two weeks and we will all be enriched by the whole range of possibilities. So, I don't think -- again, it's not that you have to be in this group forever.

MS. SWIFT: With the caveat that other people opened up the process issue, I think the work of the subcommittees is going to be most helpful if it covers the breadth of interests represented around this table, and my concern from a process standpoint is by this voluntary raising of hands, it doesn't give us a good or you a good opportunity to guarantee that each

subcommittee represents those breadth of interests and that one or the other not become dominated, and if, in fact, that happens, two weeks of intense work may not be as useful as would otherwise occur.

MR. MEDINE: And so I guess the alternative is?

MS. SWIFT: Not to -- I never want to delegate all responsibility to appointed government officials, in fact, it's against my nature, but were folks, similar to picking courses in college, to submit a ranked level of what they're interested in, you all, not to create more work, would then be able to make assignments which did reflect the -- I hope what would be the consensus of the group, that we would like the committees themselves to represent the same breadth and the same success that you've had in putting together the larger group.

MS. MULLIGAN: I'd like to second that.

MR. MEDINE: Well, if asked, we will serve. You know, we typically in terms of the private sector encourage the private sector to lead, but if you would like the government to assist you, then we will be happy to.

MS. MULLIGAN: No, we would like you to manage.

MR. CERASALE: Jerry Cerasale, DMA.

One of the things in following that group, though, or that approach is we lose today. If we

determine today what the subgroups are, we can meet right now and at least set up what we're going to do. If we go this other route, we're at least extending -- we have a short time period here, and we're losing at a minimum a day, and this is a Friday.

MS. MULLIGAN: Why don't we do it right now.

DR. LANCE HOFFMAN: You can recess for ten minutes and --

MR. MEDINE: We will take another recess.

MS. MULLIGAN: How many choices, though, four choices?

MR. MEDINE: You can submit your choices and --

MR. PLESSER: I like the idea of the straw poll first and then see --

MR. MEDINE: Well, people who have extraordinarily strong feelings I'm sure will approach us, so let's take a ten-minute break and we will at least propose a committee allegation. Actually, if you want to come up and express a strong view about which subcommittee you want to be on, that's fine. We will reconvene in about ten minutes.

(A brief recess was taken.)

MR. MEDINE: Please take your seats. Okay, thank you very much.

Okay, we have done the best job we can, trying

to take into account people's preferences and expertise. I don't think we can necessarily suit every preference or necessarily have every committee have everyone on it, but again, the benefit is it's a very transparent process. All the work results will be out there, and we are not going to make final decisions at the next meeting, so there will be plenty of opportunity to revisit issues.

Starting off with the first access group, which is on scope and categories, the following, Richard Bates, Fred Cate, Jerry Cerasale, David Ellington, Tatiana Gau, Josh Isay, Daniel Jaye, John Kamp -- this is the biggest one -- Deirdre Mulligan, Andrew Shen, Frank Torres and Ted Wham.

The second group, which is the entities group, is Alexander Gavis, Robert Henderson, Deborah Pierce, Art Sackler.

The third is cost and benefits, Steve Cole, Alexander Gavis, Rob Goldman, David Hoffman, Rick Lane, Daniel Schutzer, Richard Smith, Jane Swift and Deirdre Mulligan.

And the last is authentication, James Allen, Steve Casey, Lance Hoffman, James Maxson and Richard Purcell.

On security, the first group is standards, which

is Stewart Baker, Mary Culnan, Rick Lane, Ron Plesser, Jonathan Smith.

The following two groups are going to merge, managerial and technical, so on a combined managerial and technical, and obviously they are very interrelated issues, Deborah Pierce, Rebecca Whitener, Steve Casey, Lorrie Cranor, Greg Miller, Daniel Schutzer and Tom Wadlow.

And lastly, on disclosures, Paula Bruening, Larry Ponemon, Andrew Shen, John Kamp and Lance Hoffman.

Oh, Frank Torres will be added to the access authentication.

We encourage you all to get together among yourselves. We will be the contact people, if you need to, Hannah Stires, who is over there, can get in touch with you. Any questions, call us, e-mail us at advisorycommittee@ftc.gov.

MR. PLESSER: First, can we feedback with you a little bit on these assignments offline, and can you maybe send an e-mail or a posting this afternoon of the names on the lists?

MR. MEDINE: Yes, we will do that.

DR. JONATHAN SMITH: I would also suggest e-mail exploders.

MR. MEDINE: Which are?

DR. JONATHAN SMITH: Well, like a list, like a name like standards -- security standards at, you know, some -- some address so you can just send it and it broadcasts to everyone.

MR. MEDINE: Okay, we will explore some of the technical issues. I would ask you to -- for recycling purposes -- to give the name tag in the basket to Hannah as you leave. Thank you very, very much for engaging in this, and we look forward to seeing you at the next meeting.

(Whereupon, at 1:30 p.m., the meeting was adjourned.)

- - - - -

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 4, 2000

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: 2/10/00

SUSANNE Q. TATE, RMR

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