

0176

1 FEDERAL TRADE COMMISSION

2

3

4

5

6 ADVISORY COMMITTEE ON

7 ONLINE ACCESS AND SECURITY

8

9

10 9:00 A.M.

11 FEBRUARY 25, 2000

12 VOLUME 2

13

14

15 FEDERAL TRADE COMMISSION

16 600 PENNSYLVANIA AVENUE, N.W.

17 ROOM 432

18 WASHINGTON, D.C.

19

20

21

22

23

24 REPORTED BY: SUSANNE Q. TATE, RMR

25 DEBRA L. MAHEUX

0177

1 A T T E N D E E S

2

3 FEDERAL TRADE COMMISSION:

4 David Medine

5 Jessica Rich

6 Hannah Stires

7 Allison Brown

8

9

10

11 COMMITTEE MEMBERS:

12 James C. Allen, eCustomers.com

13 Stewart A. Baker, Steptoe & Johnson LLP

14 Richard Bates, The Walt Disney Company

15 Paula J. Bruening, TRUSTe

16 Steven C. Casey, RSA Security, Inc.

17 Fred H. Cate, Indiana University School of Law

18 Jerry Cerasale, Direct Marketing Association, Inc.

19 Lorrie Faith Cranor, AT&T Laboratories

20 Mary J. Culnan, Georgetown University

21 E. David Ellington, NetNoir, Inc.

22 Tatiana Gau, America Online, Inc.

23 Alexander Gavis, Fidelity Investments

24 Daniel E. Geer, @Stake, Inc.

25 Rob Goldman, Dash.com, Inc.

0178

1 COMMITTEE MEMBERS:

2

3 David Hoffman, Intel Corporation

4 Lance J. Hoffman, George Washington University

5 Josh Isay, DoubleClick, Inc.

6 Daniel Jaye, Engage Technologies, Inc.

7

8 John Kamp, American Association of Advertising Agencies

9 Rick Lane, U.S. Chamber of Commerce

10 Gary Laden, Council of Better Business Bureaus

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

12

13 Gregory Miller, MedicaLogic, Inc.

14 Deirdre Mulligan, Center for Democracy and Technology

15 Deborah Pierce, Electronic Frontier Foundation

16 Ronald L. Plessner, Piper, Marbury, Rudnick & Wolfe

17 Lawrence A. Ponemon, PricewaterhouseCoopers, LLP

18 Richard Purcell, Microsoft Corporation

19 Peter Reid, NCR Corporation

20 Daniel Schutzer, Citigroup

21 Andrew Shen, Electronic Privacy Information Center

22 Richard M. Smith, Internet Security Consultant

23 Jonathan M. Smith, University of Pennsylvania

24 Jane Swift, Commonwealth of Massachusetts

25 James E. Tierney, Former Attorney General, Maine

0179

1 COMMITTEE MEMBERS:

2 Frank C. Torres, III, Consumers Union

3 Thomas Wadlow, Pilot Network Services, Inc.

4 Ted Wham, Excite@Home Network

5 Rebecca Whitener, IBM Corporation

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

0180

1 PROCEEDINGS

2 - - - - -

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

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

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

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

22 James Allen? Please signify by saying "here"

23 or "yes."

24 MR. ALLEN: Here.

25 MR. MEDINE: Stewart Baker? Not present.

0181

1 Richard Bates? No response.

2 Paula Bruening?

3 MS. BRUENING: Here.

4 MR. MEDINE: Steve Casey?

5 MR. CASEY: Here.

6 MR. MEDINE: Fred Cate?

7 MR. CATE: Here.

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

9 Cerasale?

10 MR. CERASALE: Here.

11 MR. MEDINE: Very dramatic.

12 Steve Cole? Gary Laden substituting by

13 written permission for Steve Cole.

14 MR. LADEN: Here.

15 MR. MEDINE: Lorrie Cranor?

16 DR. CRANOR: Here.

17 MR. MEDINE: Mary Culnan?

18 DR. CULNAN: Here.

19 MR. MEDINE: David Ellington?

20 MR. ELLINGTON: Here.

21 MR. MEDINE: Tatiana Gau?

22 MS. GAU: Here.

23 MR. MEDINE: Alexander Gavis?

24 MR. GAVIS: Here.

25 MR. MEDINE: Daniel Geer?

0182

1 MR. GEER: Yeah, hi.

2 MR. MEDINE: Rob Goldman?

3 MR. GOLDMAN: Here.

4 MR. MEDINE: David Hoffman?

5 MR. DAVID HOFFMAN: Here.

6 MR. MEDINE: Lance Hoffman?

7 DR. LANCE HOFFMAN: Here.

8 MR. MEDINE: Josh Isay? No response.

9 Daniel Jaye?

10 MR. JAYE: Here.

11 MR. MEDINE: John Kamp?

12 MR. KAMP: Here.

13 MR. MEDINE: Rick Lane?

14 MR. LANE: Here.

15 MR. MEDINE: James Maxson?

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

17 me.

18 MR. MEDINE: He's here.

19 Greg Miller?

20 MR. MILLER: Here.

21 MR. MEDINE: Deirdre Mulligan?

22 MS. MULLIGAN: Here.

23 MR. MEDINE: Deborah Pierce?

24 MS. PIERCE: Here.

25 MR. MEDINE: Ron Plessler?

0183

1 MR. PLESSER: Here.

2 MR. MEDINE: Larry Ponemon?

3 MR. PONEMON: Here.

4 MR. MEDINE: Richard Purcell?

5 MR. PURCELL: Here.

6 MR. MEDINE: Peter Reid?

7 MR. REID: Here.

8 MR. MEDINE: Art Sackler? No response.

9 Dan Schutzer?

10 MR. SCHUTZER: Here.

11 MR. MEDINE: Andrew Shen?

12 MR. SHEN: Here.

13 MR. MEDINE: Richard Smith?

14 MR. RICHARD SMITH: Here.

15 MR. MEDINE: Jonathan Smith?

16 DR. JONATHAN SMITH: Here.

17 MR. MEDINE: Jane Swift?

18 MS. SWIFT: Here.

19 MR. MEDINE: Jim Tierney? No response.

20 Frank --

21 UNIDENTIFIED SPEAKER: I think he's here.

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

23 the door.

24 Frank Torres?

25 MR. TORRES: Here.

0184

1 MR. MEDINE: Tom Wadlow?

2 MR. WADLOW: Here.

3 MR. MEDINE: Ted Wham?

4 MR. WHAM: Here.

5 MR. MEDINE: Rebecca Whitener?

6 MS. WHITENER: Here.

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

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

18 MR. BATES: Here.

19 MR. MEDINE: Jim Tierney?

20 MR. TIERNEY: Here.

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

23 important and relevant documents relating to the

24 committee's work on the committee's web page at ftc.gov

25 and we have been sending e-mail updates to individual

0185

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

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

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

22 One business matter that I guess I'd just put

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

0186

1 make West Coast flights if the sessions end at 5:00 or
2 5:30. Is there any interest in the group in starting
3 earlier at our next meeting so that we can adjourn
4 earlier?

5 (Show of hands.)

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

9 MS. MULLIGAN: 8:00.

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

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

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

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

17 DR. JONATHAN SMITH: Excuse me?

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

20 MR. MEDINE: Well --

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

23 night instead of two nights.

24 MR. MEDINE: Okay. Should we accommodate our

25 West Coast visitors? I'm getting a lot of nods. Okay.

0187

1 8:00 a.m., okay. It's not the chair's favorite time
2 either, but in the interest of serving the committee,
3 as your designated federal officer, we will appear at
4 the appropriate hour, but again, we would be happy to
5 try to adjust this committee's work in any way that
6 meets the committee members' needs.

7 MR. TORRES: As long as you provide coffee.

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

13 UNIDENTIFIED SPEAKER: Can we nationalize
14 Starbucks?

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

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

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

22 In terms of our work today, what I propose

23 today is to go through the work of each of the

24 subgroups in order, that is, starting with access one

25 and working through security three. What I would like

0188

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

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

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

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

0189

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

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

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

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

13 MS. SWIFT: This is Jane Swift.

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

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

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

24 MS. SWIFT: I think that there seems to be a

25 lot of overlap, so the degree to which we can try to

0190

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

3 MR. MEDINE: Okay, point well taken.

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

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

6 Any other comments on that as a method of
7 proceeding?

8 Therefore, what I -- following up on that, I
9 again propose to work through each of the proposals.

10 We'll start in with access one and sort of aim to take
11 a break around 10:30.

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

21 Deirdre Mulligan?

22 MS. MULLIGAN: Deirdre Mulligan.

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

0191

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

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

16 Yes?

17 DR. SCHUTZER: Dan Schutzer.

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

22 MR. MEDINE: Some of the other subgroups or

23 within this -- within this subgroup?

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

25 MR. MEDINE: Okay.

0192

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

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

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

16 Andrew?

17 MR. SHEN: Hi, Andrew Shen, EPIC.

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

23 depends on the point of view.

24 MR. MEDINE: Is your microphone on? Just a

25 little closer maybe.

0193

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

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

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

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

16 MR. MEDINE: Deirdre?

17 MS. MULLIGAN: Deirdre Mulligan.

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

23 data might be very different if it's stuff that you

24 think could be very compromising, from a company

25 perspective it might be very important, but if you

0194

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

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

13 DR. SCHUTZER: Dan Schutzer.

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

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

0195

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

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

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

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

0196

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

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

10 MR. MEDINE: Okay.

11 Richard?

12 MR. PURCELL: Richard Purcell, Microsoft.

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

23 nightmare and would be very difficult to implement in

24 an accurate sense.

25 MR. MEDINE: James?

0197

1 MR. ALLEN: James Allen.

2 I agree with what Richard says partially.

3 First of all, I wanted to make a point that I think

4 sensitivity of data is critical to a lot of the things

5 we're discussing, but it's not critical to whether or

6 not you give a consumer access to the data about

7 themselves. I think consumers should have access to

8 the data about themselves in any case, but rather, that

9 the sensitivity of the data should dictate the means of

10 authentication, for example, used and so forth, and the

11 more sensitive the data is, the more you should do to

12 protect that data from inappropriate or unauthorized

13 access.

14 As far as -- back to the point Richard was

15 making, I absolutely agree that from a technology

16 standpoint, and I am a technologist, that it would be

17 very difficult to implement a system that allowed

18 consumers to, as Richard put it, nominate the

19 sensitivity for each individual data element. I think

20 that's why it's -- one of the many reasons why it's

21 critical to come up with some system of categorizing

22 data that puts it into relatively large grain

23 categories of a relatively small number so that you

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

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

0198

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

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

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

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

11 MR. MEDINE: Okay, Frank Torres?

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

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

16 MR. TORRES: Frank Torres.

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

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

0199

1 they have it.

2 Whereas if they have a bunch of other

3 information about me, say, you know, my account

4 balances and things like that, it might be important

5 that those numbers be accurately reflective of what my

6 creditworthiness truly is, then that's on a little bit

7 different level. Maybe we're -- you know, there's --

8 the sensitivity definition, but then you move on to

9 what -- then what does that mean as far as access goes

10 for that information and the value of access to a

11 consumer?

12 MR. MEDINE: So, just -- are you saying that

13 the more consumers know about what's being collected

14 about them -- well, that would affect the degree to

15 which access was important to them?

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

17 MR. MEDINE: Okay.

18 MR. TORRES: And David, this is Frank Torres

19 again, you made the comment should sensitivity be the

20 benchmark. I don't think there's any one -- you know,

21 what became clear working in -- within these subgroups

22 is I don't think there's any one element. I think

23 there's so many interrelationships going on here, it's

24 not just sensitivity. It is usage. And I'm glad that

25 the certification question or the certification issue

0200

1 came up, as well, because that's going to be an

2 important one down the road.

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

4 to that?

5 MS. SWIFT: Jane Swift.

6 I just want to say I think it is important that

7 notice not be separated from access when we're talking

8 about the sensitivity of information, but I would just

9 add that it becomes more important depending on the

10 usage of that information and its distribution to

11 people that we may not know it was given to. So, just

12 because you gave notice in the first instance, I think

13 access and sensitivity of information takes on a

14 different meaning -- I understand that's complicated,

15 but as it sort of goes into its third and fourth and

16 fifth generation of places that you don't know, people,

17 you don't know who they are or which information they

18 have.

19 So, just addressing notice in the first

20 instance doesn't solve the entire piece of access,

21 because you need to then know what you don't know,

22 which is where it went.

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

0201

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

5 Ron? State your name for the record.

6 MR. PLESSER: Ron Plessler, Piper, Marbury,
7 Rudnick & Wolfe.

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

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

23 list.

24 MS. MULLIGAN: May I just respond? Deirdre

25 Mulligan.

0202

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

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

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

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

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

23 transactional information, perhaps clickstream or other

24 information related to the transaction and then add on

25 information that may not have even come from the

0203

1 consumer? Are those three categories?

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

7 MR. MEDINE: Okay, Dan?

8 MR. SCHUTZER: Dan Schutzer.

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

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

23 consumers, and the people providing the database,

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

25 in the total cumulative sense of public and what can be

0204

1 done with it to both educate the public and ourselves,

2 so if they find that sensitive.

3 The other aspect of sensitive is just a

4 different kind of a way of looking at it. There is

5 some data sometimes that I would call sensitive which

6 is, let's say, if we're doing some kind of criminal

7 investigation, but it's not sure, it's alleged, you

8 know, we're just trying to collect this information, or

9 if the government suspects money laundering or

10 something like that, that's perhaps sensitive to not

11 want to have anyone to have access to. It's only

12 tentative. It's only investigating things, because

13 we're asked to investigate or we're suspicious and we

14 don't really have a firm case on it, and it would be

15 premature or wrong to provide that information,

16 perhaps.

17 MR. MEDINE: So, are you suggesting that there

18 be an exemption where there is --

19 DR. SCHUTZER: Yeah.

20 MR. MEDINE: -- illegal activity involved where

21 you --

22 DR. SCHUTZER: I think, so sensitive in that

23 sense, sensitive to not disclose the information.

24 MR. MEDINE: Okay, Lance?

25 DR. LANCE HOFFMAN: Lance Hoffman.

0205

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

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

23 was very important, which is these can be considered or

24 if you consider sensitivity, I think you have to

25 consider it as a default sensitivity.

0206

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

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

13 James?

14 MR. MAXSON: Jim Maxson.

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

23 determined by that individual, then it would be

24 literally impossible to implement. So, I think that

25 sensitivity really is an authentication issue, a

0207

1 security issue, and not so much an access issue.

2 MR. MEDINE: Well, let me just turn that around

3 just to clarify it for the group, because some would

4 say that you should not be entitled or provided access

5 to every possible bit of information about you and the

6 degree to which you should be provided access should

7 depend in part on the sensitivity. That -- obviously

8 I've just heard that from the group, but are you saying

9 that that's not the appropriate cut on the basic

10 question of who gets access to the information?

11 MR. MAXSON: No, I think probably a cut that

12 makes more sense to me would be the feasibility of

13 providing the information. I mean, one of the things

14 that we're tasked at looking at is the cost of the, you

15 know, proposals that could be implemented, and if

16 there's essentially no cost to provide all information

17 or very little cost, why not?

18 MR. MEDINE: Regardless of sensitivity?

19 MR. MAXSON: Regardless of sensitivity.

20 MR. MEDINE: And how would you assess cost on

21 an operational basis or say for -- in terms of setting

22 fair information practices or implementing those, how

23 would you -- would you do it on a company-by-company

24 basis?

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

0208

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

13 MR. MEDINE: Okay.

14 Mary?

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

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

0209

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

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

9 DR. CULNAN: Oh, yeah, yeah.

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

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

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

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

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

0210

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

4 MR. MEDINE: Okay.

5 Dan?

6 MR. JAYE: Dan Jaye.

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

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

23 shouldn't get stuck on sensitivity as being the reason

24 why things are in different categories. There are lots

25 of other good reasons to break something into two

0211

1 categories other than varying sensitivity.

2 And the final point in terms of sensitivity

3 being a consumer centric issue, I very much agree with

4 that. I do think that it may be useful to think about

5 data source or data controller as a way of thinking

6 about how things are categorized or set -- or how

7 sensitivity or access requirements are determined.

8 In other words, it may be that the data source

9 or the data controller has some degree of expressing

10 what the expected future access requirements are. So,

11 once again, data that's generated cooperatively or

12 generated sort of on, you know -- like, for example,

13 derived data is generated by a service. Once again, I

14 would say that the service probably has some degree of

15 influence over the access requirements to that data,

16 but at the same time, if it's highly sensitive and is

17 being used for making -- for decision-making

18 activities, then that might then bring on additional

19 access requirements for the consumer side.

20 MR. MEDINE: Just -- you would -- you raised

21 one point about sort of accessibility to the

22 information or keys to the information. Is that --

23 would you view that as another cut in terms of when

24 access is provided in terms of how essentially easy it

25 is or capable the firm is in terms of aggregating the

0212

1 information to provide to the consumer?

2 MR. JAYE: Yes, I -- one of the late cuts of

3 the matrix that we put together, I'm not sure if it was

4 -- was that -- was the idea of trying to matrix the

5 categories against the types of identifiers, whether

6 they were personally identifiable information, like

7 name and address, sort of online contact information,

8 offline contact information, globally unique

9 identifiers, locally unique identifiers, that there

10 would be different implications depending on each of

11 those, because implications of the data were different

12 in each of those situations.

13 MR. MEDINE: Okay, Alex?

14 MR. GAVIS: Alex Gavis, Fidelity.

15 I think to some extent, in terms of setting up

16 access, we can probably fairly easily sit down and come

17 up with sort of categories of data that we think would

18 be important to provide customers access to. I think

19 what's a more difficult decision here is at what point

20 does the data actually sort of escape the consumers'

21 hands and become derived data? And what I mean by that

22 is when essentially a company collects data about an

23 individual, if an individual voluntarily provides
24 information to open up an account with a company, for
25 example, the company has to then do a certain amount of

0213

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

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

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

18 Fred?

19 MR. CATE: Thank you, Fred Cate.

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

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

0214

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

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

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

22 Another source question is is it public source

23 data? If this came from an entirely public source,

24 something, you know, we have all been talking about

25 recently, what effect does that have? Do we want to

0215

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

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

13 Thank you.

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

23 company's doing with it. Therefore, they want to see

24 what's going on, but would you link that to the notice

25 where the company says we just collect your data for

0216

1 this limited purpose but no other, and therefore it

2 makes access irrelevant?

3 MR. CATE: I think you certainly could. I

4 think you are going to end up with multiple categories,

5 so you have a situation where frankly there is no

6 access and no notice because there is no direct

7 relationship with the consumer to start with, and that

8 to my mind would be the third party who's just

9 processing data along a chain from point A to point B

10 on the internet. If it happens to get stored in our

11 server along the way, I'm not sure we should have to

12 identify those people to provide notice or provide

13 access to it. We're not accessing the data in any way.

14 Why should anyone else be able to access it?

15 There might be the second situation where you

16 say notice is appropriate and appropriate -- and access

17 is not, so that we provide notice and it says, as part

18 of operations, we store e-mail messages on backup

19 tapes, and -- but we're not providing you access to

20 those backup tapes unless you show, you know, require a

21 specific showing, probably some form of wrongdoing or

22 something like that.

23 And then there might be a third situation or

24 there might be 300 situations where you would say

25 notice and access, and of course, they are closely tied

0217

1 together.

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

3 here.

4 Lorrie?

5 DR. CRANOR: Hi, Lorrie Cranor.

6 Two points. First, on the sensitivity, while I

7 think that it makes sense that the individual ought to

8 be able to best judge the sensitivity, I don't think

9 that's something that individuals can judge. I don't

10 think it's a meaningful question to ask somebody how

11 sensitive is a piece of data, especially when asked out

12 of context.

13 You give people a long list of data and say,

14 you know, tell me relatively how sensitive this is.

15 That's just not a meaningful thing to do. I think

16 people may be more concerned about how data is used,

17 but the question of sensitivity I think is too abstract

18 here.

19 On the access, I was reading the information

20 that the BBB provided us and their statement on the

21 kind of access that BBB seal holders have to provide I

22 think is maybe a useful starting point, where they

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

0218

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

10 MR. MEDINE: Ted?

11 MR. WHAM: Ted Wham from Excite@Home.

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

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

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

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

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

24 combination of data elements are working not in a

25 linear manner but in a geometric or exponential manner

0219

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

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

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

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

0220

1 those types of things.

2 We don't look at -- we don't let the consumer

3 come through and say you can't have this type of

4 information, and I would think that as a means of, you

5 know, providing standards of behavior, it's almost

6 impossible for the industry to come through and say,

7 I'm going to do a combination of the number of data

8 elements that I have crossed by the individual

9 consumer's sensitivity of that data element, I don't

10 know how I'd get there. And I think that was the point

11 made by Mr. Purcell from Microsoft.

12 The points about sensitivity of information,

13 and I sat on the committee, so I'm very familiar with

14 the construction of some of these elements, is that

15 there are some elements that you would come to and that

16 we would all likely agree, in a very broad consensus,

17 are sensitive information that would have a higher

18 threshold for disclosure and a higher threshold right

19 for provision.

20 Your -- whether you tested positive to an HIV

21 test is something that I think most people in this room

22 would agree is highly sensitive information. That's

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

0221

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

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

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

22 That was one of the reasons why we spent so

23 much effort breaking out the categorization itself, is

24 that we said there can be disagreement between, you

25 know, two honorable men about whether access should be

0222

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

11 MR. MEDINE: Okay, Frank?

12 MR. TORRES: Frank Torres with Consumers Union.

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

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

23 they are published in telephone directories, and I

24 forget what the percentages were, but there's a large

25 percentage of people who choose not to publish their

0223

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

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

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

23 that's kind of out there being stored.

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

25 naive, but why would companies have all this data

0224

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

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

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

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

0225

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

4 MR. MEDINE: Andrew?

5 MR. SHEN: Andrew Shen.

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

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

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

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

23 sort of information that's generated and kept around,

24 why is it stored? I mean, you can relieve a lot of the

25 responsibility if you just -- on security and access if

0226

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

2 The other question that came up earlier is

3 maybe one cut that you provide access to is information

4 that was provided as opposed to information that was

5 sort of derived or inferred. I think one of the

6 important reasons that you have access and why it is a

7 fair information practice is so you can know about that

8 provided information, know what else has been done to

9 that that you don't really realize is being done. You

10 really want to know all that information, what you may

11 have not known at the outset.

12 MR. MEDINE: John Kamp had his hand up a while

13 ago, if you are still interested.

14 MR. KAMP: Actually, the point was already

15 made, and Dan Jaye has a point I want him to make,

16 actually.

17 MR. JAYE: I just want to address the issue of

18 why that data is kept on tape and archived. The

19 primary use is for audit purposes, is that you have to

20 keep some data around in certain applications, because

21 you may be audited later on, to say your numbers were

22 correct, your ad tallies were correct. It's not

23 because it's going to be used for -- on a

24 consumer-specific basis for making decisions about the

25 consumer. It's actually -- it's a record of your

0227

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

4 MR. MEDINE: Okay.

5 Richard?

6 MR. PURCELL: Thank you, Richard Purcell.

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

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

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

23 classifications, categories of data, which they've done

24 a good job of here in detailing -- I've got a couple of

25 additions I'd like to add to that -- and sources of

0228

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

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

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

23 may be ways that we can create a dimensional matrix.

24 The other thing I'd like to just suggest as

25 additions to the categories are identifiers that

0229

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

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

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

23 going to have in terms of access? And so authorization

24 levels apply very strongly to that category, but they

25 could also apply to consumers accessing their

0230

1 individual data.

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

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

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

9 MR. PURCELL: Thanks, Frank, Richard Purcell.

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

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

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

0231

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

4 Ron?

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

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

23 needs the backup tapes and backup information to do

24 that. That's not the only reason, but it's certainly

25 one reason.

0232

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

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

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

23 it's important to have it. What I am suggesting is

24 there should be a separate category, if you want to

25 technically call it a subcategory or a separate

0233

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

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

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

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

23 it up, certainly sector is an important issue. And I

24 now have his diagram.

25 MR. MEDINE: Let me make an important access

0234

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

6 Deirdre?

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

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

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

0235

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

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

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

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

0236

1 fixed axes that would be useful in the access section,

2 I think that would be great.

3 MR. MEDINE: Also, just keep in mind that

4 simplicity benefits consumers in understanding what

5 they're getting access to.

6 MS. MULLIGAN: Absolutely.

7 MR. MEDINE: And obviously benefits firms in

8 understanding what they need to provide access to.

9 Rob?

10 MR. GOLDMAN: I guess listening to the

11 discussion, I want to weigh in a little bit on use and

12 making of decisions with information, which has not

13 been brought up as one of the dimensions on the three

14 or four-dimensional cube but one that is interesting at

15 least and seems to find its way into most of these

16 outlines somewhere.

17 I want to share an experience that I have had

18 at my company since these outlines have been circulated

19 that makes -- I think use is a difficult one, a

20 difficult one to work with. It's interesting but hard

21 in practice. Dash.com is a startup. We provide

22 customers with access to almost all of the information

23 we collect on them. There's a small piece of

24 information which is the operating system they used

25 when they signed up for our service which is not

0237

1 currently part of their profile page.

2 We work with online merchants. One of our
3 salespeople during this past period was talking with a
4 computer retailer about making offers to members of our
5 service for no-money-down financing for computer.

6 Right now we don't provide access to that old -- to the
7 operating system variable, but that variable is one
8 that we wanted to consider in choosing who to -- whom
9 to make the offer to, who would be likely to be in the
10 market for a new computer.

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

23 marketing decision, but I guess that line is vague and

24 difficult.

25 So, in practice, use, although important, seems

0238

1 like it's a hard one to pin down and certainly would

2 get away from us, I think, in industry.

3 MR. MEDINE: Dan?

4 DR. GEER: Yes, Dan Geer.

5 The only point I wanted to make is to the

6 extent we're trying to imagine the future in making

7 these rules, I think it's worth mentioning that in a

8 very short time, the number of devices that are on

9 networks and the number of entities which are making

10 and breaking connections and all of that will be

11 totally dominated by things that do not have a

12 keyboard. Your refrigerator, your car, you name it,

13 everything will be there, and the information that's

14 hardest to deal with in that circumstance is what I

15 believe would be called traffic analysis. Who's

16 talking to whom and when and what did they say?

17 That kind of stuff is, on the one hand, a rich

18 mine, and on the other hand, it's a rich mine, and the

19 question is which way do you want to go, and I just

20 want to make sure that everybody understands, just as

21 the comment was made about biometrics a moment ago, the

22 technology frontier here is advancing at a speed which

23 I think is going to be very difficult to anticipate in

24 a rulemaking proceeding such as you're attempting to go

25 to.

0239

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

5 DR. GEER: Okay, sure.

6 MR. MEDINE: No rules being promulgated here.

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

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

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

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

23 because there's been a discussion back and forth

24 earlier about whether companies keep information, why

25 do they keep information, how do they use the

0240

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

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

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

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

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

24 comment?

25 MR. LANE: No, I didn't.

0241

1 MR. MEDINE: Lance?

2 DR. LANCE HOFFMAN: Lance Hoffman.

3 A couple of points, and this is a very good

4 segue into what I'm going to say. We cannot predict

5 the future, but we have to design for it anyway.

6 That's one reason I think we came to that figure we

7 have in access group four. And Richard has a model of

8 keeping himself in check. He only showed it looks like

9 a telephone and a regular mail and a computer. We

10 talked about refrigerators and cars and all of these

11 things. He didn't put them up there. He was very, you

12 know, sedate that way, but they're coming, okay?

13 So, the point is we can't predict what's going

14 to happen, but what we do know is we don't want to make

15 rules -- sorry, I'll change that expression -- we don't

16 want to make decisions that are so binding that they

17 get us in trouble later on. We don't want to come to

18 standards too early.

19 Having said that, I think time may wish -- we

20 may want to consider time as another access of some

21 sort, because time has been left out here, and things

22 change over time, both the decisions, the access rules,

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

0242

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

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

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

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

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

0243

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

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

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

22 Alex?

23 MR. GAVIS: Just to clarify a point earlier

24 that was made about how long or why do companies keep

25 records, I mean, particularly in the financial services

0244

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

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

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

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

18 MR. MILLER: It was made.

19 MR. MEDINE: Dan?

20 DR. SCHUTZER: Dan Schutzer.

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

23 purposes of what we're talking about, data access and

24 security, we should be more concerned with the

25 sensitivity with which data is handled and to which

0245

1 access is provided and the sensitivity to an

2 individual.

3 As an individual, certainly when I see the data

4 type and you tell me how it's used, tell me who you're

5 sharing it with, I make my own determination as to how

6 sensitive I am to the data, but another factor in

7 determining whether I want to provide you that data or

8 not is how you're going to store that information and

9 how you're going to make it accessible. That's to say

10 that if you came to me for a loan application and you

11 ask to provide my Social Security number and I feel

12 you're going to safeguard that, encrypt it, and it's

13 only going to be accessible when I want to look it up,

14 used in the way you demonstrated, that's one thing, but

15 when I go to another site and they request information

16 about my Social Security number and they are going to

17 make it available by just public directory yellow

18 pages, that's a whole other thing.

19 Another issue is if we're looking at these new

20 devices, before we get to the refrigerators, we have

21 set top boxes, and when you start to look set top boxes

22 and cable head-ins, sometimes the information that's

23 stored in cookies, which is sometimes unencrypted, is

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

25 administrators and sometimes accessible to people who

0246

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

4 MR. MEDINE: Okay, thanks.

5 Stewart?

6 MR. BAKER: Thanks, Stewart Baker from Steptoe.

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

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

23 criteria do they use to evaluate a particular

24 application or customer just on their own, and we have

25 to -- when we talk about inferred data, we have to

0247

1 think very seriously about how do you protect

2 proprietary methods of analyses.

3 The second thing that happens in FOIA -- here's

4 a story, I don't know how many of you have had

5 background investigations, but if you have, you should

6 FOIA the records of that background investigation.

7 That's something I did, and it was quite interesting.

8 The government went through quite carefully, they had

9 all of the interviews that they had done with everybody

10 who had ever smoked tobacco with me, and they carefully

11 blacked out the names of the investigators to protect

12 their anonymity and left in the names of all the people

13 who were talking about their experiences with me.

14 And it occurred to me that probably from the

15 point of view of those people, this wasn't the best way

16 of dealing with the situation, but that raises the

17 question, what do you do with third-party reports?

18 What do you do about complaints from a chat room

19 directed to a particular e-mail address or screen

20 identity? Almost any information supplied by a third

21 party has the potential to put that third party at risk

22 in the wrong circumstance. And so including

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

24 a serious problem.

25 Finally, occasionally -- this also happened to

0248

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

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

22 MR. MEDINE: Thanks.

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

0249

1 MR. ISAY: Hi, Josh Isay.

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

10 MR. MEDINE: Frank?

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

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

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

24 here.

25 You raised the correctness of the records, and

0250

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

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

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

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

0251

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

6 MR. MEDINE: Dan?

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

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

23 getting faster, especially with the proliferation of

24 wireless devices, and at the same time memory prices

25 and memory -- the amount of memory on computational

0252

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

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

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

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

19 MR. WHAM: Ted Wham with Excite@Home.

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

23 correction of info, I think we might want to consider

24 having a correction of information as part of the

25 access requirements only for the information that the

0253

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

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

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

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

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

24 going to be an extremely difficult implementation in

25 the anonymous type of data which is collected, you

0254

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

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

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

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

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

23 subcommittee, really addressed that issue.

24 So, I would like to maybe move back a little

25 bit, maybe we can do this in the afternoon, to ask what

0255

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

4 Now we can take the break.

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

8 (A brief recess was taken.)

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

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

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

0256

1 (Applause.)

2 MR. KAMP: Now, will you be collecting our

3 clickstream data as we eat your cookies?

4 DR. JONATHAN SMITH: There's a motion detector

5 at the top of the box.

6 MR. PURCELL: Be careful, they are cookies.

7 MR. MEDINE: Yes, we appreciate your

8 contribution to the committee.

9 I wanted to ask a few people to make a few

10 brief comments as a follow-up to the last session. I

11 do want to move forward, but I think it will be helpful

12 to put things in perspective.

13 The first is Richard Bates.

14 MR. BATES: I just want to touch on one thing,

15 and David, you mentioned this earlier, but the most

16 important thing from businesses' point of view, and I

17 think it's true from consumer groups, as well, is

18 simplicity, and whatever we recommend has to be simple

19 so we can understand it and we can do it right, and I

20 thought we tried to do that in our little group, and

21 hopefully we did to a certain extent, but whatever we

22 come out with, it's got to be able -- it's got to be

23 easy for people to understand, to work with, and I

24 think that should be the hallmark of everything that we

25 do here and every recommendation that we make. So,

0257

1 thank you.

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

8 David Hoffman?

9 MR. DAVID HOFFMAN: David Hoffman from Intel
10 Corporation.

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

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

0258

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

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

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

23 joint marketing partners.

24 Essentially how far up the line -- we talked a

25 little bit earlier about how far up the sort of

0259

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

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

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

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

23 MR. MEDINE: Well, I guess maybe to turn that

24 around, one of the issues in the financial

25 modernization debate is who should the first entity

0260

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

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

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

23 that. The main thing is that the consumer, you know,

24 gets the notice, gets the access.

25 MR. MEDINE: Okay, Ted?

0261

1 MR. WHAM: Ted Wham with Excite@Home.
2 There's a couple things I want to address in
3 terms of that. The first one is that there's a notion
4 that data is owned by just one organization, that if
5 you give me your name, that I'm the only one who knows
6 it, and we should recognize that data is owned by
7 multiple organizations that collect it through
8 nonduplicative manners.
9 The second thing is that if you provide
10 information to me, you know, there are big smiles every
11 time that cookie box comes around, you know, but if
12 you provide information directly to me, then I think
13 that there's a right of action and a right of
14 correction to that which is available, but if you give
15 me authorization to be able to share that information
16 with third parties, I think we need to look carefully
17 at what the responsibilities are for that third party
18 to correct that information, because it's kind of, you
19 know, the horse is out of the barn at that point, and
20 the third party is a buyer of that information or is a
21 recipient of that information from a trusted source as
22 opposed to directly from the consumer that supplied it.

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

0262

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

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

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

23 market?

24 MR. WHAM: I think you want to have some

25 delineations very carefully about where those lines

0263

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

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

20 MR. MEDINE: Jonathan?

21 DR. JONATHAN SMITH: Jonathan Smith.

22 I did want to make a point. One of the

23 interesting things that we haven't really touched on

24 but we have been hitting on like edges of it is what is

25 the value of the information? I mean, I think that one

0264

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

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

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

23 modern new-age companies are, in fact, predicated upon

24 the value of this information, and that value seems to

25 me to be a very different value than the consumers seem

0265

1 to place on exactly the same information, and maybe all

2 the value added is in the data fusion.

3 I don't know, I don't have answers, but I'm --

4 you know, this is one of the things that's actually a

5 good way to think about it, which is the value of the

6 information.

7 MR. MEDINE: Okay, David?

8 MR. DAVID HOFFMAN: I just wanted to come back

9 to Ted's point about the definitions, and you go

10 through that we do have at least six different terms

11 that we haven't defined right here. I do think that if

12 we try to define all of those separately, I agree with

13 Ted, I think that's a task that will create more

14 mischief than clarity, but I would actually offer a

15 different option than what Ted offered.

16 I don't think the direction that we should go

17 is saying whether it's an ownership issue. I think we

18 have to look at it from the perspective of the

19 consumer, and we have to look at it from the

20 perspective who do they think that they're giving the

21 information to, who do they think that they're dealing

22 with? When we have a world of multi-national

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

0266

1 the way to go.

2 MR. MEDINE: So, would your operational rule

3 then be that you would send the consumer back to the

4 entity that they interacted with as opposed to

5 affiliated entities? How would you apply that in

6 practice?

7 MR. DAVID HOFFMAN: I would send it back to the

8 affiliate that they dealt with originally with the

9 opportunity, also, for them to -- if they had been

10 provided notice that the other entities were also going

11 to get the information, that notice -- I don't see how

12 you can deal with this without dealing with what

13 notice, if a third-party transfers, there are going to

14 be. The notice requirement would have to also obligate

15 notice or other entities that the consumer wouldn't

16 perceive that they are giving the information to and

17 them having the ability to contact them, and then if

18 it's taken back to the original entity, at least that

19 that's going to be done timely.

20 MR. MEDINE: Okay, James?

21 MR. ALLEN: Yes, James Allen.

22 I wanted to go back to the point Ted raised

23 about, you know, where do you correct data? Where does

24 a consumer correct data, at the point that they're

25 interacting -- at the entity that they're interacting

0267

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

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

22 MR. MEDINE: I guess maybe just to clarify one

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

0268

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

2 saying.

3 MR. MEDINE: And so an affiliate may -- unless

4 they're required to may not be able to even track it

5 back to the original source in terms of access and

6 correction issues?

7 MR. ALLEN: It may not be economically feasible

8 to maintain such a system.

9 MR. MEDINE: All right.

10 Ron?

11 MR. PLESSER: I just want to follow this line

12 directly with what the person from the other side was

13 saying. In the public record databases that we've

14 worked with, similar to the Individual Reference

15 Service Group and the FTC, and the group has been at

16 some level of disagreement on this issue, and it raises

17 precisely this question. If we are in these cases

18 replicating public record bases, real estate records or

19 others where -- or court decisions or whatever those

20 issues are, the people who -- the databases who are

21 providing it have taken a position that they will

22 notify the individual where the information has come

23 from and kind of who to contact if there is otherwise

24 public information.

25 If there is nonpublic information, then we all

0269

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

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

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

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

0270

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

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

11 MR. MEDINE: Deirdre?

12 MS. MULLIGAN: Deirdre Mulligan.

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

23 to flow, and those interests clearly, you know, from my

24 perspective include an access right and a correction

25 right.

0271

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

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

23 and it may be -- I don't think it's a compelling

24 interest to say it's most efficient here. I think that

25 you can correct it as -- I'm not sure who the person is

0272

1 sitting directly -- diagonally across from me.

2 MR. ALLEN: James Allen.

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

11 MR. ALLEN: James Allen again.

12 Just for the record, I want to --

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

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

19 MR. WHAM: You could do both.

20 MR. MEDINE: Greg Miller from MedicaLogic.

21 MR. MILLER: Greg Miller, MedicaLogic.

22 Just a couple of points. In listening to this

23 discussion, one has to wonder if what our work isn't

24 all about is setting a set of protocols for profiling

25 in general, and I just offer that up for us to think

0273

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

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

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

- 23 MR. MEDINE: Richard?
- 24 MR. PURCELL: Richard Purcell.
- 25 I'm gratified that the conversation is taking

0274

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

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

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

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

0275

1 those kinds of decisions, as well.

2 Finally, I want to raise a caution that was

3 raised in our prior meeting earlier this month. We

4 have to make a decision here whether or not our work is

5 going to inexorably lead to a recommendation or

6 guidance principles that say data must be consolidated.

7 There's a real problem with that conclusion in that in

8 order to protect your privacy, I essentially now am

9 being required to assemble more information about you

10 than I otherwise would have access to.

11 Now, it certainly eases the burden of access.

12 Certainly if I can provide a single point of entry for

13 an individual to look at the data that we have about

14 them, then I have facilitated access. At the same

15 time, I have also facilitated my ability to surveil or

16 to intrude upon the privacy of that individual, because

17 I know vastly more about them than I otherwise would.

18 Is that a data protection step or is that a data

19 intrusion or a privacy intrusion step?

20 These are hard questions, and I would say that

21 this group is going to have to come down on one side or

22 the other of these questions.

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

0276

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

7 MR. PURCELL: Richard Purcell in response.

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

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

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

23 differential infrastructures, and there's not

24 necessarily data flowing between these different data

25 sets. If we required that that data flow between these

0277

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

4 MR. MEDINE: Dan?

5 DR. SCHUTZER: I agree, I think it's important

6 to know the source, even the nature of the source,
7 because that can affect the nature of the correction.

8 In other words, if -- let's say the source is my

9 grades, the nature of the source is coming from the

10 professor, I can't necessarily just at whim change it,

11 but it's fine to know the origin, the identity of the

12 source. If it's coming from let's say a supervisor's

13 evaluation, it's not entirely clear that you're

14 entitled to know who that person was or that you are

15 able to change it. So, I think that simplicity would

16 be nice, because we understand today we don't carry on

17 like that, who is the original source and so forth.

18 So, if we could move into that kind of a way of

19 managing that, I don't know that, the transition, and

20 for simplicity I would say, even though I'm going to

21 bring it up, there could be a whole trail here in terms

22 of the original source, it goes to someone else, it

23 goes to someone else, and the data can get corrupted

24 somewhere in the process. I think that would probably

25 be too complicated to try to implement exactly finding

0278

1 the entire audit trail. I'd recommend probably just

2 the source and the nature of the source.

3 And, of course, being able to compare the data,

4 it's quite possible that the data I'm viewing in this

5 site was entered in error, that the source actually had

6 it correct.

7 MR. MEDINE: As we move forward, I have a

8 couple of -- I would like to sort of shift the

9 discussion into the cost-benefit, not that we haven't

10 been in it already, but to talk about some of the costs

11 and benefits, like correction and how to provide

12 access, what is the cost structure that's entailed with

13 setting up access for consumers in an essentially

14 otherwise highly automated database system, but we have

15 a few more comments that may or may not address this

16 issue.

17 Tom?

18 MR. WADLOW: Tom Wadlow.

19 Yeah, I wanted to actually touch on some of the

20 things that were being said here, but what triggered me

21 was Mr. Allen said what I thought was a very

22 interesting phrase, traceability is just as hard as

23 sensitivity when it comes to data. There's a very

24 interesting distinction between the two there in that

25 sensitivity of data is in many ways subjective.

0279

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

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

23 what uses, in fact, the company might wish to declare

24 that they are explicitly not putting this information

25 to. That's all very, very objective stuff, and I think

0280

1 that's very valuable.

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

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

23 that sense.

24 MR. MEDINE: Dan?

25 DR. GEER: Dan Geer.

0281

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

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

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

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

23 web forms all the time. Half the time I lie on

24 purpose. That's my right. I don't want to correct it.

25 If you want to make it possible to correct it, then you

0282

1 have to be really, really, really sure it's me and not

2 my brother, my evil twin and all of that, right?

3 MR. MEDINE: Sure. Dan Jaye?

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

5 I'm going to try to tie together actually the

6 entity discussion and the cost-benefit discussion here

7 and draw on a point that was made about a protocol.

8 There is a project underway called the Customer Profile

9 Exchange standard under development, and I hope that it

10 will be heavily informed by the work that actually

11 comes out of this committee, but one of the concepts we

12 have is to have privacy built right into this protocol.

13 There's been a bit of press about it. One of

14 the costs that we're concerned about that we're trying

15 to figure out how to address is that if you have in

16 this concept the idea that the privacy implications of

17 data are attached to the data and travel with the data

18 whenever it's transferred, so that we can deal with

19 onward transfer privacy issues, one of the concerns is

20 what about Legacy systems that you are interfacing to.

21 Suppose I'm taking an order from an order

22 processing system and I'm giving a name and address and

23 a packing slip data to Federal Express so they can

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

25 suppose I have some sort of onward transfer propagation

0283

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

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

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

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

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

0284

1 and offline files, and had different sort of standards

2 of how those things needed to move into the

3 jurisdiction of the act.

4 To my point earlier, maintaining a file that's

5 effectively a sequential file that's only accessed in

6 bulk could be much less expensive than now throwing an

7 index on it that allows it to be accessed in realtime,

8 and some architectures might not be feasible. I think

9 in today's technology, that issue becomes much more

10 apparent when we're talking about interactive data than

11 necessarily customer records.

12 In other words, cardinality, the number of

13 records we're dealing with for a customer with a

14 typical business is usually small enough that the index

15 overhead requirements aren't that bad. It's when you

16 start dealing with the huge volume of interactive data,

17 if we step into the range of saying you need access to

18 those individual records of the fact that I clicked on

19 this page and I clicked on that page, back to the

20 consumer, that's an area where the cost implications

21 start to need additional consideration.

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

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

0285

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

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

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

23 they should expect access and when they shouldn't.

24 James?

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

0286

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

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

23 identity to do that, then...

24 MR. MEDINE: Thanks.

25 Ted?

0287

1 MR. WHAM: Ted Wham from Excite@Home.

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

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

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

23 statutory requirements.

24 The second one I want to talk about is to touch

25 specifically on Deirdre's response back to me about the

0288

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

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

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

22 MR. TORRES: I want access.

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

0289

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

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

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

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

23 their access and for their correction. Further, I

24 believe that there are other categories of information

25 that is available for their access and not necessarily

0290

1 their correction, the examples that I've provided
2 earlier about what you purchased or, you know, if you
3 were in the hospital, say what day was I born, and they
4 say you were born X date, 1946, and they go, oh, I
5 don't want to be that old, therefore I was born in
6 1964, right, those types of things aren't available for
7 correction.

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

13 MR. MEDINE: Andrew?

14 MR. SHEN: Thank you, Andrew Shen.

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

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

24 that, but --

25 MS. MULLIGAN: Apparently it is.

0291

1 MR. WHAM: I was being too strong.

2 MR. SHEN: Also I would like to throw out that

3 access could also include the right to delete

4 information, and I think this is increasingly a point

5 in the modern world, and as the entities outline

6 showed, a lot of information transfers to third

7 parties, affiliated parties, joint venture marketing

8 deals, and a lot of that we don't realize is going

9 there. So, I think that a person who that information

10 describes has a right to remove it from places that

11 they had no idea that information was going to.

12 Second, in reaction to Richard's comments, this

13 very interesting sort of dilemma between consolidation

14 and access, in some ways I think on a theoretical level

15 that's very interesting, but on a practical level, it's

16 not really much. I think what we see is an amazing

17 amount of consolidation out there and not much access,

18 and I think those two need to be balanced, but it's

19 definitely out of balance right now.

20 And the consumer profile exchange that Dan Jaye

21 referred to is I think one compelling example of that.

22 I think you're seeing a lot of consolidation out there,

23 and consolidation is becoming so easy that companies

24 can transfer back and forth baseball cards,

25 essentially.

0292

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

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

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

23 dodging the question here. I can't come up with a

24 precise answer for you.

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

0293

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

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

10 MR. MEDINE: Lance?

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

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

23 think Ted had a very good example, let me take it

24 further, with the FTC, this committee.

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

0294

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

9 Now, take that and electronicize it, okay?

10 Pretty soon you have got databases talking to
11 databases, talking to refrigerators, talking to Peapod,
12 this and that, and the grocer and people like
13 that. We can have data going back and forth and back
14 and forth and back and forth and a lot of activity but
15 nothing really getting done and, in fact, us getting in
16 the way of in essence maybe performing what is
17 reasonable for the consumer. So, the real issue is
18 what is reasonable for the consumer.

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

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

0295

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

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

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

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

24 can the business be brought to court, are there

25 liabilities that attach to that, and you also have

0296

1 credibility of the business itself.

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

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

20 MR. MEDINE: Thanks.

21 Rob?

22 MR. GOLDMAN: Rob Goldman, Dash.com.

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

0297

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

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

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

23 of consolidating data from various parties, is too

24 high, that you'll see a lot of that get stifled.

25 One other point on costs and benefits, and this

0298

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

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

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

23 effectively against the costs. So, I think what

24 happens often, and I've seen it happen certainly quite

25 a bit in the space in which Dash competes, is that

0299

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

8 MR. MEDINE: Did you want to respond?

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

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

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

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

0300

1 information and all the requests that may come in.

2 MR. MEDINE: Ron?

3 MR. PLESSER: A couple of quick points going

4 back and then maybe one recurring thing in this.

5 First of all, just in terms of the source and

6 access discussion, I think it is important if we can

7 look back at kind of the old world, is the DMA for many

8 years, many, many years has had a provision not on

9 access to records but on source. So, it is the DMA

10 guideline, at least in terms of the old world of

11 marketing lists where you did get lists from another

12 person, and if you look at your mailing label, there's

13 a little number code on top of the mailing label, and

14 that always identifies where the list came from,

15 because, you know, if you're going to use that list

16 again, you want to know it.

17 So, I think the issue of source is really a

18 much different issue than access, and I think if you

19 look at least in the marketing world, source has

20 already been, at least in the self-regulatory regard,

21 been dealt with.

22 The second point, and maybe this is also

23 relevant in the flow of conversation, I agree with the

24 last comment, that I think consumers have interests

25 that have to be respected. Privacy is a critical

0301

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

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

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

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

23 Privacy Commission stage and in OPA, the integrity

24 argument is the business does get value by having

25 consumers -- there was a big fight in the Privacy Act

0302

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

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

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

22 MR. MEDINE: Lorrie?

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

0303

1 hand up since then.

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

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

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

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

23 is not only monetary costs, there is also how difficult

24 is it for me as a consumer to figure out how to get

25 access.

0304

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

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

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

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

0305

1 MR. MEDINE: Okay, Frank.

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

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

23 then turn around and use the information or provide the

24 information to somebody else, and I think that just --

25 I think we need to think about that, because I think

0306

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

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

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

23 provide consumers with appropriate access. To fix it,

24 the same thing about looking at the interests of the

25 person accessing the data. If I'm a business entity

0307

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

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

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

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

20 MR. LANE: I just wanted to clarify that.

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

23 is a good one about, you know, profiling people around

24 the table and taking a look, but a person compiling

25 that information is a lot different than a business

0308

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

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

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

14 MR. MEDINE: Dan?

15 DR. SCHUTZER: Dan Schutzer.

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

23 for somebody. So, bear that in mind. You might

24 consider in the sake of simplicity that we really are

25 talking about master records that are kept online that

0309

1 people would have access to.

2 Another thing is the nature of the data. If

3 we're talking about, as was illustrated, you know, the

4 credit report or a financial transaction, that's going

5 to be or should be kept absolutely accurate, and so

6 that's maintained. Now, when you talk about marketing

7 kind of data, most marketing data, of its very nature,

8 is basically noisy and dirty. So, don't be surprised

9 if you find a lot of times that the data from the third

10 -- that's been acquired, by the time you process it,

11 it's better than the original data, okay, because

12 sometimes the data we're receiving has typos, errors,

13 omissions, even translate that to the web.

14 I mean, you might be tracking an IP number in

15 the clicks, but the IP number is not always the same

16 person. So, we might have a proprietary algorithm to

17 help us sort of decide which ones to throw out.

18 Statistically, it might be a more valid sample, but

19 it's just marketing data. It's not, you know,

20 financial records that we want to keep. So, sometimes

21 the source is not really a good source anyhow, okay?

22 And the third or fourth party that's processed it

23 actually has better data.

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

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

0310

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

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

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

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

23 agree with Ted completely, he can choose who he takes

24 out to dinner or not, and I don't have a right to that

25 information, but at the point in time where a service

0311

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

4 MR. MEDINE: Deirdre?

5 MR. WHAM: Can I jump in on that?

6 MR. MEDINE: Very quickly.

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

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

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

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

23 to.

24 Deirdre?

25 MS. MULLIGAN: Deirdre Mulligan.

0312

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

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

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

23 for moving the task force forward to putting forward

24 recommendations, to the extent that we can identify

25 consensus, it would be useful.

0313

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

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

23 very useful to move us in that direction.

24 The third point is on Richard Purcell's

25 centralization question, which I do believe is one that

0314

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

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

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

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

0315

1 extent we can look at those issues together, it would

2 be useful.

3 MR. MEDINE: Tatiana? Would you identify

4 yourself?

5 MS. GAU: Tatiana Gau, AOL.

6 I'd like to start out by echoing Deirdre's

7 comments about Ted's example on access and also kind of

8 the question he threw out in the air that is the

9 principle of access a fundamental right of the

10 consumer. I believe it is in certain cases, as I think

11 most of us do, and just to kind of illustrate that

12 example, on AOL there are various areas within your

13 account that you can go to access information about you

14 that we might have.

15 One example might be your wallet on AOL, where

16 after entering a separate password to authenticate

17 yourself, you're able to view your name, address, any

18 shipping addresses you have on file for any of your

19 relatives, products you've purchased. For security

20 reasons, you can only see the last four digits of your

21 credit card number, but you can from that point on also

22 make one-click transactions.

23 Another example is your billing information.

24 You can go to the billing area and view a log of all of

25 your sessions, what screen names you've signed on with

0316

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

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

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

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

0317

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

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

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

23 exercise that right just along the lines of people all

24 sending in for their credit reports when the fair --

25 when that was first allowed.

0318

1 MR. MEDINE: Thank you, Tatiana.

2 Final word from Jerry.

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

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

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

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

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

25 name correctly, spell your street address correctly.

0319

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

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

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

0320

1 you have to do it with tax departments in companies.

2 It is just not correct. To do that, you are going to

3 drive the benefit of consumers of new small businesses,

4 lots of choices on the web, are going to be hampered if

5 you create a huge barrier to entry on marketing data

6 access. You have to be -- look at the use and what

7 you're using the data for.

8 I agree totally with Frank, if you're going to

9 not give me a loan, if you're not going to give me

10 insurance, those kinds of things -- that's important

11 information you're making that kind of decision on, but

12 if I'm Nordstrom trying to get a 10 per coupon to you,

13 granted you don't get it and it's probably a problem,

14 but the cost of perfection for me to get that 10

15 percent coupon to you is prohibitive.

16 MR. MEDINE: Thanks. I hear all the computers

17 chirping, which suggests to me that they need a rest.

18 So, why don't we take a five-minute break, and we'll

19 resume with the last access panel.

20 MR. PLESSER: How long is the break going to

21 be?

22 MR. MEDINE: Unless people want to push

23 forward. Do people want to press forward? That's

24 fine. What's the sentiment of the group, press

25 forward? If people want to stand and stretch, let's

0321

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

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

13 Richard?

14 MR. PURCELL: Richard Purcell.

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

23 them for access to information.

24 As David indicated, there are -- we're

25 recommending that -- for discussion that there are

0322

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

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

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

0323

1 account?

2 There's a point that we made that isn't noted

3 here that I think is perhaps worthy of consideration,

4 also. In the illustrative model, we indicate that an

5 individual uses various means, bi-directional means, of

6 gaining access to and receiving information about the

7 information stored in a system about them. It may be

8 worth considering whether or not or how authentication

9 would occur with somebody who is acting as an agent for

10 a data subject. I used the example earlier of a parent

11 who may need to be an agent and access a child's

12 account, so -- and there may be other situations where

13 somebody has to act in an agent capacity in order to

14 view somebody else's account.

15 Finally, we have taken a shot here at defining

16 a glossary. We use words in this group and in the

17 industry not always with the same meanings but using

18 the same words. We'd like to encourage the group as a

19 whole to create a sense of definition around specific

20 words. This is a hopefully somewhat provocative

21 attempt at getting people to come out with better

22 definitions. I'm not sure that we want to start

23 arguing over the meaning of words here around the

24 table, but it certainly is an effort that I think that

25 is worth accomplishing as part of the guidance that

0324

1 we're chartered with here in order to create

2 unambiguous definitions for specific words.

3 I think we all run into that problem today in

4 lacking communication in this emerging marketplace

5 where a language is yet to be defined other than in a

6 dynamic sense.

7 MR. MEDINE: Thanks. One thing I hope people

8 will address, rather, as the session goes on is the

9 issue of agents that you describe. One of the trends

10 that seems to be emerging on the internet is the

11 ability of a site to gather lots of information about

12 you and your relationships with a variety of firms for

13 bill-paying purposes or for tracking other things, and

14 that is essentially premised on that website getting

15 access to your account so that they can provide that

16 information, and the question is, is that appropriate

17 if you've authorized them? Can a site limit access to

18 only the data subject? If people have views on that,

19 it might be helpful for the discussion.

20 Ted?

21 MR. WHAM: Ted Wham with Excite@Home.

22 I particularly liked the write-up from this

23 group, from whoever was responsible for it, I think

24 there's some great depth here. I have three comments

25 here about this topic.

0325

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

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

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

23 for the users to change their passwords, and they were

24 very tight passwords, kind of nonintelligible and

25 random strings of numbers, and everybody solved that

0326

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

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

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

22 So, whatever our access and potential

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

0327

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

3 MR. WHAM: Interesting. Now we know yours.

4 Similarly, most websites already have, if a

5 loose password isn't loose enough, we have an

6 additional mechanism to have it looser, we have a

7 password hit mechanism, where if you forget your

8 initial password, we provide a way to go retrieve that.

9 One of the most wonderfully loose ones is a set of four

10 predefined questions. What's the home town where you

11 were born in, what's the name of your pet, et cetera,

12 and if you can supply those, you can get it back.

13 We actually had a system administrator within

14 our chat product who had additional rights on our

15 system, who could go in and disable accounts, you know,

16 and she was born in Peru, and her question was what

17 town were you born in, and she was born in a small town

18 in Peru, and a malicious user pulled out an atlas and

19 went one by one and went in and did that. When we talk

20 about competitors being able to do this, this is

21 already happening. So, all of this is bound to happen

22 now.

23 My third point is I want to touch again on page
24 6, the personally identifiable information, although it
25 this conforms with my understanding of it, we had

0328

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

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

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

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

0329

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

4 MR. MEDINE: Stewart?

5 MR. BAKER: Yeah, Stewart Baker from Steptoe.

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

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

23 just releasing an address could produce that harm, you

24 are going to be sued and potentially held liable for

25 not having had strong enough security. So, the default

0330

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

4 MR. MEDINE: Quick response?

5 MS. MULLIGAN: Deirdre Mulligan.

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

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

23 with a photo ID, all they provided back was what I

24 would be getting in disbursement of benefits. So that

25 the risk of a third party accessing that data was so

0331

1 reduced that you could also reduce the authentication.

2 MR. BAKER: But if I say I want to check to

3 make sure you've got my address right --

4 MS. MULLIGAN: Absolutely, but what I'm saying

5 is there is a sliding scale there, and I think in

6 providing access, if you have somebody who says it's my

7 account -- I say it's my account, you shouldn't need to

8 give me my name and address, because I've said it's my

9 account. So, if the data that you're going to provide

10 me access to is relatively benign data, people keep

11 talking about clickstream data as being very benign.

12 Some of it may be, some of it may be not, but you can

13 mitigate the risk, the liability potential, by thinking

14 about what it is that you provide access to.

15 So, I think that these things are really tied

16 together. So, I'm agreeing with you, but I think we

17 need to parse through it a little more.

18 MR. MEDINE: Well, COPA has certainly

19 introduced the sliding scale, and we're happy to hear

20 more about sliding scales if that's the group's wish.

21 Alex?

22 MR. GAVIS: Alex Gavis.

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

0332

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

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

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

23 that you use PINs and Social Security numbers or

24 disclosing that you use digital signatures or -- and

25 how that process works, I think would be an important

0333

1 element.

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

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

23 MR. MEDINE: Okay, Rick?

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

25 Deirdre, I'm just curious, when you were

0334

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

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

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

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

0335

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

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

22 Now, if he was disclosing my name and address

23 to you, that would clearly be a problem, but there are

24 ways to look at these and pull things apart a little

25 bit.

0336

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

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

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

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

12 MS. RICH: Well, under COPA --

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

15 MR. WHAM: You better get a microphone.

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

23 authentication requirement.

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

25 okay.

0337

1 MS. MULLIGAN: But you wouldn't --

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

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

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

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

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

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

23 I'm suggesting that there are ways to think about

24 structuring systems that help with that problem.

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

0338

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

12 Dan?

13 DR. GEER: Dan Geer.

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

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

0339

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

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

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

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

0340

1 to have provable access devices.

2 MR. PURCELL: Richard Purcell.

3 I just want to point quickly to the naming

4 convention that we kind of landed on for our group,

5 which is a little bit long, but hopefully it helps

6 break out this -- the thinking about this. We are

7 thinking about in this space identity, as well then as

8 authentication, as well as authorization. Biometrics

9 do a good job of identifying an individual. There may

10 be need for additional strength in order to

11 authenticate an individual's -- a known individual's

12 access to a known set of data. There may indeed

13 further be a reason to authorize or to examine the

14 privileges that that person has to certain parts of the

15 data that are being revealed.

16 Now, to David's prior point about fusing data

17 and people using different forms of identity, we have

18 to be very careful. If I can identify you

19 unambiguously, if you can authenticate yourself, and if

20 you have the authority, then I will let you look at the

21 data that's relative to that identity. If you've

22 identified yourself in three different ways, you will

23 have to further identify yourself in all three ways

24 uniquely and in different moments in time in order to

25 look at the data that is contained or linked to each of

0341

1 those identities.

2 MR. MEDINE: Jane?

3 MS. SWIFT: Just two quick points. On the

4 first, I am glad we entered into a discussion about

5 biometrics, because I think one of the biggest issues

6 we face at the state level when it comes to the time

7 where sort of the rubber hits the road and we're trying

8 to protect consumers is identity theft, and

9 particularly in the area of biometrics, I'd be

10 interested to understand how as we increase methods of

11 authenticity and identification, we also protect the

12 fact that if you steal someone's electronic thumb

13 print, it's not exactly easy to change.

14 So, how do we, you know, guarantee that those

15 things that are very, very difficult to change that

16 maybe now are being utilized for my own protection do

17 not, in fact, give me greater risk, and I think that

18 probably is the conundrum on a lot of these issues, and

19 to the much more mundane, I know this is not a

20 rulemaking body, but I would propose in the best of

21 intentions that you find some way to cool this room off

22 before the afternoon or whether or not catching a plane

23 to the afternoon isn't going to be what determines

24 participation.

25 MR. MEDINE: We appreciate the feedback,

0342

1 thanks. Let's take a couple more comments, then we'll

2 break for lunch.

3 Deirdre?

4 MS. MULLIGAN: I wanted to respond to the

5 suggestion that providing notice was going to be useful

6 for consumers in assessing security, and I think this

7 is where we have a market failure. I don't think

8 consumers can assess the appropriateness of security

9 devices. I think, you know, if you look at something

10 as simple as credit cards, debit cards and

11 check-writing cards, I don't think consumers are faring

12 that well, are they? Just that -- I mean, we have a --

13 you know, you have an issue here where the people who

14 are in the best position to assess the security are not

15 consumers. It's, in fact, businesses, and I think that

16 that does go to the liability question, which Stewart

17 put on the table, that when you have a problem where

18 the person whose data may be at risk versus who is

19 actually defining the device, which I agree with you,

20 it's -- we're talking about devices here, are

21 different, that you have to figure out how to make sure

22 that the liability is appropriately placed.

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

0343

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

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

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

18 MR. MILLER: Greg Miller, MedicaLogic.

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

23 of them and the appropriateness of them for consumers'

24 access to medical records, and I just want to point out

25 that at the end of the day I submit to you that whether

0344

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

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

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

23 you that's it. Once you start traveling biometric

24 minutia across the wire and using them as an

25 authentication, so if someone can walk up to a kiosk,

0345

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

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

17 MR. MEDINE: Okay, last comment, Frank?

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

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

22 MR. TORRES: Just real quick on biometrics, I

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

0346

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

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

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

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

21

22

23

24

25

0347

1 AFTERNOON SESSION

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

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

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

18 (Discussion off the record.)

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

22 Again I again commend the security groups for

23 their work and try to focus again on security issues

24 from translating the wide range of possibilities to

25 operational standards and implementation methods, and we

0348

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

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

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

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

17 MR. MEDINE: And identify yourself again.

18 MR. WHAM: Ted Wham. Thank you.

19 MR. MEDINE: Appreciate the comments.

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

23 literally 50 million users. I was in a discussion at

24 the end of the last session where people were crowing

25 about the benefits of thumb records that would get down

0349

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

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

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

22 I'm not aware of very many instances at all

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

0350

1 precedent for us to moving down that path in trying in

2 that direction.

3 MR. MEDINE: Any other people who would like to

4 make comments based on that discussion?

5 Okay. Moving on again to security issues,

6 anyone want to kickoff the discussion of how we go about

7 establishing operational standards for security? Dan?

8 MR. SCHUTZER: I think that --

9 MR. MEDINE: Could you just identify yourself

10 for the record?

11 MR. SCHUTZER: Dan Schutzer. I think that we

12 all mentioned, security is not perfect, and it's going

13 to change back and forth according to what you do and

14 what cost trade-offs and terms and risks are, so I don't

15 think we should legislate what level security anybody

16 needs.

17 What we should do is let the market decide that,

18 but what you need is a disclosure of the security. In

19 other words, what you need to do is you need to let

20 people know to what degree are you protecting things and

21 even if they want to, what techniques and to what extent

22 you're protecting the security and let the marketplace

23 decide, and of course your liability is also dependent

24 upon that.

25 That said, there also needs to be a companion

0351

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

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

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

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

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

24 don't understand technology.

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

0352

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

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

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

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

23 the risk involved of giving certain kinds of numbers

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

25 I think it can be done.

0353

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

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

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

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

23 can determine how much better or should the marketplace

24 determine whether there's security protection at all

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

0354

1 Fair Information Practice. Tom?

2 MR. WADLOW: A couple things. I guess -- oh,

3 Tom Wadlow, Pilot Network Services.

4 (Discussion off the record.)

5 MR. WADLOW: A couple things actually based on

6 some of the discussions that we were having at lunch,

7 one comment that I wanted to make is we were talking a

8 lot about access and security here, and I think a lot of

9 people would benefit from, perhaps this can be taken

10 as stated by the chair, access to what, security of what,

11 because I think that really focuses a lot on this

12 discussion. If we have a good sense of what that is,

13 that will shape a lot of this discussion.

14 Having said that, the other thing based on some

15 other comments here that I wanted to make up, I wanted

16 to make sure some comment came out of, was people talk

17 about security and we can have security and we can do

18 this.

19 It's very important to realize, this is what I

20 do for a living, and Dan is also in a very similar

21 situation. I can't speak for him, but I know we treat

22 security not as a thing that you have, but it's a

23 process, and if you don't think of it that way and if

24 you don't really have that in your rein, you're going to

25 lose a lot of the aspect, and you say, Oh, we have

0355

1 biometrics, therefore we have security or we have

2 encryption, therefore we have security.

3 That's crap. None of that is security.

4 Security is the process by which you employ various

5 things including those tools, and that's a very

6 important distinction, and it is one that is I think

7 very much lost in the general public. I mean, most of

8 the public's impressions of security comes from movies

9 quite frankly, and we think that, not like the movie,

10 tends very much to be something that they don't

11 understand or really don't want to get involved in.

12 I do spend a lot of time trying to educate

13 people on security issues, and I think that there are a

14 lot of subtleties here that I would not expect my mother

15 or anybody's mother for example to need to understand,

16 but it becomes very important for groups like this to

17 understand.

18 MR. MEDINE: Thanks. In terms of the focus of

19 this group, again the charter in the bylaws largely

20 speak to it, and I hate to confine it too carefully, but

21 I want to leave a lot to the group to give us feedback

22 about what it views as the scope of this group's

23 mission.

24 Obviously we're focusing on online information

25 collection and access to that information and security

0356

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

4 Stewart?

5 MR. BAKER: Sorry.

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

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

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

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

0357

1 standards and notice.

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

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

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

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

0358

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

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

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

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

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

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

0359

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

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

8 MR. MEDINE: Paula?

9 MS. BRUENING: Paula Bruening with TRUSTe.

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

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

23 impossible for the consumer to work with.

24 I mean, at TRUSTe we look at notices all day

25 long, every day. They are getting bigger. They're

0360

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

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

10 MR. MEDINE: Thanks. Greg and then Lorrie.

11 MR. MILLER: Greg Miller, MedicaLogic.

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

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

23 I'll give, you believe it or not, a significant minority

24 of individuals when asked had no idea what the lock on

25 their browser window meant, sad but true. Bear it in

0361

1 mind.

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

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

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

23 privacy and confidentiality.

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

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

0362

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

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

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

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

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

23 followed that, we know they're good, but again it's

24 constantly changing.

25 The threats keep changing so I don't think

0363

1 there's -- we can come up with some sort of list of best
2 practices and the IETF and others have done that, that
3 help to some extent. The other thing that's happening
4 is that some companies are buying insurance in case they
5 have security problems, and their insurance underwriters
6 I'm sure are examining their systems and trying to
7 determine if there is enough security that they feel
8 comfortable underwriting the insurance policy.

9 So I think a group like TRUSTe or the BBB could
10 have some sort of insurance, but unless they're held
11 financially liable in case there's a problem, it's not
12 clear that they would have the ability to do the kind of
13 checking that is really needed to assess somebody's
14 securities.

15 MR. MEDINE: Thanks. Also, just a question,
16 against what standards would the TRUSTe or BBB judge
17 security on a case by case basis. Ron?

18 MR. PLESSER: Well, two questions. One is,
19 again from looking back at the privacy commission days
20 and having a little bit of that perspective and maybe
21 talking this to 30,000 feet, the Department of Defense
22 in implementing the Privacy Act spent a lot of time

23 going through all the record systems and doing all this

24 work and getting the consent and knowledge and setting

25 up all these systems of access and all this stuff.

0364

1 And then one of the bases, I think Manila at the
2 time or maybe it was in California, decided that as part
3 of being good citizens on a paper reclamation, they sold
4 the printouts to a trash dealer, who then sold it to
5 fish guys that literally wrap fish and so the payroll
6 histories of all of the people at the base could kind
7 of -- was imprinted on fish that they were wrapped in.

8 So I mean I think that we can get a little crazy
9 about again the detail of security and talk about some
10 reasonable procedures, and it shouldn't -- you have to
11 take reasonable efforts. I think it is a good
12 standard. I think the question is really not one of
13 notification. I agree with what Lorrie said.

14 To tell a consumer anything more than you were
15 going to take reasonable steps to ensure the security of
16 the data is unreasonable. What is reasonable is to
17 require or to suggest that companies have internal
18 claims that they have to document and in advance to
19 themselves what privacy protection -- what security
20 protections they've taken given the relative value of
21 their judgment of what the risks are.

22 Will a jet plane come in and crash -- maybe if

23 you're at the end of the runway, that's not such a funny

24 risk to consider, and if you're someplace else, maybe it

25 is a funny risk to consider, but the company should do

0365

1 this themselves, assess their own risk and assess what

2 they think is reasonable response to that risk is.

3 And then if they suffer a loss, they're going to

4 be responsible to -- did they take reasonable steps to

5 avoid any anticipated risk, and I think maybe if the

6 Trade Commission goes in and looks and says, you didn't

7 even consider this, you didn't even try, you didn't even

8 think about the fact that you were at the end of the

9 runway and a jet was going to come in or whatever the

10 thing is.

11 So boom that's deceptive or unfair or whatever

12 your authority may be, not that I'm suggesting there be

13 any, but that's the standard we think. That's the way

14 you do it. I don't think you do it as a disclosure to

15 consumer. I think you in the end have to decide whether

16 or not they took reasonable and best efforts, and they

17 really had to define it. Maybe industry codes can help,

18 but it really is something that has to be done by an

19 individual company.

20 I think what I'm suggesting is very close to

21 what the requirements are at the Securities and Exchange

22 Commission where they do not require the maintenance of

23 financial records, reasonable efforts to be secure, but

24 what they require is that you've done a plan in advance

25 to assess the security risks and how to prevent those

0366

1 security risks, and if a public company then has a loss,
2 a security loss, the SEC goes in and looks at that plan
3 and thinks and sees if that plan was reasonable in light
4 of what happened.

5 And I think that's the approach you have to
6 take, not setting any specific standards or detailed
7 disclosures to consumers or any other usual things that
8 the Trade Commission might look at.

9 MR. MEDINE: How do you factor in the points
10 that Stewart made that value of the security to whom?
11 And the identity theft is a classic example where the
12 victim of a identity theft, it's a tremendous value to
13 avoid being a victim of identity theft. For a business
14 to give up the identity of one consumer inadvertently
15 proves less harm to the business than it does to that
16 consumer.

17 How do you weigh the consumer interest in that
18 process?

19 MR. PLESSER: Well, I think if you're a credit
20 card company and you have vital information about a lot
21 of consumers, then I think the risk of identity theft is
22 great, and you have to take strong action. I don't

23 think anybody is going to hold anybody to full safe

24 standard.

25 But if you're a catalog company and you don't

0367

1 have that detailed transactional information and you
2 take reasonable efforts but perhaps not as strong as the
3 card company, so I think again it's what you look at at
4 the end to -- you as government look at at the end, so I
5 think that gets worked in in terms of the nature of the
6 risk, but I don't think there's any absolute -- you
7 can't -- no one can really set up the standards that a
8 company is going to apply in a particular circumstance.

9 I think Stewart and I agree on that. I think a
10 company has to do it, and then you can judge if it was
11 reasonable.

12 MR. MEDINE: Deirdre?

13 MS. MULLIGAN: I want to agree with a lot of
14 what Ron said. When I think about measuring -- he said
15 set up some standards. I think you asked the question
16 though where is the rub, and the question of
17 reasonableness all depends on what your exposure is, and
18 unfortunately we have another incidence where the
19 exposure -- the risk of a security failure may not be
20 borne all by the person who's making the security
21 decisions as to what's reasonable.

22 And so there's another question about, How do

23 you increase the incentives to improve security when the

24 risk may not be obvious, and I think that's where

25 questions of liability, questions of -- and liability

0368

1 can be created in a number of different ways.

2 I mean, if there was a requirement, for example,

3 to notify consumers any time you had a security breach

4 that led to the disclosure of some piece of their

5 information or an inappropriate access to their

6 information, I think that all of a sudden the assessment

7 about what was reasonable security might change a little

8 bit because while it's not financial liability, there's

9 certainly an increased incentive to pay attention to

10 your assessment of reasonableness.

11 So I think there are some ways to impact on

12 what's reasonable, but I think that leaving the

13 determination of what's reasonable purely up to a single

14 company doesn't allow businesses to benefit from the

15 collective knowledge that's out there that's in a way

16 that's most productive.

17 So when I look at things like the CERT advisory,

18 I think there are some reasonable things that can be

19 built in, so, for example if you're running a specific

20 back end program, that it would be reasonable to me to

21 expect that if there are known bugs and known failures

22 that have been documented and that there have been

23 alerts about, that within X amount of time you should

24 close those holes.

25 And unfortunately we find that that doesn't

0369

1 happen all the time, and I don't think that it is --
2 it's not reasonable not to educate yourself about the
3 risks of products that you're using, and I think that
4 that's where there could be some useful development of,
5 What are the things that you should consider in
6 developing your reasonable plan, and saying, Yes, of
7 course you're going to develop it based on your
8 business.

9 But that you have to go and look in this place,
10 this place and this place to determine what would be
11 reasonable to incorporate.

12 And I think if we can move in that direction, it
13 would be helpful.

14 MR. MEDINE: Jane, your card was up earlier. Do you
15 wish to comment?

16 MS. SWIFT: No.

17 MR. TORRES: Okay. Frank?

18 MR. TORRES: Frank Torres, Consumers Union. I
19 also think Ron raised some interesting points about how
20 we go about maybe getting at that -- the reasonableness
21 question.

22 What I would like to raise is that kind of

23 something that I think has been a little bit left out,

24 and that's the consequence question. I as a consumer --

25 hopefully there will be some plain English as far as

0370

1 disclosure goes to tell me truthfully what I can expect
2 from your site as far as security goes, but at the end
3 of the day, I don't care what program you're running.

4 What I want to know is you're doing the best
5 that you can do to keep my information safe, and if for
6 some reason the information gets out and there's some
7 consequence to me, identity theft, my credit card
8 numbers get exposed online, on those types of things,
9 how do I resolve that?

10 How do I get redress? What steps would you take
11 to close down the open doors that allows this
12 information to get -- how do I go about -- will you help
13 me go to my credit card company and resolve my disputes
14 with them?

15 So in addition to just the basic security
16 question, I think it will be very difficult or if not
17 impossible to say you've got to follow this standard,
18 that standard or this standard. We recognize the risk.

19 To carry on the airline analogy the safest
20 airplane is the run that sits on the ground, but that
21 doesn't do anybody any good at all, so we've got the FAA
22 out there that says you have to meet some minimum

23 reasonable requirements or there's some government

24 overlay there, but ultimately it's -- people are going

25 to fly on the airlines that are the safest or the ones

0371

1 they perceive to be the safest, so maybe that's a

2 fitting role for the Commission to take on.

3 MR. MEDINE: We'll look forward to your

4 recommendations on that. Tatiana?

5 MS. GAU: Tatiana Gau. I would like to start

6 out by saying that it's interesting to see that these

7 discussions are becoming more and more similar to the

8 discussions that were held last week on Tuesday at the

9 White House, The Internet Summit on Security, and there

10 were a lot of the issues that we're discussing that were

11 brought on the table, but fundamentally the points that

12 I would like to mention relate to again security as

13 being something more of a process.

14 One of the things that is clear is that

15 different companies are putting different amounts of

16 money into dealing with security as a process, whether

17 it's an investment in technology or investment in

18 people.

19 And I want to stress the people aspect because

20 not only is it an issue of having the technology in

21 place, but having the people to update the technology

22 when alerts are put out and bugs are discovered and

23 fixes need to be implemented, people to monitor the
24 processes to make sure that in fact they are running
25 properly, and thirdly, people to respond to an incident

0372

1 when it happens. If a breach does occur, are there
2 people there to respond to it quickly and close the
3 hole?

4 And the experience in the room among the large
5 industry planners was that, yes, there's a certain shall
6 we say percentage of companies on the Internet today
7 that do have shall we say crisis staff or security staff
8 that are available 24 by 7, but the vast majority do not
9 have people that are available under those kinds of
10 circumstances.

11 The other point I would like to make is there
12 was great discussion of evolving standards, that it's
13 hard to actually set a standard benchmark as to what
14 kind of security companies should have, but there was
15 discussion of penetration testing, similar to kind of an
16 idea such as a licensing entity such as TRUSTe.

17 There are also companies out there that actually
18 do auditing with ethical hackers, and they'll see if
19 they can penetrate your systems. If a company invests
20 in that kind of an audit and publishes the results of
21 their audit with the appropriate caveats in case a
22 breach does occur obviously, that in and of itself is

23 probably more useful to consumers than having some

24 explanation of what the technology is that's being

25 used.

0373

1 Thank you.

2 MR. MEDINE: I guess that raises a question as
3 to whether companies ought to commit to being audited
4 and tested as part of reasonable security measures.

5 Larry?

6 MR. PONEMON: I love the word audit, very good.
7 Let's use that word more.

8 Stewart, I think I disagree with the idea that
9 there are no standards. I think we can actually create
10 a too dumb to live standard, and it looks something like
11 this. Can you imagine getting on the walkway with your
12 local airport and you see a plane without wings. In
13 fact, they're putting on the wings. Now, would you fly
14 in that plane, and the answer is I hope not.

15 That's the too dumb to live standard. That
16 means you basically do not do things that are clearly
17 going to be very silly, right, or very dangerous or very
18 risky, but I don't think that adds any value. I think
19 what people expect is a certain level of disclosure and
20 a certain level of security, and they pray that they are
21 safe, that they are not the next victim.

22 They expect organizations to produce the risk in

23 the form of a statement that articulates in clear and

24 concise language that these are the risks. When you

25 transact business with us, these are the risks.

0374

1 Now, believe it or not when we do a financial
2 statement audit of a large corporation, we actually
3 evaluate the integrity of the technology
4 infrastructure. We're already doing a lot of that
5 stuff, so I'm not sure if it's impossible to create
6 reasonable standards in a relatively short period of
7 time. I'm not saying we as an industry. It could be us
8 or it could be government, but I think it is probably
9 doable and certainly doable in my lifetime.

10 I don't think though we could ever be in a
11 situation where we will not have -- we will have good
12 disclosure or great disclosure and good security or even
13 great security and still avoid the liability issue, so I
14 think whatever we do, we always have to think about
15 something will go wrong, bad things happen, and we need
16 to have a very good, very tight remediation strategy,
17 and so that's all we can do.

18 If we try to do more than that and try and apply
19 perfection, no one's going to go anywhere, so I think we
20 can and we should work to develop some baseline
21 standard that is hopefully higher than that too dumb to
22 live standard.

23 Thank you.

24 MR. MEDINE: Thanks. Dan?

25 MR. SCHUTZER: Well, we heard a lot of things so

0375

1 I would say that what have we heard? We've heard that
2 there's obviously some minimum level best practices that
3 isn't really tied to technology at all. Do you have a
4 security officer? Is he trying to keep up with the
5 software and the technology? Is he giving people
6 background checks to those people who are sitting there
7 matching the data? Are you planning to tell people that
8 when they send you data, it's all at their risk or you
9 can offer them some kind of recourse.

10 These are simple, straightforward kinds of best
11 practices and disclosures you can make about that
12 without getting terribly technical, and certainly I
13 still think that education plays a key role because the
14 truth of the matter is is that independent of firewalls,
15 cryptography, all that kind of stuff, it's social
16 engineering that normally breaks in and gets you your
17 access, and social engineering is walking around your
18 own end consumer and their lack of ignorance which they
19 need to be educated in to just who they should trust
20 when they're giving a kind of information.

21 So if somebody phones you up and says, I'm from
22 Citibank but they've initiated the call, I'm from

23 Citibank, could you please tell me your password or
24 something like that, then you would be remiss to give
25 that password. You didn't initiate it. You didn't

0376

1 contact the individual body. They contacted you. How

2 do you know who they are?

3 So I think that some combination of education,

4 of disclosure at a gross level say, Here's the kind of

5 best practices, we're not going to tie you to a specific

6 cryptographic algorithms or something? Do you have some

7 of the basics? Do you really have some professional

8 security staff? Do you do ethical hacking? You have to

9 describe of course what ethical hacking is. You don't

10 have to show the results.

11 That could get down to bits and bytes while

12 you're doing that. Are you keeping abreast? Are you

13 checking out your people? Are you using the normal good

14 prudence? And the disclosure, because you may find that

15 the kind of business you're in and for the level that

16 you're doing, you want to just say, No, I don't have

17 that, this is the kind of business I'm in, you're at

18 risk if you use it, but I think the kind of data I'm

19 asking and the kind of service I'm doing are not going

20 to put you too much at risk.

21 The bank said that then they wouldn't have any

22 customers anymore, so it depends on the nature of the

23 business you're doing and what kind of risk you have,

24 what you might want to advertise and what the customer

25 should come up with.

0377

1 MR. MEDINE: Thanks. I would like to continue
2 the discussion but transition it into the next subgroup
3 which is not significantly different from what we've
4 been talking about, focuses on managerial and technical
5 steps, and one of the things you talked about was
6 employee screening and training and access issues.

7 So Rebecca had her card up before that, so
8 you're free to talk about the prior or current or both.

9 MS. WHITENER: Rebecca Whitener. Actually
10 several of the points I was going to make have been made
11 and have been made very well, but I wanted to again go
12 back to the whole issue of the importance of the process
13 and the organization, and in fact in looking at what
14 does make up appropriate security, generally companies
15 have used some form of risk assessment to determine the
16 appropriate mix of organizational types of processes
17 and/or technology that is necessary to address risk.

18 However, many times that risk assessment has
19 been built on the risk that the company perceived in
20 terms of their information assets from the standpoint of
21 the confidentiality, integrity and availability of those
22 assets so that if it was company financial, proprietary

23 information, it would be very miss and critical, and we
24 want to make sure we have the appropriate safeguards and
25 the controls of that information.

0378

1 I think as we begin to talk about customer
2 information and appropriate risk assessment and/or
3 security safeguards for that, it may be in a different
4 mind set or a model that companies are moving in to
5 because in reality, the risk associated with disclosure,
6 customer information, particularly customer names and/or
7 contact information, may not have been as high on the
8 list in the past as it is now becoming as the risk is
9 beginning to be seen as a far greater risk for improper
10 disclosure.

11 So perhaps what companies need to be aware of is
12 that in their current processes for evaluating risk
13 assessment and determining the appropriate controls,
14 that they begin to view company data a little bit
15 differently than they have in the past.

16 I like the analogy of the airplane, but another
17 analogy that I also like to use in terms of what
18 consumers expect when it comes to security is that when
19 a consumer buys a car, they don't but that car because
20 it has great brakes, but they sure expect that that car
21 have brakes when they buy it.

22 And so in many cases it's the same way when a

23 consumer does business with a company that they trust

24 and they have confidence in, they don't necessarily have

25 to know how those brakes work or how the security works,

0379

1 but they sure want to have the confidence that those

2 brakes are in place.

3 MR. MEDINE: Thanks. Dan? Alex?

4 MR. GAVIS: Alex Gavis, Fidelity. I think in

5 terms of the custody and storing of data which would be

6 sort of internal practices, I think it's very important

7 to consider a reasonableness standard and a standard

8 that sort of takes industry by industry because I think

9 the only way, particularly if you're looking at sort of

10 broad mandates or broad sort of policy making in this

11 area -- the only way that you'll be able to handle it is

12 by essentially looking to best practices in each

13 industry because there are different industries that

14 handle different information differently and have

15 different sensitivities and have different levels or

16 need to store information.

17 But I think there's another part of security

18 that's important which is I would term maybe

19 connectivity security which is how the customer connects

20 to you via the Internet, and I guess an analogy would be

21 we have telephone systems, automated telephone systems

22 that we use that customers can call in and actually pick

23 up their account balances or perhaps even do exchanges

24 and trades.

25 Well, they could connect to us via a cell

0380

1 phone. They could connect to us via a secured phone
2 line, and with that kind of connectivity, in a sense we
3 can't prevent them from connecting with us by a cell
4 phone. However, we can use disclosures to educate them
5 and to actually talk to them about the way in which they
6 might connect up with us.

7 The same way with the Internet. We can actually
8 use disclosure to talk to our customers about browser
9 encryption, what is 40 bit encryption, what is 128 bit
10 encryption, and in fact with financial data and
11 information, our customers are very interested in
12 learning from us how we connect with them and what kind
13 of security measures we use.

14 And in fact disclosures I think and the use of
15 educational disclosures are very, very important in this
16 area.

17 MR. MEDINE: I think it would be very useful to
18 again hear her the committee's views on this issue of
19 transmission security and the obligation on the part of
20 the web site to provide a security method of
21 transmission. Is it a notice and choice situation for
22 the consumer as to whether they choose to do business

23 with sites that don't provide transmission security?

24 Again either your thoughts or committee thoughts

25 in general would be very helpful on the issue even on

0381

1 route what are the responsibilities of the parties.

2 Lance?

3 MR. LANCE HOFFMAN: Lance Hoffman. I think even

4 before we get to transmission security in those in some

5 sense technical details, I'm taken a lot by what my

6 fellow committee members have said, and I want to extend

7 it. We have on a number of web sites but certainly not

8 all of them privacy statements already. It may be there

9 should be a security statement as well, and I'll get to

10 that more in a moment because I can see this sort of

11 akin to the ingredient label.

12 You get an ingredient label on food or on

13 vitamins or things like that. You don't have to -- you

14 can choose. You the consumer can choose exactly what

15 you want, and if it's simple enough it may actually be

16 useful. It has to be simple because I have found

17 teaching computer security for 25 years, utility trumps

18 security every time, okay?

19 Given that, what can you get it down to? Well,

20 there are only a few things. One is people. We have so

21 many people doing security or so many people per -- for

22 the size of our business per a hundred or a thousand

23 customers or whatever it is.

24 The next thing is audit there is no way you can

25 say we're doing 128 bit encryption or this or that or

0382

1 anything else that is not going to confuse people more
2 than it's worth I think. Much better off saying, Last
3 time we were audited by so and so was on this date and
4 here's the URL to the executive summary or something
5 like that.

6 So there's people, audit, and the third thing is
7 liability. If you don't like this, here's your
8 recourse. That simple, that kind of statement on what's
9 going on in security doesn't bind you, doesn't tie you
10 up to a given security architect which is going to
11 change all the time, does address indirectly raising the
12 standards of both what security has done and who's going
13 to do it.

14 Do you have any idea what the average tenure is
15 of a security officer in an installation? Last time I
16 looked several years ago it was three months. That's
17 the career path. So I mean we've got problems here. I
18 think a simple label might do more than anything else.
19 To put in standards is pretty premature at this point.

20 MR. MEDINE: Stewart?

21 MR. BAKER: That was great, so you've got the
22 auditors, the computer security guys and the lawyers all

23 hired in one speech, and I especially like the airline

24 analogy. I expect it to be told many times now, At the

25 recommendation of the FTC please put down your reading

0383

1 materials for an important message. I think the
2 internal plan idea has a lot of promise, but it does
3 separate the I'm too dumb to live from people who have
4 thought about it and provides for some flexibility.

5 And I suppose if you have a disclosure of some
6 elements of it given the FTC's deceptive practice
7 jurisdiction, I think it still leaves us with a question
8 of, Well, what do you do if it isn't good enough or how
9 do you decide it isn't good enough. I don't think the
10 idea of going in after there's been a problem and then
11 finding the plan inadequate is a good one.

12 All patents are obvious after the fact, and all
13 security's inadequate after it's failed so that's
14 probably not the right way to approach it, and again I
15 think it's very hard to leave people responsible for the
16 consequences to consumers.

17 I have -- I'm carrying around this device that
18 the state of Virginia gave me that discloses the best
19 way to steal my identity. It gives my Social Security
20 number to anybody who looks at it, and then you just
21 have to find out my mother's maiden name which isn't all
22 that hard and you're done.

23 MR. MEDINE: Again for the record that was your

24 driver's license.

25 MR. BAKER: Yes. Does this mean Virginia is

0384

1 liable for having disclosed this private information

2 about me or have they now made it public?

3 So I think that is a problem, and I think also

4 the idea that we can say, Well, dummy, you didn't follow

5 the CERT advisories. I'm willing to bet there's nobody

6 in this room who has all of the CERT advisories

7 accounted for in his machine with the possible exception

8 of I guess Tom.

9 MR. WADLOW: Thank you.

10 MR. BAKER: That's a very expensive proposition,

11 and I think trying to set a minimum standard is just not

12 going to work for us.

13 MR. MEDINE: Rick?

14 MR. LANE: I would just like to echo this.

15 Security I think is a process, and how you go about it

16 depends on what the needs are, but also getting to best

17 practices, we held The Partnership for Critical

18 Infrastructure at the Chamber last week. We had over

19 120 corporations talking about how we protect the

20 nation's infrastructure, and it's not just physical but

21 network security and it was kind of in addition to what

22 was going on at the White House.

23 The biggest problem in terming best practices

24 was the sharing of information and the antitrust laws

25 and FOIA. So there are current laws in place that

0385

1 hinder the ability of an AOL to talk to a Yahoo about
2 security, so I mean there are some issues out there that
3 need to be addressed on a broader -- before we even get
4 to the best practices, can we even share best practices
5 or is that a violation of antitrust?

6 MR. MEDINE: Let me step into my role as an FTC
7 official, not on the competition side, but I want to
8 just note the fact that the Commission gave the Direct
9 Marketing Association an opinion that they could require
10 as a condition of membership adherence to certain
11 privacy practices.

12 We are very willing to entertain that
13 possibility elsewhere and would be happy to engage in
14 dialogue and have discussions and not let notions or
15 undue fears of antitrust liability interfere with good
16 efforts.

17 I'm not going to say that that's going to cover
18 the whole territory, but it's worth I think a dialogue
19 so we see where the lines are drawn.

20 MR. LANE: Just to continue on the transmission
21 side and get back to the wireless issue, I mean I have a
22 digital phone here that was secure three months ago that

23 is no longer secure. If I make a trade over that or
24 whatever I dial into has a potential of being tapped
25 into, recorded and used by somebody else.

0386

1 Is that the fault of QualComm who makes the
2 digital phone? Is it the fault of the end person or the
3 end company I'm going to who for whatever reason can't
4 stop or prohibit me from using my digital phone, or is
5 it my fault for not knowing any better?

6 And if we try to legislate that, it's the
7 business's fault for a consumer not knowing any better
8 we get into a really dangerous territory.

9 MR. MEDINE: We have a critical infrastructure
10 commissioner formerly. Mary?

11 MS. CULNAN: Mary Culnan, but that's not what
12 I'm going to talk about. We did address, did raise the
13 issue of the antitrust information sharing issues in our
14 report so hopefully something will be done about that.

15 But I want to go back to the -- I agree with the
16 point that's been made that security is a process and
17 it's very context driven and it changes and all this
18 kind of stuff, but in the financial world there is an
19 analogy that might help us. If you want to invest in a
20 publicly held company, you don't have to go in and you
21 can't go in and look at how they do business and how
22 they keep their books by themselves.

23 But if you get their annual report and open to
24 the front page, there's a statement with standard
25 language from the public accounting firm that has

0387

1 audited them saying they adhere to Generally Accepted
2 Accounting Principles, and that doesn't say they
3 implement all the CERT advisories.

4 But it says for their situation, they play by
5 the rules, and you can have some confidence that it's
6 okay to go ahead and do business with this company, that
7 they haven't cooked their books.

8 I think that might be a good analogy. It's an
9 easy to understand disclosure once people have learned
10 what it means, and it provides a way to have a sliding
11 scale. The only issue is who does the audit and who
12 provides the notice in a way that's fair to small
13 businesses and big companies since doing an audit is
14 very expensive, and Larry left the room, and in a way
15 that's not scoopable, right.

16 MR. MEDINE: Right. Ted?

17 MR. WHAM: I don't know how Mary got on the list
18 before me because she stole one of my points here much
19 to my chagrin, but very similarly, it's the UL for
20 auditing rights or it's the Underwriters Laboratories.
21 There's a set of rules that come in to there, and you
22 can simply say, I followed the set of rules or I didn't

23 follow the set of rules.

24 I was reading an annual report on the way here

25 for an investment that I've had for about a year and a

0388

1 half that has just done terribly. I'm almost holding
2 the investment out of morbid delight anymore to see how
3 much worse it will get and whether I come back up, and I
4 was going through and looking at the report, right, and
5 there's the blather from the chairman, right?

6 You never read what he says. Who cares what he
7 or she says. It's the stuff which are coming down into
8 the actual financials itself, and I can have confidence
9 that there's something there even though I have no idea
10 how they're actually doing the audit because there's
11 somebody who does have some idea of what an appropriate
12 set of standards is who's come through and said, Yes,
13 they've played by the rules.

14 Auditing was invented by Pacioli I believe back
15 in the 1500s, and yet they find ways to set standards
16 and those standards change. For us to say that we can't
17 set standards is I think to let ourselves off the hook
18 far too easily, that it is possible. The only question
19 in my mind is what is the appropriate body to set those
20 standards and what are the mechanisms for those
21 standards to resolve overtime and things progress and
22 become available for them.

23 Another point was brought up on disclosure
24 information. I'm 110 percent in agreement with what
25 Lorrie was saying, with what Deirdre has mentioned. The

0389

1 average consumer is not going to be able to care, know
2 what the difference between 128 and 40 bit encryption is
3 nor are we ever going to successfully teach them what
4 that is.

5 I think that instead if we can point to a
6 third-party and say, You met the standard, you did not
7 meet the standard, that's going to be a much more
8 effective way of doing that.

9 The final thing is assessing costs and
10 appropriateness of measures. There's two different ways
11 I think someone earlier brought this up, that there's
12 the cost to the organization if they disclose the
13 information, and there's the cost to the consumer if
14 they disclose the information.

15 I think market forces will take care of the cost
16 of the organization. The organization will implement
17 appropriate security measures to make certain that
18 they're trying to protect that asset to whatever value
19 it is to them. If it isn't very valuable then they
20 won't spend much money on it, conversely if it is.

21 The issue is if it's more valuable to the
22 consumer, the identity theft example was brought up, and

23 again I'm going to agree very strongly and steal

24 Deirdre's ideas here, this is a market failure. There

25 is not a market incentive that is appropriate enough to

0390

1 take care of the organizations around this table to make
2 certain that they value the data to the same degree
3 necessarily that the customer does.

4 And that's why you have governments. That's the
5 province of legislation to put that in there because if
6 left just to industry, we're going to act rationally and
7 value it based upon our own needs around those things
8 including the risks of PR and so forth if that
9 information is disclosed.

10 To be able to determine what the appropriate
11 security is, however, for that information, that means
12 you need to know what the value of that information is
13 to the consumer, and I don't think I can succeed as a
14 business of having a security implementation for this
15 record which is different from this record.

16 I don't think I can do that, which again ties
17 down to a premise that I hold very strongly, and that is
18 that I think that for any given class of data or data
19 element there is a security threshold that you have to
20 hit, and it's very black and white, did you hit it, did
21 you not hit it, is it, you know, medical information
22 that you can't share or is it financial information that

23 you can't share under any information or is it adverse

24 information that isn't as bad if you share it, et

25 cetera.

0391

1 And there has to be some way of valuing those
2 data costs to the consumer to hold industry then
3 responsible.

4 MR. MEDINE: By the way, just to make it clear,
5 we do pay attention to and take seriously what our
6 chairman says at the FTC. Dan Jaye.

7 MR. JAYE: Dan Jaye. A couple points related to
8 the security management and insurance process. I am
9 very concerned about audit being the only solution for
10 the smaller companies, albeit there may be -- there may
11 arise a set of outsource services that allow smaller
12 companies to have all the security protections of a
13 larger company because they get the economies of scale
14 of using an outsource service, although that introduces
15 another bunch of issues in that you have to trust the
16 outsource service which is now holding customer data on
17 behalf of lots of different companies, so there's sort
18 of a little bit of a catch 22 that you have to work
19 through.

20 But I go back to my prior life in the financial
21 services industry and there certainly are when we deal
22 with sensitive data a variety of techniques that can be

23 used that I think can credibly create assurance of

24 security. I remember being bonded as an employee of a

25 company that had sensitive financial information and

0392

1 having to have my fingerprints taken and actually
2 wondering as an employee the loss of anonymity, that all
3 of a sudden it was public record, that I had my
4 fingerprints in some database somewhere, but -- which
5 does bring up the issue of employee privacy and right of
6 data, but I do think that there's certainly a clear high
7 watermark.

8 There's privacy audits and, sorry, data security
9 audits that I have been in in my prior life and current
10 life, and I do think that once again it is possible for
11 accounting firms and entities to issue guidelines such
12 that in a privacy policy you can say, We have been
13 reviewed by such and such and they've -- for a copy of
14 their opinion or to reference the summary of their
15 opinion, you can reach that.

16 My concern is as we look at the sensitivity of
17 different types of data that we still don't create an
18 impractical market for the smaller entrepreneurial start
19 ups and innovators to enter and compete because they
20 can't afford to have five out of the six first employees
21 be data security and privacy compliance officers.

22 MR. MEDINE: You touched on the employee issue,

23 and again if people would like to address the issue of

24 security vis-a-vis your own employees and access

25 controls and so forth and whether there are clear

0393

1 standards there or not as compared to general technology

2 standards, that might be helpful.

3 Frank?

4 MR. TORRES: Frank Torres, Consumers Union. I

5 think in getting to that point a little bit, clearly we

6 need to develop mechanisms so that the smaller companies

7 who are doing business online aren't at a competitive

8 disadvantage when it comes to security. I mean, there

9 are small restaurants that still have to comply with the

10 health code and still get inspected.

11 Maybe we need to think of something to help out

12 the small businesses in this regard. I was happy to

13 hear Ted's comments and others that people do think that

14 there can be some minimal standards that are developed

15 to provide the consumer with some assurances because

16 after all, isn't that what we're about, and that is

17 to -- what can we do as far as security goes?

18 I think it's one issue that we all agree on that

19 something needs to be done, so that the consumers using

20 the web have confidence that the security's protected,

21 and I think that we need to exercise some caution when

22 -- in thinking about if I do trades online, am I

23 assuming the risk or is it -- or can I depend upon the
24 company with whom I'm conducting these trades that
25 they're doing what they need to do?

0394

1 Because if we've got a bunch of consumers that
2 all of a sudden lose the money because of a security
3 breach and the response from the business community is,
4 Well, you should have read our statement, it's going to
5 be a strong disincentive for people to offer good words
6 of advice to consumers saying, Well, gee continue to
7 doing business online as opposed to, Well, there's
8 nothing that you've got that you can latch on to to
9 provide you with some confidence when you do do business
10 online.

11 So I think we need to exercise some of that to
12 secure data.

13 MR. MEDINE: Thanks. Andrew?

14 MR. SHEN: Andrew Shen. I think I share the
15 same skepticism of a lot of the earlier speakers about
16 notice and choice. I have some of that same skepticism
17 to all sorts of privacy practices, but security
18 especially. I think a lot of the terms and technologies
19 ought there, even the little browser window locks, are
20 still beyond a lot of people.

21 And on a second sort of larger point, I think
22 it's really interesting that so far in the realm of

23 security, we've talked a lot about dispute resolution,

24 auditing. We didn't extend any of the same topics when

25 we were talking about access because wherever we draw

0395

1 the line of access, what is proper access, what is
2 reasonable access, wherever it may be, there still needs
3 to be some way to verify whether it's through TRUSTe,
4 PricewaterhouseCoopers, FTC, that those companies are
5 actually providing access to all the information that is
6 there.

7 MR. MEDINE: Thanks. Dan Geer?

8 MR. GEER: Yes. Dan Geer, @Stake. On the
9 security front, I assume that this is common knowledge,
10 but if it isn't I would be remiss in not saying it. For
11 all of you who don't deal in that arena regularly, by
12 far the greatest threats to any business are internal
13 and not external by far, and so businesses, if they are
14 not themselves too dumb to live, already have a
15 considerable incentive for data integrity and the like
16 on an internal basis.

17 And I suspect that most of the conversation
18 today has not dealt with that because in some sense it
19 solves itself. Either you pay attention to your
20 internal data or your trade secrets walk or whatever it
21 might be. I mean, there are serious incentives there.
22 There's no argument. I think those of you who use the

23 phrase market failure, and I'm not an economist so it's

24 possible that I misunderstand it, but there's no market

25 failure in terms of protecting yourself on the internal

0396

1 side because it's well understood in the regulated
2 industries, which tend to be the ones, by the way, that
3 collect the most data because most of the time they are
4 the ones required to collect the most data.

5 With that being said, I'm not myself all
6 together certain that we have had enough market trial to
7 know that we have had a market failure in the consumer
8 space. In the field I'm working in now, as far as I can
9 tell for Internet start ups in particular, first mover
10 advantage is so substantial that anything you do that
11 loses your first mover advantage is as close to suicide
12 as it can be.

13 And in particular having any kind of failure
14 that costs you the one thing that you trade your -- on
15 IPO day you trade in your reputation capital for money,
16 that's what you do, and anything that costs you your
17 reputation capital, whether it's that you can't keep
18 your servers up, I don't want to pick on EBay, but you
19 get the idea, or that you put too many credit card
20 numbers in the same place, CDU -- those kind of things
21 which take -- CD Universe, right, those kinds of things
22 which take the reputation capital that you are amassing

23 which is the only value you have, of course prior to

24 revenue, those things I would argue are such a strong

25 incentive that the only thing that keeps people from

0397

1 paying attention are the same things that keep them from
2 paying attention to anything else that doesn't --
3 doesn't lead them to getting out the door as fast as
4 possible.

5 I don't think, in other words, that we've had a
6 sufficient market test to declare a market failure even
7 though I would not know how to explain most of what I do
8 to most of the people I do it with, and so there's no
9 argument that this stuff is complex, particularly at the
10 edge where you're talking about protecting yourself
11 against the unseen villain kind of thing, but don't
12 confuse that with the absence of incentive.

13 MR. MEDINE: With regard -- let me just follow
14 up.

15 MR. WHAM: I'm going to try to intercept one
16 quick comment. I'm going to through a market failure
17 out there and enforcement failure, in my opinion I
18 believe it was XXXXXX, correct me if I'm wrong somebody
19 here, please, that was identified and sanctioned by the
20 FTC for deceptive trade practices where they said they
21 selected

22 (GROUP OF SPEAKERS:) GeoCities.

23 MR. WHAM: GeoCities, thank you. The day after
24 that enforcement action came out, if I'm not incorrect,
25 the IPO kept getting enormous explosive, about five X

0398

1 times their initial offering. The cost of some of this
2 information are not borne by the market. There are
3 costs to the consumer in many cases, and I think it's
4 very risky to be dependent completely on the market.

5 MR. GEER: Well taken. I don't want to debate
6 you personally, but my actual training is as a
7 statistician, and one outlier does not a trend make.

8 MR. MEDINE: Can I go back to your point about
9 internal threats? Can you -- is it possible to
10 articulate a minimum standard of care with regard to
11 internal threats, or does that also fall under
12 reasonableness?

13 MR. GEER: Sure, speaking as someone who has
14 tried to sell security partners for better than a
15 decade, there are only two people who are willing
16 customers. That is someone who has just been
17 embarrassed in public and someone who's facing a
18 management audit. You can wave now. Those are the only
19 two people -- that's the only two people who are ready
20 customers that think that they want to buy.

21 Now, in terms of where the threats are, by and
22 large the threats in a large -- in a corporation of

23 internal -- internal misuse represent the misuse of

24 legitimate authority. It's not a question of whether

25 this person is who they said they were or whether they

0399

1 actually had authority. It's misuse of legitimate
2 authority. That tends not to have a technical solution,
3 but it tends to have a process solution back to this
4 point of technique versus process.

5 MR. MEDINE: Deirdre?

6 MS. MULLIGAN: Deirdre Mulligan. I wanted to
7 talk a little bit -- you were talking about cell phone
8 connection. How do you deal with client side or
9 individual decisions and the security risks that they
10 may pose? And you have that both if you have an
11 employee who's trying to dial in or use a remote device
12 to access information, how do you deal with the risks
13 that that poses because they're not on site but also
14 from the consumer perspective?

15 And I agree with you that it's hard to sometimes
16 derail those risks without some costs, but I do think --
17 I want to get a little personal CDT experience. We
18 sometimes run different kinds of petitions and things
19 where we ask people if they want to join.

20 And sometimes in order to participate, they give
21 sensitive data. We had one where we were allowing
22 individuals to, for example -- we were assisting them in

23 opting out of different things, some of which might

24 require financial account identifiers because they were

25 for banks, some of which required Social Security

0400

1 numbers, and we had both a fairly high level secure
2 server where we were handling things, but we also found
3 out that there were individuals who were back dooring
4 into the cue and coming in through on an insecure page.

5 And I went and I made a decision despite the
6 fact that I could have told people that you're putting
7 yourself at risk, institutionally I'm not willing to let
8 people who I don't think can assess the risk make that
9 decision, so what I did instead was they had to download
10 the form, print it out and fill it out manually.

11 Now, I got a lot of people calling me and
12 saying, Hey, I want to be able to fill this in online.
13 And I said, Well, look, you're behind a firewall, you
14 can't get to my secure page, there's a risk of you
15 putting this data and transmitting it over the Internet
16 insecurely and schedule, and that's why I won't let you
17 do this and I understand you're willing to take this
18 risk, but institutionally I don't want to be inviting
19 you take that risk and so I'm going to force you to do
20 it this way.

21 And you can make that decision as a business to
22 help direct people to better security choices. I

23 realize that there are downsides. Sometimes consumers

24 get frustrated and I have had that experience, but I do

25 think as somebody who was in a better position to assess

0401

1 the risk that I also take on a responsibility to educate

2 people about those risks and help direct.

3 MR. MEDINE: Thanks. Greg?

4 MR. MILLER: Greg Miller, MedicaLogic. As a

5 side bar, I would move the Commission to consider

6 striking the errant reference to XXXXXX on the record

7 since it is a public record, and everyone is extremely

8 sensitive now about being blamed for things that they

9 didn't do.

10 MR. WHAM: I think that's an excellent idea.

11 MR. MILLER: Secondly, with regard to this

12 whole notion of standards, I think the discussion has

13 been moving this way so it may be redundant to just come

14 out and say it, but it seems to me that we need to move

15 to standards of care as opposed to standards of

16 technology or standards of practice.

17 The problem that we have, and I too referring to

18 Rick's comment earlier, was at the Critical

19 Infrastructure Partnership Summit, and one of the things

20 we were talking about is that liability will come and,

21 Stewart, it's going to happen, and the problem is this.

22 It's going to be standards of care.

23 At what point does the mom and pop shop who's

24 decided to take their silk flower business and put it

25 online, calls up Dell, orders their first NT server

0402

1 ever, is totally jazzed and excited about their new DSL
2 connection and, Look, Ma, I can have a phone
3 conversation while being on the computer and this is so
4 cool I'll never shut it off -- how many of those of us
5 out there with DSL connections are leaving our machines
6 on for hours or days at a time and have no idea or
7 knowledge that we currently are parking DEOS code for
8 another denial of service attack on the net because of
9 all of these Window's machines out there on the net with
10 DSL connections.

11 And you know what? I've got my best friend who
12 works, and MedicalLogic has that, and he doesn't even
13 know what to look for. He wouldn't even know where to
14 start. The first thing he did was he pulled the plug on
15 his DSL collection because he suddenly panicked.

16 He was reading USAToday, and they say, Hey,
17 liability and negligence is coming, and I think we're
18 well served here to think about you don't know what you
19 don't know, and maybe we should be thinking of standards
20 of care and let other bodies emerge to help understand
21 what the technical aspects of that are, but what's a
22 standard of care for a small shop since small business

23 runs America?

24 MR. MEDINE: Good question. Dan?

25 MR. SCHUTZER: Talking about this standards

0403

1 stuff and audit and so forth, and I guess it may be
2 strange, but I think you really ought to think about
3 moving in that direction, kind of a tiered kind of
4 service.

5 I belong to one of the most heavily regulated
6 industries because of the sensitivity of the kinds of
7 data and service we have, so we have internal audits,
8 external audits, and everything else, and it's a cost of
9 doing business I might say, and of course in the web now
10 people recognize that's fuzzy so you may not be a bank,
11 but if you're acting like a bank, you look like a bank,
12 smell like one, you're holding the financial
13 information, providing financial advice, you're offering
14 some kind of payment service, then you probably should
15 be subjected to the same kind of regulation I am.

16 But on the other hand, let's say I as a bank or
17 you as a company want to go into some other kind of
18 service, let's say I want to throw up some kind of
19 bulletin board service where people can sit around and
20 chat about advice in different sectors and so forth,
21 buying, whatever, then I think -- and I make it clear
22 that all I'm doing is providing a service where people

23 can come and chat and talk and I'm openly not assigning

24 any kind of security officers or any kind of audit

25 processes to this and no security and I'm not going to

0404

1 be held liable for it, that might be a service that
2 should be answering to a different level of standards
3 perhaps even without order because now I'm trying to do
4 a different kind of business with different kind of
5 data, different kind of sensitivity.

6 So I'm trying -- sometime in the future we may
7 find that that kind of business exposes us to a
8 different kind of risk, you get concerned and people
9 will then talk at that kind of a business to for a
10 different level of protection, and that seems to be the
11 way we work in the U.S., but when we can recognize that
12 there's a concern where people are at risk, we then put
13 down certain kinds of standards and orders.

14 But for a small business to get up and get
15 started or even a large business in this other sector,
16 they should be allowed to tell what you they have in
17 disclosure, and it may not be the same level of standard
18 to require audits to the same kind of degree or at all
19 to what you might require in a financial or medical kind
20 of an industry.

21 MR. MEDINE: Andrew, was your -- John?

22 MR. KAMP: Yes, I would just like to make a

23 small--

24 MR. MEDINE: Can you identify yourself?

25 MR. KAMP: John Kamp from the AAAA. I want to

0405

1 associate myself with the notion here that we're talking
2 about a very important reputational value of doing
3 things in secure ways, and in fact my remembrance of the
4 effect of the GeoCities case is very different than
5 Ted's.

6 I remember it having a very serious effect on
7 the GeoCities, the value of GeoCities, and I think we
8 must remember that in these cases when the FTC or
9 another official body does something that calls into
10 question the security or other reputational value of a
11 company, it has a tremendous effect, and that's a
12 positive thing. That's a positive thing for the value
13 of this agency operating in this space, and in no way do
14 I want to minimize that here today.

15 MR. MEDINE: Thank you. Jerry.

16 MR. CERASALE: Jerry Cerasale, DMA. I wanted to
17 agree with Mr. Miller that I think we have to look at
18 some standard of care. From the point of view of
19 security and the DMA guidelines that we have, you have
20 to train people, make sure you have access, certain
21 things of that sort, and I think that's a standard that
22 we say.

23 I also think however that we have to be careful
24 here with security, and I think that what we're thinking
25 about now is security of the information that we

0406

1 collect. I don't think it's security of the server
2 that's only been used to go bombard Yahoo or
3 something of that sort. It what we're charged to look
4 at. It's just information that we have.

5 It's important, it is -- the reputation that
6 John just talked about is very important, and word gets
7 around in this new system of ECommerce.

8 This Christmas time when there were press
9 stories concerning -- and the FTC knows lots about
10 this -- certain web sites being unable to produce goods
11 at times promised or within the proper rules, and
12 they're doing some looks at that, we found a significant
13 drop off in orders that unfortunately spilled over into
14 the catalog area two weeks before Christmas time.

15 And so a big boom in our business and then
16 suddenly a stop or virtually a stop right before
17 Christmas two weeks before because of the press reports,
18 so reputation is very important, and I also think that
19 as we go into having -- so it's important for businesses
20 to do that on the -- so they want to make sure they have
21 security.

22 And the other is I don't think we're ever going

23 to amiss liability, and I think that from that score as

24 you look at it, liability potential is going to be the

25 major force here to get -- to make sure that ECommerce

0407

1 businesses take care of the information we have on
2 individuals which is I think what we were talking --
3 what we're charged with looking at here. Thank.

4 MR. MEDINE: Thanks. Tom.

5 MR. WADLOW: A couple of things here.

6 MR. MEDINE: Identify yourself.

7 MR. WADLOW: Tom Wadlow, Pilot Network
8 Services. The gentleman over here in the corner, I
9 apologize for not knowing your name, had spoken awhile
10 back about outsourcing security and allowing the small
11 companies to compete on the same basis as larger ones.

12 I want to thank him because he essentially
13 described my business plan in a nutshell, and we've been
14 doing that for quite awhile. Some interesting
15 experiences to share about that that I think are
16 relevant, some of the things that we do, some of the
17 practices that we follow are in fact that we do have
18 ourselves audited on a regular basis by outside
19 agencies, and I mean mean nasty audits so they really
20 come out good.

21 We want to get pain so we make sure we're doing
22 it right. We do that. We provide summaries of those to

23 our customers and to our prospects, and that -- and we

24 also do background checks, and we were asking about that

25 fairly hefty within the limits of the law, of course

0408

1 background checks on everybody that we hire from the
2 receptionists all the way up to the security officers.

3 And that has served as very well in terms of
4 getting customers, but it's a very interesting thing to
5 go back to something that Dr. Geer was saying which is
6 that those same customers who work really hard to make
7 sure that we live up to their expectations from a
8 security standpoint are also the same ones that don't
9 want to wait an extra day for example for a code review
10 of their CGI code because it would take too long and it
11 would keep the web site from getting online.

12 And for those of you who aren't aware of it, any
13 time you've ever seen graffiti on a web site or a web
14 site broken into, there's an excellent chance it came
15 through a hole in their CGI code so it's a matter of
16 that people want this at least in principle, but in fact
17 in practice they are very reluctant to put up with some
18 of the demands that getting those things take.

19 The other thing I wanted to mention and also
20 talk about something that Dan said is that the
21 fundamental operating principle that we work under is
22 that anybody can break into anything if you have

23 sufficient skill, motivation and opportunity, and

24 therefore our goals in everything that we do are to

25 raise the skill bar very high.

0409

1 We know you can never max it out. There's
2 always going to be someone that has more skill, but you
3 want to reduce it, require a very, very high level of
4 motivation from the hacker and give them as little
5 opportunity as possible to do that.

6 The reason why I'm referring to Dan's comment is
7 that if you think about the people that have the highest
8 skill, the highest motivation, the highest opportunity
9 they are in fact the people that work in your company,
10 and those insiders are really, absolutely the most
11 dangerous people around, and that's something that
12 really has to be checked, and it really has to be made
13 certain whenever you think about security for any
14 reason.

15 MR. MEDINE: Thank you. Given the hour why
16 don't we take a 15-minute break and come back and
17 discuss the security three and then go forward into our
18 wrap up. Thanks.

19 (A brief recess was taken.)

20 MR. MEDINE: I understand Ron Plessner would like
21 to make a request.

22 MR. PLESSER: Out of courtesy to our West Coast

23 colleagues and out of courtesy to some of us that have
24 work to do at the end of a Friday, I would wonder if the
25 Chair would consider having the committee assignment

0410

1 discussion now so that we can get that resolved for
2 people who have to leave, and then you can continue on
3 with the public comment.

4 But it would be helpful if we could do it that
5 way.

6 MR. MEDINE: Is the committee amenable to
7 shifting things and moving on to assignments? I'm
8 seeing lots of nods. I'll say ayes as opposed to nays
9 and the ayes have it.

10 (Discussion off the record.)

11 MS. MULLIGAN: As long as everyone doesn't run
12 out before the public comments happen.

13 MR. MEDINE: I'll tell you what, let's see if
14 there's any expression in interest in public comment, so
15 we can -- is there anybody present from the public who
16 would like to make a comment? This is it? Then we
17 certainly don't want to shortchange public comment, but
18 I think we've given it sufficient opportunity.

19 Okay. Then moving on to the suggestion at hand,
20 just to reiterate my comments this morning, what we
21 would suggest to the committee is that it move into the
22 next stage which is the committee has done a suburb job

23 fleshing out the issues and the outlines and the

24 discussion today, and we would recommend the committee

25 move on to developing specific options with regard to

0411

1 access and security, and that subgroups be formed to
2 create those options, that those options be circulated
3 to the committee through us and put on the web site as
4 the outlines were for this session, deadline for
5 submission of Friday, March 24 which would give us a
6 chance to have that up on the web site and give the
7 committee a week before the next meeting which is March
8 31 starting at eight a.m. as a courtesy to our West
9 Coast visitors to review it.

10 So option papers, March 24, and then we can
11 spend the next meeting on the 31st discussing the
12 variety of options that have emerged.

13 I guess we are -- your designated federal
14 officer is prepared to suggest some subcommittees and we
15 in light of our experience last time have taken a stand
16 of putting together some subcommittees and subcommittee
17 assignments. If there are others who would rather
18 proceed a different way, it's your committee, but once
19 again we're prepared to serve, if that's the committee's
20 pleasure.

21 MS. SWIFT: Go for it.

22 MR. CERASALE: Please serve.

23 MR. LANE: Wait, wait, hold it. I have a

24 question.

25 MR. MEDINE: Could you identify yourself?

0412

1 MR. LANE: Rick Lane. If you are not happy with
2 the pre assigned committees, I would just like to say
3 that you have -- we should have the option to pick the
4 committees that we are interested in and let you know by
5 such and such date, whatever date is determined. That
6 way everyone feels that they're in the appropriate
7 place.

8 MR. WHAM: My only concern about that is --

9 MR. MEDINE: Identify yourself.

10 MR. WHAM: This is Ted Wham -- that my fellow
11 committee members might want to remove me.

12 MR. LANE: You can't remove someone else. You
13 can only change your own personal identifiable
14 information.

15 MR. MEDINE: Here's our goal here. We've tried
16 to form these sub groups to have a range of background
17 and experience to bring to the table. I guess what I
18 would propose those who wish to change perhaps could
19 contact the committee, FTC staff serving the committee
20 within the next two or three days to clarify any changes
21 and so that the groups can get working; is that --

22 MR. LANE: By close of business Monday?

23 MR. MEDINE: Okay. Jonathan?

24 MR. JONATHAN SMITH: Jonathan Smith. I just

25 have a procedural question. Will these groups be the

0413

1 groups that will stay in place until the final report is
2 due May 15? That is, if we are to produce options this
3 will probably be the end grouping?

4 MR. MEDINE: You're already thinking further
5 ahead than we are. I think we're amenable to going
6 either way on that. Do committee members have feelings
7 one way or the another on the that? Identify yourself.

8 MR. PLESSER: Ron Plessler. Maybe the way to
9 resolve this is to request that mainly you stay where
10 you assign them, but if somebody wants to double up and
11 go on another committee as well, that that's something
12 you can entertain. I would maintain your balance but
13 then allow people to share.

14 MR. MEDINE: Share some particular expertise in
15 other areas, that might be an useful.

16 MR. LANE: Well, that doesn't that -- if I'm
17 not -- Rick Lane U.S. Chamber of Commerce. If I'm not
18 interested in being on a committee and I go on and
19 double up and I just don't participate in the other one,
20 is that just kind of de facto I'm taking myself off of
21 that one and going to another one?

22 MR. MEDINE: Well, I'm sure everyone has lots to

23 contribute. Why don't we take those up on a case by
24 case basis preferably by the close of business Monday so
25 again we can get the committees working. At least we'll

0414

1 have an extra week from last time.

2 MR. PLESSER: Don't forget Art Sackler. He's

3 not here today but I know he wants to participate.

4 MR. MEDINE: We assigned everybody prior to this

5 meeting, so why don't I run through our proposed sub

6 groups.

7 If I can have the order of the committee, we are

8 proposing a slightly different organization. We think

9 that the subcommittee format last time was a useful time

10 to develop certain issues, but I think as we move to

11 options, perhaps a slightly different organization might

12 serve better.

13 So what we would propose, the same number, that

14 is four subgroups access and three security, and at

15 the suggestion I will go through the titles first and

16 then go back and go through the titles and the committee

17 members.

18 The first under access is degree of access and

19 terms and conditions of access. The second is entities

20 covered.

21 The third is ability to correct or edit data,

22 and the fourth is authentication and technology issues

23 related to access.

24 MR. PLESSER: Three was ability to correct

25 and --

0415

1 MR. MEDINE: What we would propose is in terms
2 of relating this structure to the structure of the first
3 processes is access one for this session developed a
4 very extensive list of categories of information, and
5 what we would propose is that each of these four groups
6 in its work among other things consider how those range
7 of categories or range of sensitivity of information
8 fits into the work of each of those groups.

9 That is more or less sensitive information
10 relate to the ability to correct, more or less sensitive
11 information relate to authentication. Again not to say
12 that you won't project that, but we would urge that that
13 range of responsibilities be at least addressed by each
14 of these groups.

15 So I guess should I move to our proposed
16 assignments and those people want to discuss the
17 structure?

18 MR. WHAM: Do you have a three for security?

19 MR. MEDINE: The three for security are, the
20 first are what we call internal or managerial security
21 issues. The second is external or technical security
22 issues, and the third is disclosure assurance and notice

23 of security.

24 Again would people like to discuss the sub

25 groups or should I move to assignments, proposed

0416

1 assignments?

2 MR. WHAM: On discussing the sub groups --

3 MR. MEDINE: Again identify yourself.

4 MR. WHAM: Ted Wham with Excite@Home. I think

5 even the court reporter knows who I am.

6 On the security assignments there was a lot of
7 discussion about rulemaking and hitting a certain
8 standard of procedure and appropriateness of care and so
9 forth. I don't know if that's going to be addressable
10 very well in the three groups that you've gotten.

11 MR. MEDINE: I guess: Why wouldn't it be?

12 MR. WHAM: I would look at that in terms of
13 you've got disclosure as an area, what you say about it,
14 but I think you need to have some level of do we want to
15 have a bright line rule, do we want to have minimum
16 standards, do we want to have ones that are by
17 third-party, do we want to have government oversight, do
18 we want to create an independent industry report.

19 I'm not sure if I understand where that fits
20 very well within that scribe.

21 MR. MEDINE: I guess I would propose that they
22 could fit into either -- to any of the groups but

23 particularly the first two groups, that is, for
24 instance, the second group would be external security
25 issues. Those could be addressed through standards,

0417

1 through audits, through any number of means that we're
2 discussing.

3 MR. WHAM: The very fact that it fits in
4 multiple groups seems odd.

5 MS. CRANOR: This is Lorrie Cranor. I would
6 suggest there be only one security group that covers all
7 of this, especially given last time that the three
8 security groups spent a lot of time talking to each
9 other, and they were really held to the same thing
10 essentially.

11 MR. MEDINE: Do people think that's a practical
12 way to proceed, a more efficient way to proceed than
13 last time? I'm seeing some nods.

14 MR. TORRES: This is Frank Torres. Are you
15 saying combine A, B and C into just the one so we have
16 just the security?

17 MR. MEDINE: The three security groups is the
18 proposal.

19 MS. MULLIGAN: I think it would be useful to do
20 so.

21 MR. MEDINE: Identify self --

22 MS. MULLIGAN: I but she knows who I am too.

23 I'm sitting right next to her.

24 But I think the way that you wrote this out I

25 don't think for me reflects the tone of the focus of the

0418

1 discussion. The things that seem to come out of the
2 discussion were there was a notion that came out that
3 seems to be very important of auditing and testing, so
4 how do you assure that what you're doing works, a notion
5 of how you establish what it is you should be doing
6 which is the standard of care, how do you assess
7 reasonableness, and then the question of whether or not
8 there are sufficient incentives.

9 I thought it was very telling that Mr. Geer
10 talked about you weren't sure there was a market
11 failure, but then he said that the only people who
12 really come in dying to have security are people who
13 just had a big public humiliation or people who are
14 highly regulated to me which indicates that there may be
15 a failure.

16 I'm not sure, but so when I think about
17 technical and managerial, those have to apply both to
18 internal and external. I just wouldn't break them in
19 that way, but I think one group is fine, but I would
20 prefer to have people focus on three different subjects
21 rather than these three subjects.

22 MR. MEDINE: I think that would certainly be an

23 appropriate thing for the group to do among themselves

24 is to allocate responsibility for those issues and other

25 issues, and again remember that the goal here is not a

0419

1 consensus. If anyone has a single view, that ought to
2 be presented as well, and again I will just make it
3 clear, that the subgroup's role is simply to report back
4 to the larger group for consideration.

5 These are just proposals for options to be
6 considered by the larger group at the next public
7 meeting. So it sounds like -- there seems to be a
8 consensus to have the security three groups merged into
9 one. No, we're having an objection.

10 MR. KAMP: It was another question.

11 MR. MEDINE: Yes.

12 MR. KAMP: I've resolved that and --

13 MR. MEDINE: Okay. Resolved. Does anybody have
14 any objection to merging? Again it seems as though
15 there's a consensus to merge three in effect. I think
16 that addresses some earlier question is that people had
17 overlapping expertise, and this would create a greater
18 synergy among the levels of expertise in the group, I
19 think that sounds like a reasonable proposal.

20 John? John Kamp.

21 MR. KAMP: John Kamp from the AAAA. Mine is a
22 question, and it probably reflects the fact that I work

23 inside the Beltway, but when I see options, I think what

24 options are there other than policy options, and I

25 thought it might be useful for you at least to discuss

0420

1 what you were thinking about inside that so that I could
2 get a sense of what our reports would look like.

3 MR. MEDINE: This is -- the committee has total
4 discretion to submit whatever options it thinks
5 appropriate, whether they're technical options, policy
6 options, options to do nothing, options to do lots of
7 things.

8 I mean, that's what exactly we're looking to the
9 committee to give us feedback on. Obviously we have an
10 immediate interest in understanding these issues
11 particularly in the context of the web survey that's
12 going on this month, but unless -- I'm not sure if I'm
13 answering your question, but I think that's for the
14 groups to decide, what kind of options they want to lay
15 out and which will benefit the Commission.

16 Deirdre?

17 MS. MULLIGAN: Deirdre Mulligan. I have one
18 more. On the access of sub groups, I don't feel like --
19 and other people of course disagree vehemently if you
20 need to, but the entities subgroup, I feel like we kind
21 of went through that issue very quickly during the
22 general meeting, and I don't know that it would warrant

23 a full separate sub group.

24 It seemed to be pretty tightly intertwined into

25 other discussions, and I'm wondering if other people

0421

1 feel like there needs to be a separate sub topic on the
2 topic of entities.

3 I think as Lorrie talked about earlier if you're
4 talking about sharing data, absolutely, but when you're
5 talking about access and security I'm not so sure.

6 MR. KAMP: And John Kamp. Just to sort of
7 respond to that, the way I understand then which I may
8 be again incorrect is that it's the third-party transfer
9 problem. It's the multiple entities that might be
10 involved, and given that I don't think I have Deirdre's
11 problem, but the way Deirdre expresses it I may agree
12 with her.

13 MR. WHAM: What is it that you have a problem
14 with?

15 MR. MEDINE: Being from inside the Beltway
16 comment.

17 MR. WHAM: If you want like me to come closer
18 to tease you personally I'll be more than happy to do
19 it.

20 MR. JAYE: Don't take this as a volunteer for
21 the entities sub subcommittee, but I do think that there
22 are a few issues there that we didn't talk about today

23 that probably should be addressed here.

24 One is onward transfer and where this data

25 control is inside. We about editing at the source,

0422

1 editing at the target. One issue we didn't talk about
2 today though specifically was actually the issue of
3 jurisdiction, and I know that it comes into a scope
4 issue, but obviously that can be interpreted as sort of
5 from a federal perspective.

6 But also there's the concern of what about
7 onward transfer to a jurisdiction where the FTC might
8 not have direct recourse under Fair Trade Practices, so
9 it's kind of the inverse of the what the EU has been
10 doing, but I think there are a couple issues like
11 that -- they may only take one minute to address, but
12 there's probably a couple things there that we need to
13 at least check mark.

14 MR. MEDINE: Okay. Okay.

15 MR. PLESSER: Maybe if you put entities and
16 sectors in the second one so that we were -- had some of
17 the sensitive sector kind of, Do we deal with everything
18 one way or separate sectors in terms of access,
19 obviously some overlap, but I think that would then give
20 much more meat to the second committee and then
21 splitting it.

22 MR. MEDINE: We can take comment on that. Even

23 if we did that, I would urge the other groups to still

24 consider the sensitivity and the range of issues that

25 access one has laid out, but I don't know if that helps

0423

1 people, but I think certainly the conception about the
2 entities relates to onward transfer sharing, joint
3 efforts, joint ventures, joint marketing, all the
4 various business relationships that data can be subject
5 to.

6 MR. GAVIS: As a members of the entity group, I
7 think Deborah and I are the only two people here. We
8 had a hard time getting our arms around this, and I kind
9 of second the thought that maybe we want to roll it into
10 maybe even number three, the ability to correct, ability
11 to reach inside the organization and correct from
12 whatever entity it's shared with.

13 MR. MEDINE: I'm seeing some nods. Are people
14 amenable to merging the entities in the corrections
15 group? You don't have to identify yourself.

16 MR. WHAM: Actually I have a concern here that
17 this is a relatively large issue that we didn't spend
18 any time talking on, but there's a lot there. If it
19 isn't for access, it isn't for security per se but it is
20 for transfer data to third parties whether that's --
21 explicitly out there whether it's EBay or whatever it
22 is.

23 If that's within the mandate of this group, then

24 I for one would participate on a committee like that

25 because I think there's all sorts of detailed

0424

1 information. Do we have a right to transfer it to a
2 joint venture partner? Do we have a right to transfer
3 to a wholly owned subsidiary? What if we owned 49
4 percent of that subsidiary?

5 I think that there are questions -- what if it's
6 a marketing partner? We're doing something with Proctor
7 and Gamble.

8 MR. GAVIS: This is Alex from Fidelity. I would
9 jump in and say I'm not so sure we want to focus on
10 whether we have rights to transfer from one to the
11 other. The issue is whether the information that gets
12 sent along can be accessed by a consumer or customer.

13 MR. MEDINE: I think that's consistent with the
14 scope of this group, is assuming information is legally
15 transferred, what are the access consequences in the
16 context of how that information is being transferred?

17 Lance?

18 MR. LANCE HOFFMAN: Lance Hoffman. I think
19 we're rapidly nose-diving, and I don't want to do that.
20 I don't want to fly at 500 feet when I think in order to
21 plan for next time we have to stay up at least at 20 or
22 30,000 feet.

23 I think Deirdre was on the right track when she
24 said, Look, I think what I've been hearing and the
25 discussion of the committee as a whole day was she said,

0425

1 they could be different, I had them as standard of care,

2 audit and incentives, but they could be other things.

3 The point is whatever the subcommittees end up

4 being I would like as a committee member to get not

5 direction but a couple bullets, several bullets from the

6 FTC saying, We think what we heard were these, you might

7 want to consider these to focus your discussion, maybe

8 taking Deirdre's as a starting point.

9 That way as a process point down the road we can

10 roll some of these things into that and we won't have

11 things all over the map.

12 MR. MEDINE: We're willing to do that, but again

13 I really and truly don't want to constrain your groups'

14 discussion and the scope of the issues that the groups

15 raise.

16 MR. LANCE HOFFMAN: One of the --

17 MS. PIERCE: This is Deborah Pierce from EFF. I

18 just wanted to echo what Alex said. When we were going

19 through our outline, we found ourselves really

20 discussing a lot of scope issues, a lot of ability to

21 correct and edit, and I agree with him. I think that an

22 appropriate place to roll this into would be the third

23 category or even the first category.

24 MR. MEDINE: Okay.

25 MR. GAVIS: Alex Gavis from Fidelity. One thing

0426

1 that I think maybe that I'm hearing is that if we're
2 going to be an effective advisory to the FTC, I think
3 maybe we need more guidance from you as to whether you
4 want us to focus on policy or you want-- whether you
5 want us to focus on sort of our expertise in industries,
6 and to some extent you may have some ideas and you would
7 like to sort of hear what our expertise and various
8 industries so it comes to bear on these subjects as
9 opposed to what from a policy standpoint we might do.

10 Or on the flip side you might not care as much
11 about that but really want us to think from a policy
12 perspective, what would we do if we were a policy maker,
13 and I think that's sort of the tension that's going on
14 here.

15 MR. MEDINE: In some ways we're looking for the
16 intersection of the two because we are looking for your
17 expertise in translating what's going on into
18 operational or implementations approaches to access and
19 security, and again the very specific goal is as we
20 survey web sites right now and discover certain
21 practices on those web sites with regard to access and
22 security, are those consistent with Fair Information

23 Practices?

24 So it's a little bit of both. I don't think

25 it's a pure policy, and I don't think it's pure

0427

1 technical, and I think from the security discussions,
2 certainly we learn that there are some array of
3 technical issues that may force the policy in certain
4 directions.

5 MR. BAKER: Actually I think we know pretty much
6 what the options are on the security side. It's
7 harder on the other side. I was going to ask a similar
8 question about where this is -- what we should be
9 putting together.

10 We could write the options in about like a 20
11 minute phone call is my guess; writing the pros and
12 cons is a more substantial effort, and I'm assuming you
13 want that, but I wasn't sure.

14 MR. MEDINE: No, I think that's a good question
15 and the answer is yes. I mean, what ultimately will
16 benefit the Commission is not so much six different
17 positions as understanding why those six different
18 positions advance Fair Information Practices and
19 considering the costs and benefits of those various
20 approaches.

21 So I think certainly identifying the options is
22 obviously the starting point, but then beginning to

23 flesh those out with pros and cons is exactly what we're

24 looking for.

25 MR. BAKER: One related point to that. Stewart

0428

1 Baker again. What should we assume is going to happen
2 with the stuff we've been outlining? Obviously it would
3 require a lot of work to be useful. Is that going to --
4 are we envisioning that that will be a report, and the
5 options will come at the end? Should we just figure
6 we'll do the options and it was a learning experience to
7 produce the outlines? What do you think our final
8 product is here?

9 MR. MEDINE: Again that's going to be up to the
10 committee. I guess we viewed the exercise of creating
11 the outline largely to inform the discussion about where
12 to head on options, so I think the body of the report
13 ought to be mostly options rather than spending time
14 writing a treatise on the array of infinite
15 possibilities here.

16 We want to have a relatively practical guide for
17 the Commission on where do we go from here on these two
18 very important issues.

19 Richard?

20 MR. PURCELL: Richard Purcell. As a note of
21 encouragement to whatever subgroup each one of us ends
22 up on, I would like to encourage all of us to be

23 continually thoughtful about this glossary that I think
24 is going to be very important to our work here and for
25 each of the sub groups to try their best to maintain and

0429

1 to create some level of consensus around definitions for
2 some of these important terms that we're using and that
3 perhaps we might be understanding but perhaps need to be
4 brought forward in our final report in order to further
5 the understanding beyond the committee itself or the
6 Federal Trade Commission and out into the marketplace
7 itself.

8 MR. MEDINE: I think that will be a very useful
9 part of the report.

10 Deirdre?

11 MS. MULLIGAN: Deirdre Mulligan. As the holder
12 of the categories document, I will actually update it to
13 reflect the discussion and recirculate it. I mean,
14 there was a desire to have of transactional data. There
15 were two or three other things, and I did take detailed
16 note, and I will update it and circulate it because I
17 completely agree with Richard's point that a common
18 taxonomy is really important for anything, so I will
19 circulate this early next week.

20 MR. MEDINE: Great.

21 MR. LANE: You have the sweeps going on on
22 access and security starting, probably they've already

23 started or are starting very soon. Yet we in this room
24 haven't come up with an idea of what exactly is proper
25 access and proper security, so how are you running the

0430

1 sweeps on an issue that we haven't been able to resolve
2 here? So do you already have what the options are and
3 what the best practices should be?

4 MR. MEDINE: Well, the question has arisen
5 before. What we're trying to do in the sweeps is to
6 gather as much information as we can about what web
7 sites are doing in fact today and then have the work of
8 this group inform the Commission as to whether what is
9 going on today constitutes sufficient self regulation
10 and meets what are considered Fair Information
11 Practices.

12 So that's our challenge is to get enough
13 information to give this group flexibility in making
14 recommendations that we can then assess against
15 essentially a snapshot of the world that we find today.

16 MR. LANE: If we had found on the security
17 discussion which was processed and all you're looking
18 at -- and I'm not sure how you're getting at the
19 process, I mean, I don't know if you're calling the CEOs
20 of the different companies and saying, Please detail us
21 your security process and how many people you have --
22 there's some comments about numbers and audits and

23 things of that nature.

24 Is that what the sweeps are doing, or are they

25 just looking at the web site?

0431

1 MR. MEDINE: They're looking at the web site.

2 And maybe that's an advertisement for our last

3 discussion which is there's a question that I think this

4 group can be very helpful on to the Commission, and that

5 is do you have to disclose or should disclose your

6 security policies, practices? Should you just have good

7 security?

8 I think informing us on that issue would be

9 extremely helpful, and then we can read the results of

10 the survey in light of what was discussed here.

11 MR. LANE: Maybe it will help us in formulating

12 our ideas on the security side. What are you looking at

13 for security -- what are you judging and basing your

14 security sweep on?

15 MR. MEDINE: Well, we're primarily looking at

16 what sites are saying about their security practices,

17 and certainly to the extent that sites use SSL as part

18 of it as well, but we're looking for this group's

19 guidance as to whether security is something you talk

20 about, is security something you have, if you talk about

21 it to what degree do you talk about it?

22 We are primarily capturing what sites are saying

23 at least on that principal limited element of SSL doing

24 in this area.

25 MR. LANE: So you could actually have a very

0432

1 secure site that doesn't talk about it, but it could be
2 interpreted just by raw numbers that you actually have a
3 secure that or a site that is not telling you about the
4 security, and that -- my concern is that that could be
5 interpreted as an unsecure site even though it may be
6 the best security of all the sites, even the ones that
7 are disclosing.

8 MR. MEDINE: That's where this committee can be
9 very helpful to the Commission in evaluating that
10 information for its release to assess the issue again of
11 whether people should be told about security. Part of
12 the issue of security is do consumers have confidence
13 that their information will be kept securely, and part
14 of the consumer's concerns is will their information in
15 fact be kept securely.

16 So this group's advice and final report will be
17 helpful in evaluating how the Commission should approach
18 the data that emerges on that issue.

19 MR. CATE: I'm sorry, could you tell us whether
20 Stewart Baker will be a catering his group and if so
21 which group he'll be on?

22 MR. MEDINE: That would give his group an unfair

23 advantage. Stewart?

24 MR. BAKER: This is Stewart Baker. A couple

25 thoughts on this survey. I certainly agree with Rick,

0433

1 the fact that you have no security statement at all
2 might not mean you know anything about your security so
3 to the extent you're doing this sweep, there shouldn't
4 be an implication as there might be on the privacy side
5 about the lack of a statement is a fall.

6 But if you're going to do it, some things that
7 might be useful to know is whether, one, is there a
8 security section; second, does it mention particular
9 technologies, SSL's commonly mentioned; does it mention
10 particular security standards to which it is -- that is
11 adheres to; does it mention an audit or an auditing firm
12 that may have checked their security standards; and how
13 long is it?

14 Those are all useful pieces of data. I don't
15 think it tells you whether there's good security or bad,
16 but it will it us to figure out does it really matter to
17 have a statement like that.

18 MR. MEDINE: Let me just say that those are
19 obviously the kinds of options that will -- as you
20 predicted would take a short period of time to start
21 spilling out the options, but those are the kinds of
22 options that would be helpful for the Commission to have

23 along with pros and cons to evaluate what it's learning

24 in the survey.

25 This will be useful generally but its most

0434

1 direct and immediate application will be survey

2 interpretation. Jonathan?

3 MR. JONATHAN SMITH: This is Jonathan Smith.

4 Why don't you just do something pragmatic? Why don't

5 you just do short scans, go and check their --

6 MR. BAKER: Buy a war dialer?

7 MR. JONATHAN SMITH: Go for that.

8 MR. MEDINE: Okay.

9 MR. RICHARD SMITH: I think I can answer that.

10 MR. MEDINE: Richard Smith.

11 MR. RICHARD SMITH: I was just -- Richard

12 Smith. I was just involved in a project for doing a web

13 sweep for E Health Sites, and we faced the same problem,

14 what do you do about security and pretty much just let

15 it -- take a peak at the privacy policy and what we

16 talked about.

17 So we made no judgment calls about security, and

18 what I kept telling -- when we got started on this, I

19 don't want to do things like short scans because I don't

20 want to go to jail. If you start testing external

21 security that gets into a real fuzzy legal area, so I

22 don't recommend that.

23 MR. PLESSER: Point of personal --

24 MR. RICHARD SMITH: Overall what was interesting

25 is we were still able to find security problems. Like

0435

1 we found a complete database log in information in HTMO

2 comment so it is possible to find security problems

3 without that, but over all --

4 MR. MEDINE: Ted?

5 MR. WHAM: That's not good, is it?

6 MR. RICHARD SMITH: I don't think so, and were

7 taken off two days after our report back out and still

8 not back online again.

9 MR. MEDINE: Ron?

10 MR. PLESSER: I thought we were about to get our

11 assignments, and we went down this road so if we could

12 focus back on the assignments.

13 MR. MEDINE: If that's a motion to --

14 MR. PLESSER: I blame the Chamber completely.

15 MR. MEDINE: I take that as a motion --

16 MR. LANE: We'll bring our coffee the next time.

17 MR. MEDINE: Hearing no objection we will

18 proceed.

19 Starting with new access one which is degree of

20 access and terms and conditions of access, we propose

21 Alex Gavis, Deborah Pierce, Steve Cole, James Allen,

22 James Maxson, Jane Swift, Art Sackler and Richard

23 Purcell.

24 For the new combined entities and sectors as

25 well as ability to correct or edit the data all combined

0436

1 into one we propose Richard Bates, David Ellington,
2 Tatiana Gau, Frank Torres, Fred Cate, Dan Jaye, John
3 Kamp, Deirdre Mulligan, Dan Schutzer, Josh Isay, Ron
4 Plessner, Rick Lane, Rob Goldman and Jim Tierney.

5 For the access three, the new access three
6 authentication and technology issues related to access,
7 Robert Henderson, Richard Smith, Andrew Shen, Ted Wham,
8 Jerry Cerasale and David Hoffman, and the security group
9 which everybody has left, but I'll read it any way
10 because there is some duplication of people, Deirdre
11 Mulligan, Rebecca Whitener, Larry Ponemon, Dan Geer,
12 Lance Hoffman, Andrew Shen, Tom Wadlow, Greg Miller,
13 Jonathan Smith, Stewart Baker, Steve Casey, Mary Culnan,
14 Stewart Baker, Lorrie Cranor, Paula Bruening and Dan
15 Schutzer.

16 Let me again just reiterate that while this is a
17 large group, its task is only to develop a set of
18 options to report back to the full committee. Because
19 of the public nature of the advisory committee meetings
20 no decisions will be made at the subgroup level, but the
21 subgroup obviously can be very valuable in developing a
22 series of option for the full group to consider.

23 Why don't you all --

24 MS. GAU: Tatiana Gau, when you post this on

25 the site as I imagine you will could you be sure to

0437

1 include a definition as what you see as the objective of
2 the individual sub groups?

3 MR. MEDINE: We will do our best to do that,
4 yes. If people don't have further discussion on this
5 issue, perhaps we could move very briefly to the last
6 issue which relates to disclosure. Andrew?

7 MR. SHEN: Andrew Shen. Just a really quick
8 question. Last time around the authentication group had
9 sort of control over the definition glossary or glossary
10 of terms.

11 Is that going to continue or is that going to be
12 thrown to a new group?

13 MR. MEDINE: It's up to the group. Dan?

14 MR. SCHUTZER: I think the spirit of what was
15 said starting with the glossary, and as we all proceed,
16 we can review that and find any additions to this
17 growing glossary, I would recommend we do it that way.

18 MR. PURCELL: I agree. I wouldn't characterize
19 our effort as controlled, as rather volunteer effort to
20 just start something up.

21 MR. MEDINE: Dan?

22 MR. JAYE: What is the mechanism for providing

23 feedback on the glossary? I'm not sure this is the

24 right forum to do that. Is that just E mail to the --

25 to that subcommittee, the authentication subcommittee in

0438

1 its new form?

2 MR. MEDINE: I'll leave -- why don't we have the

3 group decide that.

4 MR. JAYE: For people in another group though?

5 MR. WHAM: Why don't we give our --

6 MS. MULLIGAN: Richard, don't you have the

7 master of that?

8 MR. PURCELL: Yes, I do, but it's also posted on

9 the web site.

10 MS. MULLIGAN: Can you edit it?

11 MR. PURCELL: I can certainly edit it.

12 MS. MULLIGAN: I was forcing him voluntarily.

13 MR. PURCELL: Keeping clearly in mind that

14 editing invokes a certain level of control, don't hold

15 me too tightly on that, and if you have any dispute over

16 the editing or that control, please be vocal about that

17 as I know that you probably will.

18 MR. MEDINE: And as the transparency that we

19 have of posting things and having the next meeting as an

20 opportunity to discuss these raise issues.

21 MR. ALLEN: James Allen. I thank Richard for

22 volunteering to do this, but I think it would be very

23 useful if it could be published periodically over the
24 next three or four weeks so that we can see that, and I
25 would hope that the FTC would help Richard in doing

0439

1 that.

2 MR. MEDINE: Certainly. We'll be happy to
3 either distribute to the group or post on the web site
4 anything you like.

5 MR. PURCELL: Tell you what we'll do. This is
6 Richard Purcell. I will do my best on Fridays to post
7 an update to the designated federal officer, and I will
8 leave that officer the accountability for having it
9 available on the web site for the general group's
10 access.

11 MR. MEDINE: I accept that responsibility.

12 MR. WHAM: Might there be an alternative for
13 that actually to be posted on a Microsoft site updated
14 as you've got the availability to provide a link off the
15 ACOAS site?

16 MR. MEDINE: Well, I think it's probably more
17 appropriate to be on the advisory committee site, and
18 you can feel free to link to it from anyplace that you
19 would like. I think it's more appropriate to be on our
20 site.

21 Any other procedural issues before -- if people
22 can stick around a few minutes for those who can, I

23 would like just briefly discuss the issue that was just

24 raised a moment ago which is people's views about

25 security, which is do you have to talk about the

0440

1 security you have, or is it enough to have security in

2 the context of Fair Information Practices?

3 Again that will be as I said before very helpful

4 and informative for the Commission to evaluate the results

5 of our survey matter. Mary? Why don't we just discuss

6 this for 10 or 15 minutes because I know people look

7 boiling.

8 MS. CULNAN: One thing I took away from the last

9 discussion is that perhaps disclosures about security

10 itself were pretty meaningless, but people want an

11 assurance that's useful and quick to pick up and

12 understand that this is a safe place to do business in

13 across from the medium, et cetera, so I would say that

14 should be the goal of disclosure is to build trust in

15 the medium and to focus on what's the best way to do it?

16 Is it through a third-party assurance? Is it

17 through some kind of statement? Those would clearly be

18 options for disclosure.

19 MR. MEDINE: Lance?

20 MR. LANCE HOFFMAN: There's this ongoing issue

21 in the security community about full disclosures versus

22 security by obscurity, okay? And it's not going to get

23 solved by this committee either. I think Mary's on the

24 right track when she says people want assurance.

25 I would harken back and make a minor

0441

1 modification to what I said earlier, and I'll make it
2 brief in terms of putting out there we're doing
3 something or we're doing this on the security, and I'm
4 taken on your comments about the small initial -- what's
5 the barrier for a small firm starting up and all that.

6 In essence again very quickly, an ingredient
7 label kind of thing where it says, Here's what we're
8 doing on security, we're devoting X amount of our
9 resources, our revenues or whatever it could be zero.
10 It could be zero. You could hire it out, contract it
11 out for something, you are taking care of the audit.

12 We have hired so and so, Pricewaterhouse or
13 whomever to do our -- whoever, to do our audit and
14 here's the -- as I was just talking to Stewart in the
15 hallway conversations, here's the standards they're
16 using whatever they are, could be -- whatever they are,
17 and then finally if you will the liability notice or
18 recourse notice, something like that.

19 Bang, bang, bang, bang that's it, nothing else,
20 that let's people know without burying them -- once you
21 say SSL 95 percent of the world tunes out, you know?

22 MR. MEDINE: John?

23 MR. KAMP: Not to respond to that, but John Kamp
24 from the AAAA, and perhaps at the risk of picking up on
25 what might be a sensitive issue, I do think that this

0442

1 discussion about what security is and the notification
2 of security might underline an issue that some of us in
3 the business community have said for some time, and that
4 is the FTC web sweeps might be better off done after the
5 report from this committee comes in.

6 And I would ask the Commissioners and the
7 Commission staff to review the record of this to hear
8 some of the conversation we just missed, that just went
9 on.

10 MR. MEDINE: Thanks.

11 MR. PONEMON: May I comment on audit? I think
12 when we say audit --

13 MR. MEDINE: Can you identify yourself?

14 MR. PONEMON: Larry Ponemon, Pricewaterhouse
15 Coopers. It's a long name, I'm sorry.

16 But when we think about auditing, there are
17 different types of audits or different types of
18 assurance services. For example one could argue that
19 TRUSTe and BBB online provide a form of assurance, so I
20 think that when we look at the options each one carries
21 a certain degree of comfort and security to the reader
22 of the disclosure but also carries a cost and so we need

23 to factor that into the equation as well, so....

24 MR. MEDINE: Again keep in mind as you formulate

25 options as to what the disclosure -- there are two

0443

1 issues, one is what should you be adopting and the other
2 is what should you be telling consumers about what you
3 adopted?

4 Why don't we just go down the line with Frank
5 and then Jim and then Jonathan Richard?

6 MR. TORRES: My comment is simply disclosure of
7 the site's security sense is a good idea to establish some
8 consumer confidence and I think it can simply be the
9 truth about what a site feels about its security.

10 Certainly what I've gotten out of some of this
11 discussion is any site that fully guarantees to the
12 consumer that it's 100 percent secure and under no
13 circumstances will your information ever be broached is
14 just an out and out lie.

15 But a site that says, Listen, we'll protect your
16 information to the best of our ability and should in the
17 unforeseen circumstance happen, here's what we'll do to
18 protect your information, and I think to the extent that
19 those disclosures are truthful, simple, plain English,
20 it actually provides a good feeling sense for consumers
21 and could be very useful in that sense.

22 MR. MEDINE: Jim.

23 MR. TIERNEY: Jim Tierney, I had vowed to try to
24 keep quiet, but John invited the Commissioners to review
25 the transcript about the feeling that this group might

0444

1 have about the timing of these particular sweeps, and at
2 least as one member of this Commission, I'm delighted
3 that the Commission is doing the sweeps, not only that
4 they're doing it but when they're doing it and that this
5 information will be made available to us and that there
6 are indeed difficulties and problems or defects in the
7 Commission's methodology, that we'll still be sitting as
8 a committee and be able to remedy and point to the
9 public there are defects that the FTC has proceeded but
10 I'm delighted it's being done.

11 MR. KAMP: Let me respond to that. John Kamp.
12 I'm not sure, Jim, if what you said is correct that this
13 committee will have an opportunity to fully review the
14 results of the study before this committee submits its
15 report. That might change my attitude about this a lot,
16 but I don't have any sense that this committee will be
17 able to have any data available to it before this report
18 comes in.

19 MR. MEDINE: I think that in fact the current
20 thinking is that the Commission would consider the work
21 of the committee in evaluating the results, but that the
22 results would not be circulated to the committee for

23 review prior to their public release, and I think we

24 know how quickly things make the right public.

25 And so I think to give the Commission sort of a

0445

1 full opportunity to consider both and have a full
2 opportunity for reflection, they will both be issued
3 together in a Commission report, but of course that's
4 not to say that the Commission in considering the
5 results may learn some things from this committee's work
6 that may cause it to reevaluate both the survey, its
7 methodology and what it wants to report in this area.

8 That is the benefit of linking the two is the
9 Commission has the opportunity to consider the points
10 that you're making in deciding how it wants to proceed
11 with regard to a public release of anything at this
12 stage.

13 MR. LANE: But I thought originally you said we
14 would have access to this information to help us base
15 our decision --

16 MS. GAU: Quite the contrary no, no, no.

17 MS. CRANOR: This is Lorrie Cranor. So I
18 understand that we wouldn't have access to the results
19 because they could be leaked, but could we have access
20 to the methodology?

21 MR. MEDINE: Let me raise that internally, and
22 I understand the question and I will get back to you on

23 that. That's a fair question. I can't decide that for

24 the Commission, but I'll get back to you about that.

25 We were working our way down this line. Richard

0446

1 and Andrew?

2 MR. RICHARD SMITH: Richard Smith real quick

3 here. I just wanted to shift gears back to this issue

4 of security disclosures, and I think we'll keep it

5 simple is the real key word because most people don't

6 really care.

7 The one thing I would say is it's okay to

8 probably brag about your SSL capabilities because

9 sometimes people do understand that, but that's about

10 the limit of jargon they would get into.

11 Another quick point that I would make is I'm not

12 in the ECommerce business myself, but I suspect there's

13 been some discussion about not hurting small companies

14 by undue security burdens but I believe a lot of

15 companies, small, medium and large actually use hosting

16 services themselves for doing this stuff.

17 And those are the folks who are providing the

18 security, and that has pluses and minuses, the plus

19 being that they may have the critical mass to provide

20 the security that a large company could even for the

21 smallest group.

22 On the other hand you have to have then access

23 to your databases by the company that's off site, and

24 that opens security holes on its own, so it's a more

25 complicated situation in security once you get more

0447

1 companies mixed into the stew here if you will.

2 MR. MEDINE: Thanks. Andrew?

3 MR. SHEN: Andrew Shen. I just want to sort of
4 emphasize something that Frank brought up before. Maybe
5 the most important thing about security in terms of
6 notice is what sort of security you're providing under
7 ideal conditions, but sort of what happens when security
8 breaks down. That's one of the topics we brought up in
9 the security three group because I think that's
10 something very important and I think it goes back to
11 comments that people brought up earlier about market
12 influences, whether there's perfect marketing conditions
13 whether a security breakdown does lead to some
14 tarnishing of reputation.

15 I think clearly in past security breakdown
16 incidents that has not occurred, particularly the CD
17 Universe case. The break in and CD Universe negotiating
18 with this guy who was holding all the credit card
19 numbers for hostage. None of that was made public to
20 the customers for a couple of months. Now I think you
21 see that same sort of incident repeat itself. Northwest
22 Airlines had a similar incident, Outpost.com.

23 So I think you clearly can see at least in terms

24 of notice one way you can provide some sort of

25 assurances in terms of dispute resolution.

0448

1 MR. MEDINE: Richard seems anxious to weigh in on
2 this.

3 MR. RICHARD SMITH: I am. Richard Smith. A
4 real quick comment about CD Universe. I think it's a
5 little bit premature to judge on that case because it's
6 entirely possible that they didn't go public because
7 they had the FBI involved from day one, and I ended up
8 chatting with a guy, the Maxis guy via E mail, and he
9 just got anxious, and we don't know how it was going but
10 the way it looked to me get they were trying to get this
11 guy to come to the U.S. and then bust him, so they
12 probably handled it okay.

13 MR. MEDINE: Deirdre?

14 MS. MULLIGAN: I think most people or many of
15 people in this room are in the business of manipulating
16 data. I know it's quite possible to collect data and
17 analyze it later on, and I think that the only tension
18 between the Commission doing their sweep now and the
19 Commission doing their sweep later is whether or not we
20 would think that you're collecting the wrong data and
21 whether or not we could change your mind.

22 And my sense is that you are going to collect

23 notices regardless of what we think, so I don't know

24 that if we came up and said notice means nothing in the

25 security context, which I'm of the general mind to

0449

1 believe, that it might mean something for your
2 enforcement powers, but I don't think that it means a
3 whole lot as to whether or not the security's good.

4 So I might suggest that you do something that's
5 much more like Richard Smith did in trying to assess
6 security standards on the web, but I don't have the
7 sense that the Commission would be interested in
8 pursuing such a recommendation so therefore I don't see
9 that there's a harm in you collecting the data now and
10 then using whatever recommendations we come up with to
11 analyze it.

12 However, I do want to ask a question about the
13 survey. My understanding I think is that you're only
14 looking at a hundred sites? How many?

15 MR. MEDINE: No.

16 MS. MULLIGAN: That's what I want to know.

17 MR. MEDINE: Well, we are looking at two
18 samples. We are looking at the top 100 sites as has
19 been done in the past two years by Professor Culnan in
20 and by us in '98, and we are looking at a sample of an
21 universe of the busiest sites, and I quite honestly
22 don't have a precise number to give you because that's a

23 number that -- it's a random sample but then sites get

24 kicked in and out.

25 So I don't want to give you a precise number but

0450

1 it's a random sample of the busiest sites similar to
2 what Professor Culnan did last year, but as we said in
3 our public statement we're using a different essentially
4 rating service to develop the list but I would say the
5 methodology is in a very rough way similar to what was
6 done last year.

7 MS. CULNAN: Which was similar to what was done
8 the first time, just more? None of these are
9 reinventing the wheel because otherwise you end up with
10 something that you can't make any comparison to.

11 MR. MEDINE: That's right. The biggest
12 difference between '98 and '99 just to clarify is in '98
13 we surveyed the entire body of U.S. commercial web
14 sites. In '99 --

15 MR. WHAM: Can't do that anymore.

16 MR. MEDINE: Well, you can't survey it and
17 sample it, but instead we -- Professor Culnan surveyed a
18 weighted sample of the busiest sites, and that's a
19 methodology we are following for this year as well.

20 MS. CULNAN: So the one thing that will be able
21 to be done legitimately is to this year compare between
22 last year's survey and this year's survey because you're

23 looking at the same populations pretty much?

24 MS. MULLIGAN: Except --

25 MR. MEDINE: Roughly. I don't want to be

0451

1 absolutely -- it's much closer than between '98 and '99.

2 MS. MULLIGAN: I just want to voice that last
3 year survey done by Mary Culnan at Georgetown was only
4 at the busiest sites, and the top 100 was not done by
5 Mary and for several very important reasons from at
6 least the consumer and the privacy community.

7 MR. MEDINE: The FTC in '98 did the top 100
8 sites so we are again --

9 MS. MULLIGAN: I know, but the top 100 and the
10 entire universe.

11 MR. MEDINE: Right. This year we're doing the
12 top 100 and busiest sites, which accounts for I believe
13 on the order of 99 percent of unduplicated reach.

14 MS. MULLIGAN: I'm just flagging it.

15 MR. MEDINE: No, no, no. Those are fair. We
16 will be very transparent about our methodology as we
17 were in '98, and people will be free to comment on it.

18 MR. LANE: Rick Lane, U.S. Chamber of Commerce.
19 The CD Universe comments, can we get that stricken from
20 the record because a lot of it's hearsay about not
21 having the information out and the reasons why? Can we
22 just kind of get that all taken out because it is a

23 public record?

24 MS. MULLIGAN: It's a public record?

25 MR. SHEN: May I respond? I don't think --

0452

1 Andrew Shen, sorry. I don't think it qualifies as
2 hearsay anymore. I think it's established since it was
3 reported in the press and a lot of people know about it.

4 MR. LANE: But the reasons why. We heard two
5 different opinions of why something occurred, and that's
6 the problem.

7 MS. MULLIGAN: They were stated.

8 MR. SHEN: Like you say its CEO shouldn't have
9 told investors?

10 MR. MEDINE: Why don't we take that request
11 under advisement as we review the transcript.

12 Dan?

13 MR. JAYE: On the issue of security under the
14 review I think one of the key questions is how will the
15 results be applied or interpreted or used. In other
16 words, as you look at the security Fair Information
17 Practices? As you look at disclosure, for what purpose
18 will the information from the survey be used? How will
19 it be interpreted because if you're interpreting is
20 there adequate security, then obviously it's going to
21 drive it versus are you trying to do a survey to see
22 whether policy practices are effective at addressing

23 consumer competence in which case there have been very

24 good discussions about the fact that saying something

25 might be not necessarily meaningful and not as useful as

0453

1 doing something even if you didn't tell the consumer.

2 MR. MEDINE: Well, that is the exact subject of

3 the what we're -- merits of this current discussion of

4 that trade-off, and that is what we'll inform the

5 Commission in evaluating results, so I guess it would be

6 helpful to hear again people's views on whether

7 essentially you should have good security and whether

8 you should be disclosing something about security to

9 consumers.

10 Obviously we're looking at just at what the site

11 says and possibly does with regard to SSL.

12 MR. JAYE: My question comes back to: To what

13 use will the results be put because that would inform

14 what data we need to collect and how it should be

15 interpreted?

16 MR. MEDINE: Okay. The results will inform the

17 Commission's observing of web site practices with regard

18 to security. That is on the face of the web site not

19 going behind and pinging the web site or contacting web

20 site officials. It will be simply essentially what is

21 the consumer's experience in dealing with the web site

22 on the issue of security.

23 MR. JAYE: So from a consumer's experience
24 standpoint and competent standpoint versus is there
25 sufficient security for data protection.

0454

1 MR. MEDINE: That's right. That's the direct as
2 applied to the survey results of course the committee
3 can be very helpful in educating the Commission and
4 ultimately the public about whether Fair Information
5 Practices call for having certain security measures as
6 we've discussed throughout the afternoon as well as what
7 the web site might disclose to consumers.

8 MR. JAYE: So the key point I wanted to get to
9 is to the extent that the results are interpreted for
10 example as a basis for -- are interpreted, that's going
11 to be very important that, for example, if the
12 methodology is to look at, Is there sufficient security
13 disclosure, that we want to be very careful that that's
14 not necessarily a statement on whether there is
15 sufficient security and that no conclusions be let to
16 based on that once again as they sometimes are.

17 MR. MEDINE: That's certainly a fair comment.
18 Rob's been waiting a while.

19 MR. GOLDMAN: Rob Goldman, a couple small points
20 on this. Appreciate the comment on small businesses
21 outsourcing security to out posting groups and web hosting
22 groups and also the point on, it seems like a curious

23 thing to look at certainly whether sites say they have
24 security versus whether they deliver it. Certainly it's
25 more relevant -- it would seem to be it would be more

0455

1 relevant as to whether or not there's actually security,

2 whether or not the site claims there is.

3 MR. MEDINE: Could I ask, how does the consumer

4 know? How would a consumer know?

5 MR. WADLOW: That is the point.

6 MS. MULLIGAN: That's true on privacy also. I

7 would like to highlight the fact.

8 MR. GOLDMAN: Absolutely. Two small points, I

9 sympathize. It's a hard thing to measure certainly from

10 the outside and than often from the inside as well. I

11 can certainly say we've had issues -- and it may be an

12 issue for an entity's group within the security

13 subcommittee, but issues with out posting groups and

14 who's owning particulars of pieces of software, who's

15 managing switches, who's managing routers, where are

16 there holes and where aren't there holes, and how are

17 those holes measured.

18 Certainly it would be a much more accurate

19 measurement to have any of the security experts in the

20 room take a look at the site even from the outside, much

21 better from the inside to actually measure whether or

22 not security is there than to read what is or isn't

23 written on a statement.

24 MR. MEDINE: All right. Stewart? Okay.

25 MR. BAKER: I'm not sure this is an initial

0456

1 committee proposal but it seems to me there's an awful
2 lot of sort of the unhappiness about the idea of doing
3 this because of the security disclosures, but as you say
4 or as Deirdre says you can do what you want.

5 My thought would be that to suggest that Rick
6 and Deirdre and I just try to write a short letter
7 disassociating the members of the committee who want to
8 sign it from that, saying there a lot of risks in this,
9 this is only one of the options that you might consider
10 in security, and one as to there a lot of doubts and you
11 shouldn't view this as a test of whether there's good
12 security, circulate it around and see if people want to
13 sign it.

14 I don't know of anyone that wants to participate
15 in that, but I think it might be useful to send the
16 Commission something that says, There's a problem here
17 and you ought to recognize it.

18 MS. MULLIGAN: Since my name was invoked can I
19 rejoin? Deirdre Mulligan. I would actually like to say
20 I think that would be a good idea except the fact is it
21 extends to privacy also, and that one of the
22 difficulties in assessing privacy is that it's very nice

23 if a web site says we do X, Y and Z.

24 We don't transfer your data, we do transfer your

25 data, as a consumer it's very hard for me to assess

0457

1 whether or not that's happening, and with the FTC
2 without poking around very difficult to assess, the same
3 with security.

4 MR. BAKER: I'm looking for whether everyone
5 agrees with.

6 MR. MEDINE: Let me suggest as DFO that if you
7 as private citizens wish to communicate to the FTC
8 outside of the scope of this committee you're certainly
9 free to, and if it's something that you want to put as
10 an option and again as part of your report to help
11 educate the Commission on its interpretation I think
12 it's also appropriate, but I believe we have to separate
13 those two in terms of committee process.

14 MR. TORRES: Frank Torres. I think we have to
15 recognize that disclosure is only one part of the
16 process here that -- and I echo concerns that other
17 folks raised. I'm very positive about disclosure if
18 it's truthful and meaningful and simple but we do have
19 to get beyond that, and we've said before in the privacy
20 debate disclosure is not protection.

21 Privacy disclosure is not the same as privacy
22 protection. First of all it can be a lousy best privacy

23 in the world, but if it's not followed it doesn't do the
24 consumer any good, and the same holds true for the
25 security question.

0458

1 So I think I'll say something positive about the
2 sweep. I think it's commendable that the Commission is
3 taking a look at this, but you need to take the next
4 step and see what's actually being implemented and
5 whether or not the security protections are real to the
6 extent that they're disclosed or that they even exist.

7 MR. MEDINE: Again I think the value of this
8 committee is it can educate the Commission on both those
9 questions which is, What is good security or how do you
10 go about providing security on the one hand, and the
11 other is what do you disclose to consumers which may be
12 separate issues, in fact sometimes as we heard earlier
13 may even be in conflict to some extent because you don't
14 want to disclose too much about your security.

15 But again the question that I posed to the
16 committee for feedback on is a minimum disclosure
17 important for consumers to have at least some sense of
18 confidence in how the web site and companies are
19 handling their information. Jane Swift.

20 MS. SWIFT: Jane Swift. Now I have two now. I
21 would just say --

22 MR. WHAM: Does one of those say CBS on it?

23 MS. SWIFT: I think disclosure is only important
24 when it's accompanied by some sense of verification, and
25 disclosure in and of itself which I'm not sure is

0459

1 exactly the same as the reality of security.

2 Verification means is what they're saying

3 they're doing is what they're doing, which I think is

4 the same point Deirdre is making on privacy is it's good

5 to have disclosure. It's good and I think necessary

6 that you have it in terms that folks who -- you all

7 design your software so idiots can use it. You should

8 have that same standard for defining other policies that

9 people can understand, and I include myself in the idiot

10 column, so it's not as insulting.

11 But verification, I think most consumers believe

12 that verification has to come from a third-party, and

13 that's where I think the conundrum is when you're

14 talking about self regulation.

15 MR. MEDINE: Again those are useful comments and

16 certainly there are skilled programs and others who do

17 verification. There also is a link between disclosure

18 and what people are doing which is the FTC Act's

19 prohibition on deceptive trade practices. That is if

20 you're saying you're doing something, then there is a

21 legal standard by which you can judge whether someone is

22 actually doing. It you might want to consider that in

23 the security context as well which is you hold yourself

24 up to a certain standard, then the public is relying on

25 that representation that's being made.

0460

1 MR. PONEMON: May I emphasize one point? As I
2 said before -- Larry Ponemon, Pricewaterhouse Coopers.
3 The level of verification depends, and I don't want
4 there to be -- consumers misled that because they have
5 seal A, B, C or firm X, Y and Z doing the work that they
6 assume that it is in fact 100 percent or 95 percent
7 level of confidence that everything that is in the
8 system is secure, that privacy is maintained and so
9 forth.

10 There are different levels of security. There
11 are different levels of assurance and so that has to be
12 factored into the equation as well?

13 MR. MEDINE: Alex and then Lance happens.

14 MR. GAVIS: Alex Gavis, Fidelity. I want to go
15 back or move back to 10,000 feet for a second in that
16 brick and mortar companies for a long time have been
17 dealing with information that's been provided to them by
18 their customers, and in fact information security
19 practices and have been around for a long time, and I
20 guess to some extent the case has to be made as to why
21 suddenly in this regime there needs to be a disclosure
22 practice or there needs to be some sort of enhanced

23 method of disclosing practices.

24 And I'm not quite sure we made that case. I'm

25 not quite sure where we are. Maybe your survey will

0461

1 explain at the outset sort of why you're in this space
2 and why you're thinking about it, but I do think
3 companies do and a number of them have had information
4 security practices and quite reasonable ones and don't
5 necessarily disclose them to the public, and there
6 probably hasn't been a need to disclose them to the
7 public.

8 MR. MEDINE: Just to respond briefly to that
9 point. The Commission since 1996 has laid out what it
10 has viewed as Fair Information Practices, and it arrived
11 at that by examining the work of others in this area
12 including the OECD's 1980 guidelines, the work of the
13 Commerce Department, Ron's Privacy Commission and so
14 forth in reaching those conclusions but viewed these as
15 all interrelated components of Fair Information
16 Practices, that not only does a company treat your data
17 the way it says it does and tells you what it's doing
18 about it but that essentially may not be much comfort if
19 they don't protect it from improper access and improper
20 use.

21 But I think that's basically what led to the
22 Commission in '96 enunciating what it viewed it's Fair

23 Information Practices.

24 MR. LANCE HOFFMAN: Lance Hoffman. Disclosure

25 is important but it does have problems. We all realize

0462

1 that, and indeed in the security three subgroup I was
2 in, one thing we pointed out we were concerned about the
3 fact that, for example, mandatory check off could serve
4 a disclaimer function for bad actors arguably relieving
5 them of liability, so that's an issue that always comes
6 up with this sort of thing. I want to get that on the
7 record because it is something to look at.

8 I want to note also that I would suspect that
9 the vast majority not by traffic but by just counting
10 the sites, web sites do zero when it comes to -- I'll
11 lump together Deirdre's do zero in terms of talking
12 about it in terms of disclosing.

13 The Yahoos and the AOLs and so forth, no
14 problem, but there are a lot of web sites that do
15 nothing, okay. So again this sort of what you do just
16 saying I do anything at all differentiates and I think
17 that's important, but I won't beat that dead horse
18 anymore.

19 I do want to say something with regard to the
20 sweep since I hadn't focused on it until people started
21 saying Oh, the sweeps, the sweeps are coming, why not do
22 this first and that first. I really disagree I think

23 it's very important the FTC does the sweeps when they

24 said they were going to do them.

25 Time marches on. There's always a good reason

0463

1 for postponing something, new things happening. You
2 know, come on, you have to work on Internet time.
3 Sweeps will happen they'll happen next year or two.
4 We're going to make changes incrementally so I don't
5 think the level of error, if you would, or embarrassment
6 that might come out of the sweeps is going to negate
7 their value relative to the information we get to build
8 a frame to work on.

9 MR. LANE: Rick Lane, U.S. Chamber. It's not
10 embarrassment. It's more misinterpretation that we're
11 fearful of, and that's in an election year and political
12 ramifications -- maybe I'm too much inside the Beltway,
13 but perception becomes reality in this town very easily,
14 and in a election year it's even more heightened, and
15 the concern is if you have raw data that's not explained
16 or not in context, the perception becomes a reality.

17 And you have knee jerk reactions that could be a
18 hindrance to the current economic development we have
19 seen in the ECommerce world, so that is the concern that
20 is shared before there's a context put in place, so that
21 is on that issue.

22 MR. MEDINE: Can I just add to that, that again

23 this committee is uniquely situated to get the

24 Commission's ear as the Commission considers the raw

25 data and the Commission analyzes the data and the

0464

1 Commission writes the report that explains the results.

2 And so this is an opportunity to make your case

3 to the Commission about how the data ought to be

4 interpreted and this committee's work will be the tool

5 the Commission uses in evaluating that information.

6 MR. LANE: Can Congress get the data before the

7 report is written?

8 MR. MEDINE: Before the report is written?

9 MR. LANE: Once the sweeps are done and the data

10 is in place --

11 MR. MEDINE: Counsel's advised me that I

12 shouldn't answer that questions because that's a loser

13 either way. I don't know.

14 MR. KAMP: John Kamp from the AAAA. I just

15 wanted to underline the political danger of

16 misinterpretation. In fact in a public meeting this

17 week a member of the White House staff in a meeting by

18 an OPA has already opined that the industry is not going

19 to do well in the study, and that is going to increase

20 the calls from the Congress to have legislation in this

21 area.

22 So we're talking about a politically very

23 important, if not volatile, explosive possibility being

24 created here by doing this study I think prematurely.

25 MR. WHAM: This is Ted Wham from Excite@Home. I

0465

1 would argue that any organization of any size on the
2 Internet that didn't see this coming and didn't act for
3 it deserves whatever the hell happens to them because
4 exactly the same thing happened last year. Exactly the
5 same thing happened the year before.

6 The basic fundamentals as I understand them of
7 how the study's being run are very, very close and
8 certainly within the public's eyes are
9 indistinguishable. I think Lance's comments about how
10 time marches on and you do the best could not be more
11 apropos to the situation that's right here.

12 In 1997 we were an early participant with
13 TRUSTe. TRUSTe hadn't been around that long. They had
14 20 different people out there, and the FTC is out
15 drumming -- I have to take that back, 1998, they're
16 drumming on the -- their thing and saying, We're going
17 to do a sweep, We're going to do a sweep, and TRUSTe
18 contacted us and said Oh, my God, industry didn't have
19 their act together, can you help us.

20 And I spearheaded an activity with all of the
21 executives where we wrote letters to the top 100 domains
22 out there and said, You got to have a privacy policy up,

23 and then I it corralled all of those executives and I

24 got George Bell and Brent Bollington and Joe Kraus

25 to sit down on the telephone, and getting a

0466

1 slice of their time is no fun.

2 And we were calling people that didn't want to

3 receive our calls, like CEOs of Lycos that didn't

4 think that highly of us, all sorts of different

5 people saying, You have to have a privacy policy out.

6 This is a year and a half ago. Since then COPA's come

7 out. Since then the first policy sweeps have come out

8 and so forth.

9 If I'm not incorrect what the FTC is doing out

10 there is taking a review of privacy policies, is taking

11 a top line, saying who has them and we did this three

12 years ago, only 22 percent or whatever the numbers were,

13 and then we did them a year after that and 68 percent of

14 them top out there, but if there's one of the top 100

15 that doesn't have a privacy policy up, shame on them.

16 MR. JAYE: Can I just take a comment on that for

17 a second because it's very interesting we looked at

18 the '98 sweeps. I think this actually portrays why

19 interpretation methodology is so important.

20 When you actually went into the data on the '98

21 sweeps it was not nearly as bad as it was initially

22 portrayed. On page 1 they talk about 14 percent of

23 sites that is the general sites of general ECommerce

24 companies which generally were brick and mortar companies

25 that had web sites only had privacy statements.

0467

1 Ted's exactly right. There was a massive
2 industry effort to try to get the web -- and the focus
3 was completely on web centered companies, and back on page
4 6 was the first mention of the fact that the web
5 actually didn't do as miserably. Admittedly they should
6 have had 99 percent compliance because of the outreach,
7 I forget whether it was 50 percent or 60 percent, but
8 back on pages 6 was the details that the top 100 sites
9 had actually done significantly better than that 14
10 percent.

11 But the front page talked about a set of sites
12 that candidly those of us who were out canvassing and
13 doing outreach weren't even talking to because we had --
14 basically two years ago they weren't really -- they
15 weren't as important as they are now because the general
16 top large companies weren't really on the web that much
17 back then.

18 MR. LANE: This was a front page story.

19 MR. JAYE: The issue was 14 percent, and nobody
20 dug down to page 6 where it talked about what the
21 largest sites which represented the bulk of the percent
22 of time consumers spend browsing so that the bulk of the

23 percent of time consumers spend browsing was being spent

24 on these top sites which related -- which had although

25 not acceptable way below par privacy statements and

0468

1 coverage, still were significantly north of what

2 primarily got presented or picked up by the media.

3 So that's one of the reasons why we do have a

4 very -- a great deal of sensitivity about interpretation

5 of the results.

6 MR. MEDINE: If I could make two points of

7 clarification, and then we can continue for just a

8 little while longer one, is the Commission's report and

9 the survey result will follow this committee's report

10 the Commission will have the opportunity to consider the

11 work of this committee.

12 Second, if anyone is reporting on the results of

13 our survey, I can assure you we don't know what the

14 results of our survey are going to be, and so I don't

15 know how anyone else could possibly know what the

16 numbers are going to look like because we're in the

17 middle of it and we don't what the numbers are at this

18 stage in the process

19 Larry?

20 MR. PONEMON: One thing that I just wanted to

21 mention about based on our experience and looking at

22 privacy policies, we do a lot of privacy risk management

23 and privacy work and the majority of our clients are not
24 in compliance, are not in compliance with their stated
25 policy.

0469

1 So the mere fact that you have policies that
2 gives false confidence and false praise in many cases to
3 companies. It's easy to write it but it's a lot harder
4 to walk the talk, and that's what we see. That's across
5 the board, not just in the e-space for all
6 organizations.

7 MR. MEDINE: I'm attempted to say provide us a
8 list of those companies, Richard and then Stewart.

9 MR. RICHARD SMITH: I would like to agree with
10 that, also the little bit I've looked at privacy
11 policies and security practices there's a -- and so it's
12 sort of amusing here, this discussion of interpretation
13 of and results I find interesting because if you really
14 get down -- the privacy policy is one aspect. Practices
15 is the more interesting issue.

16 But one thing that's important to say about
17 disclosure I want to make one small remark about
18 disclosure is privacy policies do have another use
19 beyond consumer confidence and explaining to consumers
20 what's going on which is also it gets into written form
21 for people at the company to understand what their
22 company is committing to, but, yes, they don't always

23 follow it all, but it is there written, and I think

24 it's an important thing. It's just like a contract.

25 It's there. You make your mark in the sand so I

0470

1 don't want to discount disclosure totally as another
2 whole aspect because it lets people in the company.

3 MR. MEDINE: Why don't we, given the hour, take
4 a handful more comments and then we can wrap up for
5 today. Stewart?

6 MR. BAKER: I tried my hand at a draft while you
7 guys were talking. It doesn't actually say they
8 shouldn't do the survey or they should, but just says
9 there's a problem so I'll read it.

10 We're all members of the FTC advisory committee
11 writing in our individual capacity. At our last meeting
12 there was extensive discussion of the Commission's plans
13 to do a sweep of major commercial web sites to examine,
14 among other things, the security disclosures provided to
15 the public by those sites.

16 Disclosure of security practices, however, may
17 have little or nothing to do with the actual security
18 provided for customer data. Equally important, the lack
19 of a statement on security practices does not mean that
20 a site provides inadequate security.

21 While disclosure of security practices is an
22 option for encouraging good security, it is only one of

23 many options the committee is evaluating. There is a

24 real risk that a survey limited to the presence or

25 absence of a security statement on a web site will be

0471

1 misinterpreted.

2 We urge that the Commission consider these views
3 in deciding whether to conduct such a survey and how to
4 present and interpret any data that may result from such
5 a survey.

6 That was sort of --

7 MR. MEDINE: I'm going to terminate discussion
8 of things that the committee members do in their
9 individual capacity, but let me just say that that's the
10 kind of committee report that would be extremely helpful
11 to the Commission in interpreting the results of this
12 information so you might want to consider in the
13 security group addressing that as part of your report in
14 terms of how the Commission ought to evaluate survey
15 results.

16 Let's take it like one or two comments.

17 Deirdre?

18 MS. MULLIGAN: Deirdre Mulligan. I fully
19 support that but I think the frustration is that it
20 appears that everyone around this table recognizes that
21 a security statement does not give us adequate
22 information to evaluate security.

23 Yet people seem to want to hang on to the fact
24 that privacy statement might give us adequate
25 information to evaluate privacy, and I think I would be

0472

1 overjoyed if the people around this table would like to
2 write a joint letter to the Commission suggesting that
3 rather than doing another sweep, where I completely
4 agree can be wildly misinterpreted, 66 percent increase
5 in a discussion about privacy, it tells us nothing about
6 whether or not people's privacy is being protected or
7 not -- if we would like to suggest that the Commission
8 use its resources in another manner.

9 For example, I think the survey that Richard
10 Smith did in coordination with the California Health
11 Care Foundation was an incredibly useful detailed
12 survey. It showed both what the policy stated and
13 whether or not there they were being adhered to, and
14 that's the kind of information that I think you can use
15 to do a valid assessment.

16 And if other people think that would be an
17 useful thing to do I would love to do it. Our public
18 fund should be spent wisely.

19 MR. MEDINE: Thank you all for a lively, and
20 informing day, and we'll see you on March 31. We're
21 adjourned.

22 (Time noted: 5:08 p.m.)

23 - - - - -

24

25

0473

1 CERTIFICATION OF REPORTER

2

3 DOCKET/FILE NUMBER: P004807

4 CASE TITLE: ONLINE ACCESS AND SECURITY

5 HEARING DATE: FEBRUARY 25, 2000

6

7 WE HEREBY CERTIFY that the transcript contained

8 herein is a full and accurate transcript of the notes

9 taken by us at the hearing on the above cause before the

10 FEDERAL TRADE COMMISSION to the best of our knowledge

11 and belief.

12

13 DATED: FEBRUARY 28, 2000

14

15 SUSANNE Q. TATE, RMR

16

17 DEBRA L. MAHEUX

18

19 CERTIFICATION OF PROOFREADER

20

21 I HEREBY CERTIFY that I proofread the transcript

22 for accuracy in spelling, hyphenation, punctuation and

23 format.

24

25

DIANE QUADE