

1		I N D E X
2		
3	Session	Page
4		
5	Opening Remarks	479
6		
7	Scheduling Discussion	484
8		
9	Access Discussion	525
10		
11	Entities Discussion	591
12		
13	Authentication Discussion	633
14		
15	Afternoon Session	657
16		
17	Security Discussion	673
18		
19	Public Comment	731
20		
21		
22		
23		
24		
25		

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

FEDERAL TRADE COMMISSION

ADVISORY COMMITTEE ON
ONLINE ACCESS AND SECURITY

8:00 a.m.

MARCH 31, 2000

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

REPORTED BY: SALLY JO BOWLING and DEBRA L. MEHEUX

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 COMMITTEE MEMBERS:

2

3 Robert D. Henderson, NCR Corporation

4 David Hoffman, Intel Corporation

5 Dr. Lance J. Hoffman, George Washington University

6 Josh Isay, DoubleClick, Inc.

7 Daniel Jaye, Engage Technologies, Inc.

8 John Kamp, American Association of Advertising Agencies

9 Rick Lane, U.S. Chamber of Commerce

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

11 Gregory Miller, MedicaLogic, Inc.

12 Deirdre Mulligan, Center for Democracy and Technology

13 Deborah Pierce, Electronic Frontier Foundation

14 Ronald L. Plessner, Piper, Marbury, Rudnick & Wolfe LLP

15 Dr. Lawrence A. Ponemon, PricewaterhouseCoopers, LLP

16 Richard Purcell, Microsoft Corporation

17 Roger Kirkpatrick, Time Warner, Inc.

18 Dr. Daniel Schutzer, Citigroup

19 Andrew Shen, Electronic Privacy Information Center

20 Richard M. Smith, Internet Consultant

21 Dr. Jonathan M. Smith, University of Pennsylvania

22 David Veator, Commonwealth of Massachusetts

23 James E. Tierney, Consultant

24

25

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 COMMITTEE MEMBERS:

2

3 Frank C. Torres, III, Consumers Union

4 Thomas Wadlow, Pilot Network Services, Inc.

5 Ted Wham, Excite@Home Network

6 Rebecca Whitener, IBM Corporation

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 it some time this morning, that I think will be helpful
2 to all of us to keep focused and keep on track as we
3 try to complete this -- complete this task that we have
4 asked all of you to do.

5 As you know, the committee's final report is
6 due on May 15th, that as I look at that calendar, it
7 looked like six weeks to complete this task. But based
8 upon what you've already done so far, we have every
9 confidence that it will go forward.

10 I want to particularly commend all of you for
11 being so dedicated to attending every meeting and to
12 getting the work done. It really has been hard,
13 schedules change and it's been a really dedicated
14 effort on all of your part, and on those of the public
15 who have -- are not officially members of the
16 committee, have also come, which is important to us.

17 So, let me just remind you that everyone should
18 take advantage of the opportunity to speak up during
19 the public periods. Also to comment as we go along,
20 and again, on behalf of our staff and the
21 Commission, we are very appreciative of all the work
22 that's been done. We look forward to the day's arduous
23 meeting agenda, and to the completion of the work
24 coming up soon in six weeks on May 15th.

25 I can assure you the Commission is very much

1 looking forward to your report and to your advice,
2 because that's the purpose of this task and is coming
3 to completion soon.

4 So, thanks again, now let's all get to work.

5 MR. MEDINE: Thank you, Jodie. Let me begin as
6 usual by calling the roll. James Allen?

7 MR. ALLEN: Present.

8 MR. MEDINE: Stewart Baker? Richard Bates?
9 Paula Bruening?

10 MS. BRUENING: Here.

11 MR. MEDINE: Steve Casey?

12 MR. CASEY: Here.

13 MR. MEDINE: Fred Cate? Jerry Cerasale?

14 MR. CERASALE: Here.

15 MR. MEDINE: Steve Cole?

16 MR. COLE: Here.

17 MR. MEDINE: Lorrie Cranor?

18 MS. CRANOR: Here.

19 MR. MEDINE: Mary Culnan?

20 MS. CURNAN: Here.

21 MR. MEDINE: David Ellington? Tatiana Gau?

22 MS. GAU: Here.

23 MR. MEDINE: Alexander Gavis?

24 MR. GAVIS: Here.

25 MR. MEDINE: Daniel Geer?

1 MR. GEER: Here.

2 MR. MEDINE: Robert Henderson?

3 MR. HENDERSON: Here.

4 MR. MEDINE: David Hoffman?

5 MR. DAVID HOFFMAN: Here.

6 MR. MEDINE: Lance Hoffman?

7 MR. LANCE HOFFMAN: Here.

8 MR. MEDINE: Josh Isay? Don Jaye?

9 MR. JAYE: Here.

10 MR. MEDINE: Don Kamp?

11 MR. KAMP: Here.

12 MR. MEDINE: Rick Lane?

13 MR. LANE: Here.

14 MR. MEDINE: James Maxson? Greg Miller?

15 MR. MILLER: Here.

16 MR. MEDINE: Deirdre Mulligan?

17 MS. MULLIGAN: Here.

18 MR. MEDINE: Deborah Pierce?

19 MS. PIERCE: Here.

20 MR. MEDINE: Ronald Plessner?

21 MR. PLESSER: Here.

22 MR. MEDINE: Richard Purcell?

23 MR. PURCELL: Here.

24 MR. MEDINE: Robert Kirkpatrick?

25 MR. KIRKPATRICK: Roger Kirkpatrick.

1 MR. MEDINE: I'm sorry, Roger? Roger
2 Kirkpatrick is here. Dan Schutzer?
3 MR. SCHUTZER: Here.
4 MR. MEDINE: Andrew Shen?
5 MR. SHEN: Here.
6 MR. MEDINE: Richard Smith? Jonathan Smith?
7 David Veator?
8 MR. VEATOR: Here.
9 MR. MEDINE: Jim Tierney? Frank Torres?
10 MR. TORRES: Here.
11 MR. MEDINE: Tom Wadlow?
12 MR. WADLOW: Here.
13 MR. MEDINE: Ted Wham?
14 MR. WHAM: Here.
15 MR. MEDINE: Rebecca Whitener? Thank you and I
16 think we have a quorum to allow us to proceed.
17 Once again, let me remind everybody that we do
18 have a court reporter today, so please make an effort
19 at least until she gets to know you to state your name
20 before you speak, and speak into the microphone, and to
21 try to speak one at a time so that she can keep the
22 record straight.
23 In terms of public comments, as you know, we've
24 been accepting public comments on the process and have
25 been posting them on our website. We've received about

1 a dozen comments from members of the public to date,
2 and I would urge all the committee members to regularly
3 check the -- our web page for the committee on the
4 ftc.gov website as the comments are directed to you as
5 committee members for your review and consideration.
6 And so we urge you as you move forward in completing
7 the report to consider the comments from the public.

8 As Jodie said, the committee's report as you
9 know is due to the Commission no later than May 15th,
10 and so we would like to try to focus on how we can go
11 about meeting that deadline. We were talking earlier
12 about how we've been kind of pacing ourselves so far,
13 but now we're in the sprint stage of the process to get
14 all the work done on time.

15 We have put before you a proposed schedule,
16 which I would like to discuss. We looked at today's
17 date and we looked at May 15th to try to figure out how
18 we could get the committee's work done on time and also
19 make sure that all the committee members had a chance
20 to express their views on all subjects, since we
21 appreciate the fact that you've broken up into
22 subgroups, but of course you all are free and
23 encouraged to comment on all the issues.

24 So, what we're proposing, again, as an
25 ambitious schedule of trying by April 14th, in two

1 weeks, to have each sub -- keep in your current
2 subgroups who produced the options papers today and
3 transform those options papers in a draft section to
4 the report to the Commission. We would like to ask
5 each subgroup to nominate or have a volunteer of one
6 member to be the lead person in getting that
7 section together, and by April 14th to email, as you've
8 done in the past, the draft section of the report to
9 the advisory committee mailbox.

10 We will then post the drafts on the website and
11 we would encourage all members of the committee to
12 review all of the drafts and to make sure that your
13 views are represented, and if not, by April 21, to
14 submit comments or propose additions to the lead draft
15 person for that particular section so that they can
16 then incorporate any additional comments from the group
17 at large, and to aim to have a revised draft submitted
18 to the committee and on the website by April 26th,
19 which is just two days before our final meeting on
20 April 28th.

21 What we would then propose to do is to meet on
22 April 28th, review the draft report and then allow
23 essentially a few -- a little bit more time for the
24 advisory committee members to submit comments on the
25 final report and then basically propose to have two

1 days to review the report after the last meeting and
2 then call for an email vote two days after that. And
3 so people have had a chance to review the final report
4 and then rather than convening again, allow a vote by
5 email on the final report.

6 I guess I would like to see if that -- it may
7 not be ideal, but if that -- if people would like to
8 discuss that and have -- are comfortable with it or
9 would like to suggest alternative approaches. Deirdre?

10 MS. MULLIGAN: I would very much be in favor of
11 pushing the date for the first draft back until about
12 the 19th and pushing the schedule back a little bit
13 from there. I think many of the people here are going
14 to be involved in Computers, Freedom and Privacy, which
15 occupies basically all of next week, and those --
16 particularly because it then runs into Passover, I
17 think it would be better to give people some more time
18 to incorporate the comments from the work today. So,
19 that would be my request.

20 MR. MEDINE: So, just to clarify, would you
21 then propose essentially moving all of the key events
22 back, say, three days from their current -- three or
23 four days from their current --

24 MS. MULLIGAN: Yeah, I mean with some
25 flexibility. If there are some deadlines that you

1 can't move back, that would be okay.

2 MR. MEDINE: Well, I mean it does leave
3 some time, I guess, partly, and one of the other
4 things I guess I wanted to see if we could get
5 somebody to volunteer to merge in format and word
6 processing into one document, and if the group
7 could be --

8 MS. MULLIGAN: I will sign up for all of that
9 if we can move it back three days.

10 MR. LANE: Sold. I second that.

11 MR. MEDINE: I don't think we even have to put
12 that one to a vote. I think that would be helpful
13 -- we will, of course, produce it in a final report
14 version, but if it can be delivered to us
15 electronically, and you are now volunteering to do
16 that, I think that gives us some flexibility on time
17 frame.

18 MR. PURCELL: Richard Purcell, I will volunteer
19 to be your scribe, Deirdre, or your helper in whatever
20 way I can.

21 MS. MULLIGAN: Thank you.

22 MR. PURCELL: I think we have a smaller group
23 of people that are on that last formatting stage.

24 MR. PLESSER: Ron?

25 MR. PLESSER: I would be happy to help with

1 that.

2 MR. MILLER: Me, too.

3 MS. BRUENING: I will help as well.

4 MR. MEDINE: Any additional discussion about
5 the -- Jerry?

6 MR. CERASALE: Jerry Cerasale. What does it do
7 with the 28th? I think that Deirdre's schedule is
8 fine, but we've got everything set up looking in our
9 calendars blocked off the 28th and I don't think moving
10 three days, it's silly to have -- I don't know if it's
11 silly, would be less fruitful to have that meeting and
12 not at least have a day to look at whatever the revised
13 section of the report we're going to get.

14 MR. MEDINE: John and then Frank?

15 MR. KAMP: John Kamp. I propose that we do, we
16 do sort of a compromise method, we pick up the three
17 days between now and the 28th, but we keep the 28th day
18 right where it is, essentially to respect the fact that
19 we have to do the meeting on the 28th, and we move the
20 first couple of things back a few days, in order to
21 make it possible to respect Deirdre, I think, sort of
22 well suggested problem with the -- all of a sudden we
23 have a deadline that seems like tomorrow morning, but I
24 think we have to -- we have to stay on the 28th
25 schedule.

1 MR. MEDINE: Frank?

2 MR. TORRES: I agree with that comment that we
3 stick to the 28th, but if we move the first draft to
4 the 19th, and push the comments, say, to the 24th,
5 which is the Monday. It kind of crunches the folks
6 that then incorporate the comments into the revised
7 section report to you on the 26th, but I think provided
8 everybody gets the comments in on the 24th, that that
9 might provide enough time. So, that puts us back on
10 track.

11 MR. MEDINE: That seems like a reasonable
12 suggestion. I'm seeing a lot of nodding from everyone
13 about that. Again, we appreciate that this is all
14 because we've got to get our job done on time and I
15 think this will accomplish it, and most importantly
16 give all the committee members an opportunity for input
17 along the way.

18 MR. PLESSER: So, what's the final?

19 MR. MEDINE: The final bidding is that the
20 first draft of the report is due from the subgroups on
21 April 19th, comments will be due from the full
22 committee on any section people want to comment on by
23 the 24th, and just confirm, are we going to say that's
24 the revised section will really make absolute best
25 efforts to circulate the revised section of the report

1 before the meeting on the 28th and ideally perhaps by
2 the end of the 26th?

3 MS. MULLIGAN: Could we actually put hard time
4 deadlines on the 24th and the 26th?

5 MR. MEDINE: Okay.

6 MS. MULLIGAN: I'm comfortable doing something
7 that is more friendly to our Pacific coast friends, but
8 just a hard time deadline.

9 MR. MEDINE: Okay. Would you like to propose
10 one?

11 MS. MULLIGAN: 5:00 p.m. would be fine, for me,
12 east coast standard time, but I don't know if that's
13 acceptable for people on the west coast.

14 MR. MEDINE: So, the proposal is --

15 MR. CERASALE: Eastern daylight time.

16 MS. MULLIGAN: Eastern daylight time, oh, okay.

17 MR. MEDINE: The deadlines for the 24th and the
18 26th would be 5:00 p.m. eastern daylight time.

19 MR. HENDERSON: That's acceptable.

20 MR. MEDINE: That was Robert Henderson. Then I
21 guess I would -- any further discussion about that?

22 MR. SCHUTZER: So, the event on the 24th, the
23 day is on the 26th?

24 MR. MEDINE: No, actually the 24th.

25 MR. SCHUTZER: What's the 17th? That's also

1 the 24th?

2 MS. MULLIGAN: That's just a review, though,
3 that's not a deadline.

4 MR. MEDINE: The 1st is not so much as a strict
5 event.

6 MS. MULLIGAN: It's a hint.

7 MR. MEDINE: So much as a period of time for
8 the review.

9 MR. SCHUTZER: Okay.

10 MR. MEDINE: And then again I guess we're
11 proposing, just let's complete the process, after the
12 meeting on the 28th, we are proposing two additional
13 days for final, final, final comments on the report.

14 MR. COLE: I have a question about that.

15 MR. MEDINE: Sure.

16 MR. COLE: Steve Cole. What exactly happens on
17 the 28th? Does this committee vote on a report?

18 MR. MEDINE: Well, I was just going to get to
19 that.

20 MR. COLE: Well, afterwards, then, I will have
21 a question what happens those two days and then what's
22 the next vote. Why don't you go first.

23 MR. MEDINE: What we were proposing to do is
24 give the committee two or -- we'll propose two days
25 after the meeting on the 28th, two business days to

1 review what both the final report and whatever
2 discussion ensues at the meeting on the 28th, and then
3 I guess incorporate any final, final revisions, and
4 then what we're proposing is an -- that the committee
5 vote by email and have a 48-hour period by email so the
6 committee doesn't have to convene again in Washington
7 just to vote on the final report.

8 MR. COLE: Let me ask the question again, is
9 there not a vote on the 28th?

10 MR. MEDINE: I guess there's not a vote on the
11 28th.

12 MR. COLE: I see this as a deliberative body,
13 and I see this as a problem with deliberative bodies
14 voting by mail without a discussion of the items. I
15 don't have a solution, but I do have a concern.

16 MR. PLESSER: Could we have a decision on the
17 28th and then the final by email? I mean I think
18 Steve's point is, I mean I think you can have a slot on
19 the 28th, see how close you get, then take revisions
20 and have subjects. So, I have another point, though,
21 that I would like to -- Steve, does that resolve your
22 concern?

23 MR. COLE: Yes, it does.

24 MR. SCHUTZER: So, email is on the 28th?

25 MR. MEDINE: To clarify, we will vote on a vast

1 majority of the documents sort of as a principle to
2 approve the report as it exists at that time, subject
3 to the discussion at the meeting, at the close of the
4 meeting on the 28th.

5 MR. COLE: That reduces the last few days of
6 gee, if we miss something or there's one more thing, it
7 narrows it down as opposed to opening up every single
8 word of the document to a vote where there's no
9 discussion. So, that does handle it.

10 MR. MEDINE: And then a final, final vote by
11 email on whatever minor, hopefully minor, changes would
12 be made after the 28th.

13 MR. COLE: Yeah.

14 MR. MEDINE: Ron?

15 MR. PLESSER: Ron Plessler. I mean I know the
16 way the report seems to be taking shape, it's going to
17 have a lot of options, but there may be a time when
18 either individuals or groupings of individuals may want
19 to have comments. You know, I hate to call it a
20 dissent or a concurrence or, you know, have some
21 specific views, and I'm not sure that that's going to
22 happen, but I wondered, you know, if you -- if you had
23 space for that.

24 If there will be, you know, an opportunity, and
25 perhaps on these deadlines, in terms of submitting it,

1 to view -- I mean, I hope we don't get 50 views, I hope
2 it maybe gets narrowed down to, you know, the primary
3 groupings, but I think it would be very important to be
4 able to do that, and I don't know -- I don't see that
5 on the schedule and I don't know that that's part of
6 your process. Have you thought about that?

7 MR. MEDINE: Well, let me suggest our thinking
8 about that, but again it's obviously it's the
9 committee's decision. Because the document is
10 an open document and this process is designed to
11 encourage everyone to have their views input at the
12 appropriate parts of the document, it's hard to imagine
13 that there would be dissenting views, because there are
14 going to be -- there are going to be pros and cons on
15 every possible issue and so that everyone will have had
16 an opportunity to express their views in the context of
17 the pros and cons.

18 So, I guess the question is whether there will
19 be a need -- I mean typically if this group were to
20 come to a single proposal, then one could anticipate
21 the need for dissenting or concurring views, but to the
22 extent that this whole process is designed at every
23 stage to express everyone's point of view, I guess we
24 didn't really see that there would be a need for it,
25 because you will express your view on the pros and cons

1 of a particular issue that you will say that I think
2 this is good or bad approach and you will express your
3 views at that stage.

4 MR. TORRES: David? Frank Torres. Then I'm a
5 little bit confused about the purpose of the vote if
6 all the views are supposed to be considered, and my
7 approach to it might be like this: I think just in
8 terms of the discussions that we've had in the
9 subgroups, that hopefully there will be lots of areas
10 where everybody around the table will agree to certain
11 general concepts and principles, and to the extent that
12 we get kind of a unanimous decision that, you know,
13 here are some elements that everyone agrees to should
14 be part of this report, and then allow for what Ron, I
15 think, has suggested, and that kind of the ability to
16 kind of have the -- I think some people put it down as
17 pros and cons and be able to explain it and flesh it
18 out.

19 But to me, if you take a vote on whether or not
20 you support what some of the consumer groups might
21 think is a con against something or that doesn't make
22 sense, can the rest of the group say well, we won't do
23 that in the report? But I don't think that's the way
24 it is, but I think there's some confusion about
25 that.

1 MR. MEDINE: Let me just respond to Ron and
2 then Jerry. But to the extent the committee presents a
3 report or proposal with no cons, then presumably that
4 would reflect the views of the entire group and if
5 there were varying views, again the report would
6 reflect that. I guess the vote would really be that
7 every committee member, or the majority felt
8 comfortable that the report adequately represented
9 their views, not that they necessarily endorse any
10 particular view in the report, but that they would feel
11 comfortable that they had had a chance, as did
12 everybody else, to express their views in the report.
13 And again, if at the end of the day there's a
14 particular recommendation that all 40 of you have said
15 it's a good thing and no one opposes it, I think the
16 message has come across from the report itself that
17 this is a strongly held view.

18 Ron and then Mary.

19 MR. PLESSER: Mary first.

20 MS. CULNAN: Mary Culnan, I would offer one
21 possibility and that would be that members of the
22 committee either singly or in groups on behalf of
23 whoever they represent could file public comments and
24 put those in an appendix in the report similar to what
25 we did last year with the Georgetown Study, and for a

1 process of that, there was a firm deadline when it had
2 to be in, everything had to conform to a certain type
3 font so it fit with the rest of the report, and you had
4 a fixed page limit. And --

5 MR. MEDINE: Again, I would just suggest as a
6 first shot that you do that, but that your comments be
7 incorporated in the body of the report as part of the
8 report, and that's the advantage unlike the Georgetown
9 Report where there was essentially a majority view
10 which people then dissented from, this is your report
11 and --

12 MS. CULNAN: My view in terms of what we did
13 and people were then allowed to then comment. So, in
14 this case --

15 MR. MEDINE: The majority one.

16 MS. CULNAN: The M plus one view, but people
17 wanted to comment on the findings since there were no
18 conclusions drawn in the report itself in terms of --
19 but I just I toss that out as one possibility because
20 it seemed to make people happy just to have a voice.

21 MR. MEDINE: Why don't we work our way around.
22 Dan?

23 MR. GEER: Dan Geer. I represent.

24 MR. MEDINE: Can you use the microphone?

25 MR. GEER: Sorry, of course.

1 I would rather prefer that there be some
2 explicit place where I as an individual, and I would
3 hope everyone here as individuals, would write their
4 view on this much the way frankly not so much a
5 legislative body, but our friends at the Supreme Court
6 do. I'm very much more interested in having that kind
7 of clarity.

8 No offense to the operation here at all, but the
9 committee's whole job is to sand off sharp edges and if
10 you're looking for as many options, as many possible
11 tacts you might take, you will not get clarity out of a
12 committee report that's consensus. It cannot be done
13 in my view. You can only get it from the kind of
14 single voice clarity that would come in addition to
15 this is the best we can do as a group, but, and then
16 have each of us, I would actually, if it were me, I
17 would make it a requirement that each of us file a
18 separate --

19 MR. MEDINE: Let me just emphasize, this
20 committee is not operating by consensus, and so
21 everyone will have their say in the body of the report.
22 Obviously the committee will decide how it wants to
23 structure the report ultimately and you will be doing
24 the drafting, but just remember this is not a committee
25 report where you have to reach accommodation on any

1 issue. We encourage 40 people with distinct views to
2 express themselves in the body of the report itself and
3 not come to any particular conclusions as a group
4 necessarily.

5 Rick?

6 MR. LANE: Rick Lane, U.S. Chamber. One of the
7 pros and cons will be in there, but just because
8 there's pros and cons, I may agree with some of the
9 cons on a particular issue, but the pros override those
10 cons. And so there may be a vote, even though you're
11 listing them, where there is a consensus or we all
12 agree, even with those cons. I think we need to make
13 sure that those votes are taken.

14 The other question I have is more of a
15 technical question, which is are we allowed to do our
16 votes by email? Is that legally binding, you know,
17 considering all the rules?

18 MR. MEDINE: The by-laws and the charter
19 are silent on that and so I think it's within the
20 prerogative of the group to authorize that if the group
21 so chooses. I think again the alternative is to meet
22 again.

23 MR. LANE: No, I don't want to do that, I don't
24 want to go through the coffeegate thing again.

25 MS. BERNSTEIN: We'll get somebody else to do

1 the coffee.

2 MR. MEDINE: Greg?

3 MR. MILLER: Greg Miller, MedicalLogic. First
4 of all I want to thank Rick for the coffee.

5 Two questions. One, I just want a
6 clarification that the purpose of the vote is to accept
7 the report as compiled?

8 MR. MEDINE: It's to authorize the committee to
9 transmit the report to the Federal Trade Commission as
10 compiled.

11 MR. MILLER: Okay. In the unlikely event, and
12 I can't imagine this happening, that the group were to
13 vote in favor of not doing that, do you have a
14 contingency plan?

15 MR. MEDINE: The committee may not report it --
16 it's hard to imagine that that would happen again,
17 because the whole design is to incorporate everyone's
18 views.

19 MR. MILLER: Right.

20 MR. MEDINE: So, it's hard to imagine the
21 committee having had a chance to incorporate their
22 views in the report in any fashion they wish, but also
23 vote no on the transmission of the report, but the
24 committee would not report it, I mean the committee
25 goes out of business on May 31st and there's not much

1 time to reconvene and draft a new report.

2 Deirdre?

3 MS. MULLIGAN: Deirdre Mulligan. You know, my
4 hope would be to the extent possible that we could meet
5 your vision of making sure that people feel as though
6 their views are adequately reflected and where there's
7 consensus, consensus is identified as such.

8 I am anxious about having a document that
9 everybody says yeah, yeah, we sign off on that, but
10 here's my real view and having, let's face it, an awful
11 lot of individuals who represent organizations, trade
12 associations, you know, and there's one thing, Dan, I
13 definitely hear you speaking as an individual in your
14 own voice what does this mean. All of us are free to
15 file public comments. Our organizations can, you know,
16 our businesses can, et cetera, so there is a way for
17 people to make their views heard.

18 I don't think it's a bad thing to necessarily
19 incorporate individual statements from each of us, but
20 to the extent that it takes away from efforts to try to
21 develop consensus, I am anxious about it, and so I
22 would prefer that we focus on trying to develop a
23 consensus document, acknowledging that within the
24 consensus document, there's going to be explicit
25 disagreement about which option people like.

1 And so, you know, maybe at the -- at the point
2 where we're looking at the first draft, if we say you
3 know what, I want to be able to file my own specific
4 statement on this, and then we decide I don't think
5 it's a problem incorporating, I don't know, 35
6 different statements, but I do say that it could divert
7 some of our resources, if each one of us feels as
8 though we have to do that.

9 MR. MEDINE: Ron?

10 MR. PLESSER: Well, I don't think anyone has to
11 do it, I think we could even do a page limit. You've
12 made -- the last time we made committee assignments,
13 you said they would change. This time you've said they
14 are the same, you're going to appoint leaders. I think
15 all of us are comfortable in going along with the
16 system, but you have to give us a little bit of a
17 safety valve to be able to -- and I would hope this
18 would be done in groupings, if somebody didn't like the
19 way the pros and cons were developed.

20 If they thought the approach -- then you put --
21 otherwise you put way too much pressure on the yes or
22 no vote. Then I, you know, I or others have to sit
23 here and decide that it really doesn't reflect the way
24 the balance of things that I like to do it, then I'm
25 going to vote no. But if you give me a safety valve, I

1 can vote yes and then I can say, by the way, to the
2 Commission, who has asked for my views and the views of
3 everyone around the table, say here's a concurring
4 comment, we thought it should have been looked at that
5 way.

6 Hopefully there won't be any of those, but I
7 just think if you don't have a safety valve of that
8 and, you know, I think Frank's -- I would join with
9 Frank, I mean it's not just from our point of view,
10 consumers may want to have a statement in there as
11 well. If you don't have that safety valve, then I
12 think you're putting a lot of pressure on that vote,
13 and I think you should at least think about having a
14 safety valve. It's not a matter of public comments.

15 We were asked, you know, to advise the
16 Commission, and I think if we have a dissent or
17 concurrence, you're not going to get a -- you may not
18 get 100 percent vote, you may get a 90 percent vote,
19 and those 10 percent who disagree, there should be an
20 opportunity for them to put in a dissent or a
21 concurrence, and I don't think this is a big deal, and
22 it's not going to cut against -- in fact, I think
23 contrary to Deirdre's point, I think it's going to
24 allow more concurrence and more people to come
25 together, because then you can kind of make your fine

1 line distinctions if you need to in a concurrence, but
2 join along with the body. If you don't allow that, I
3 think you're going to get more no votes than you
4 thought you would get.

5 MR. MEDINE: Let me just express this, I guess
6 your staff's sort of conception of how that process
7 would work. Our view is that the period of time, which
8 would now be between the 19th and the 24th, would be an
9 opportunity for you to review the draft. If you felt
10 that the approach didn't meet -- wasn't appropriate,
11 that it wasn't expansive enough, didn't cover the
12 issues sufficiently, you would submit an alternate
13 approach by the 24th, and that alternate approach would
14 then be fully incorporated into the document so that
15 the document which once said now do it this way would
16 say on one hand you could do it this way, on the other
17 hand you could do it that way, and then all the views
18 would be represented.

19 Yes, Steve?

20 MR. COLE: I'm going to admit to being
21 thoroughly confused. And I think of myself as being as
22 conceptual as the next guy, but I'm thinking of the first
23 committee meeting we had. Now, ours was the first
24 subgroup, and as you see by the papers, we had a lot of
25 propositions followed by pros and cons. So, when we sit

1 down for our first meeting after this, I think the pros
2 and cons are terrific, let's say. I have a strong view
3 on some of them which pros clearly outweigh the cons or
4 vice versa, but some propositions, I think, are
5 terrific, and some I think are really bad.

6 Do I vote for this document because the pros
7 and cons are fairly stated when I think the
8 proposition in some measure is not so good, or do I
9 say -- or do I vote yes and then write what I think the
10 right answer is, or what do I do in the committee when
11 the committee meets? Because I think we're all going
12 to -- we're making ourselves feel good that we're all
13 going to have an opportunity to express our views by
14 the first committee meeting, I don't think we're going
15 to know what to do. Because if what we're saying as
16 long as all the issues are on the table and we're happy
17 it's on the table, we could probably condense this
18 process and take votes very quickly, at least in our
19 committee. And I think we were expecting that we were
20 putting the options for the committee, the committee
21 would discuss them, we would then go back and make some
22 tentative decision.

23 MR. MEDINE: Again, I'll go to Richard, but let
24 me emphasize the committee is not designed to make
25 recommendations as a committee. The committee is

1 designed, we started off on day one -- the goal of this
2 committee was not to reach a consensus, but to reach a
3 range of options for the Federal Trade Commission to
4 consider as it examines these issues of access and
5 security.

6 So, it was not the goal of the committee
7 to create a consensus or a majority, and as Deirdre
8 pointed out, this committee was not comprised to
9 represent a representative sample of the world, it was
10 designed to represent a degree of expertise on these
11 particular issues, which is different in terms of the
12 significance of a particular vote on it. So, I guess
13 the conception was to articulate a range of options and
14 draw on the group's expertise, but not for the
15 committee to have a consensus view on any particular
16 issue.

17 Richard?

18 MR. PURCELL: This is Richard Purcell. After
19 many, many weeks and months of labor over this issue,
20 let's be cautious here to stick to the goal, and
21 although it's important that voices be heard, there's
22 nobody in the room I think is going to try and quash
23 somebody's voice, it's also vitally important that we
24 solve this challenge, and that we provide reasonable
25 solutions to these very, very difficult issues.

1 Notwithstanding the designated federal
2 officer's comments around consensus, it's my view that
3 we are tasked with solving one of the largest social
4 challenges that faces our industry at this immediate
5 time, and to produce reports that simply lay out here's
6 a problem, here's lots of things that are in support of
7 a particular solution, here's some contravening kinds
8 of issues that do not support that conclusion, to me,
9 does not create the result that we're looking for here.
10 It does not create a solution, it only furthers a, you
11 know, a level of confusion.

12 Let's be very, very, very clear in our final
13 report to provide the one thing that we absolutely need
14 for ourselves, collaboratively, for each other in the
15 industry, and for the Commission here, and that's a
16 document that guides actions into the future.

17 MR. MEDINE: Dan?

18 MR. GEER: I agree with that, and in fact, what
19 I was trying to say was, as a group, we're going to
20 bring in a sack of rocks, and we can all vote that one
21 of those is gold, but I'll bet you anything we don't
22 agree which one is gold.

23 I'm happy to take the vote now to transmit the
24 report, because I have no doubt that this sack will
25 contain the gold that I'm looking for. But I would

1 want each of us to, in fact, vote, if you want to call
2 it that, in the form of an opinion about which parts of
3 this sack of rocks are the ones that are valuable. I
4 don't think a binary bit, a yes or no, a single digit,
5 makes it.

6 MR. MEDINE: Again, let me go back to the
7 original Commission's formulation of this committee,
8 which is again, not as a -- as far as the vote, let's
9 say you won't have the opportunity to draft it because
10 it's your report to express your views and make it
11 clear what you think the correct answer is, but the
12 committee itself was not comprised to create a
13 consensus view, clearly again, to the extent that
14 everyone agrees on an issue, I think that will merge,
15 but I think it's important that those who think they
16 are rocks and those who think they are gold, will have
17 those in the final report so the Commission can benefit
18 from both sides.

19 Dan?

20 MR. SCHUTZER: Yeah, I support the
21 undercurrents going on. I'm trying to explain from my
22 point of view what I think we're striving for. If you
23 look at the way the options and the alternatives are coming
24 out now, like when I see a lot of people starting to
25 read, it's a complex document to get things out of,

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 in terms of the fact that we have a whole array of
2 options, and many different pros and cons, and they're
3 all listed without any kind of, you know, weight or
4 interpretation for how these pros and cons are.

5 Now, in our subcommittees, it would appear we
6 could go a little bit further, you know, as we were
7 talking, I could actually begin to eliminate some
8 options as not practical and take all the pros and the
9 cons, because everything has pros and cons in their
10 substance and talk about other ones, and try to reach
11 forth to a simpler document that adds a little more
12 clarity to the problem.

13 Of course, as we move to that objective, it's
14 clear that it's likely we're going to have some
15 minority opinions, but the report would be stronger.

16 So, I think that's the sense of what we're
17 hearing, is that since there's probably a lot more
18 consensus than lack of consensus, it would be nice to
19 move it one step further and get a clearer report that
20 gives a lot of insight and not just dry pros and cons.
21 If we use just dry pros and cons and what happens is we
22 know we're going to vote for it that way, I'm going to
23 add all the pros that I can and all the cons that I can
24 just to make sure all my stuff is there and then the
25 report gets even more complex in terms of saying

1 anything.

2 So, I would say that we should be striving to
3 reach a consensus in the report, but striving to
4 defuzzify, decloud all these options, and simplify the
5 process, and that means that we should be allowing
6 people to have some form of dissenting views. Now
7 hopefully those dissenting views might not only be one
8 per person, you know what I'm saying, but there might
9 be a minority view that gets expressed or two minority
10 views that might get expressed if there's a strong
11 dissent in a particular view.

12 MR. MEDINE: Let me add one comment, I think
13 again the groups have done a tremendous job of laying
14 out a number of options. I think as you draft the
15 report, think about it perhaps from the point of view
16 of a website operator and are you offering sufficient
17 guidance to that website operator to know, whatever your
18 view happens to be, what to do. Because some of the
19 formulations are extremely complex right now, and maybe
20 that's your -- the design is usually free to do that,
21 but consider operationally how well your
22 recommendations work in practice and can you formulate
23 them in a way that somebody could understand what to do
24 in terms of when the consumer comes and says I want
25 access, do you have a checklist, do you have -- what

1 criteria are you proposing that that website operator
2 use to respond to that request?

3 Secondly, I think it would be very helpful,
4 again, and I know we're under time constraints,
5 I think the pros and cons are excellent, and but they're
6 shorthand that I think the people at the table
7 understand, but I think could probably use some
8 fleshing out, again time permitting, so that the
9 commissioners and the public who read the report could
10 get a better understanding of what you mean by the
11 shorthand pros and cons.

12 So, again, time permitting, I would encourage
13 you to flesh out the arguments on both sides of these
14 issues.

15 Ted?

16 MR. WHAM: Ted Wham. With respect to your
17 comments about not searching for a consensus opinion,
18 that's been clearly stated by you, David, through the
19 entire process from your initial opening remarks and I
20 think it's unreasonable to think that the category of
21 work many are going to have a consensus opinion from a
22 lot of the groups.

23 I think there's going to be a lot of areas of
24 common belief in it and then there's going to be some
25 areas where there's some differences. It may make some

1 sense to shift tacks a little bit in terms of the way
2 the report is presented. So far what we have done
3 is try to do an exposition of what the alternatives are
4 and what the relative pros and cons are of those.

5 In some of those areas, we may want to start to
6 come down with specific recommendations for the
7 committee, where we don't just have a vote, because I
8 think a numerical vote is going to be an unfair process
9 because this is not a representative body of public
10 opinion. There are more industry experts than consumer
11 experts and a pure, you know, numerical isn't fair
12 to represent a balanced viewpoint at all. But it might on
13 a section-by-section basis say within the area of
14 access to, you know, anonymous profiles, the
15 recommendation is X, and the following people would agree
16 with that recommendation and the following people would
17 disagree with that recommendation or posit the
18 alternative as a response. Then within the following
19 area, the access to perhaps nonfinancial data is, you
20 know, here are the recommendation and so forth.

21 And so there's a series of recommendations
22 throughout there and everybody can, you know, sign up
23 for or to, you know, say that they're against different
24 ones. I'm very concerned that if we have a document
25 that has all of the pros and cons or all of the issues

1 out there, it's kind of like saying that one of the
2 pros and cons of taking somebody who has just had a
3 heart attack to the hospital is that they will die from
4 an auto accident on the way. And if we just provide a
5 list of all of those to you, we haven't really helped
6 the debate, and I think some recommendations would
7 help.

8 MR. MEDINE: I think that's fine, again, just
9 to respond to what would be helpful from the
10 Commission and following up on your example, you could
11 certainly do that and hopefully your discussion of that
12 would indicate the pros and cons of that scenario, that
13 pros and cons are of critical importance
14 and there's a minimum con and the Commission could then
15 evaluate that option among the variety of options, and
16 again the value of this diverse committee is to present
17 not one but a number of views for the Commission's
18 consideration and presumably the strengths of the
19 arguments on both sides will help guide the Commission.

20 I'm not saying you can't still express your
21 particular views on particular options, but I think
22 it's the well thought out series of options that will
23 be very beneficial to the Commission going forward.

24 MR. WHAM: In respect to that, I think the
25 example I brought was a very extreme one. I think

1 there are certainly going to be cases where two
2 reasonable men can disagree on what the right
3 recommendation is, and that's what we really need to
4 make clear.

5 MR. MEDINE: Lance?

6 MR. LANCE HOFFMAN: Lance Hoffman, George
7 Washington University. Let me suggest a process which
8 might be a third way which incorporates some of the
9 comments so far because I think -- I don't think any of
10 us wants to come up with a report which is perceived as
11 mush, okay, which is what I hear some of the concerns
12 about. So, I would propose a report that in essence
13 has three parts.

14 The first is a non-mush synopsis. The second
15 part is the pros and cons. The third part, and by the
16 way, that has in essence the sense of limited size or
17 pointers to the sense, whatever is appropriate. The
18 third is a appendices, okay, that way you can put the
19 important material that is generally agreed upon, let's
20 say by a two-thirds majority, or whatever number we
21 agree on, up front. And this still gives the
22 Commission the benefit of all of these ideas, yet it
23 gives the public and everybody the basic areas of
24 consensus.

25 It seems to me this would only require an

1 appropriate delegation of subgroup representatives to a
2 larger writing group, and would end up with something
3 which people could then easily vote on and say yes, I
4 approve, because, for example, we're explaining to
5 Ron's concern, and others, if I really hate this one,
6 pro this one, con, it's stated, not necessarily in the
7 written report, which may be inappropriate, but at
8 least somewhere else people can look at.

9 MR. MEDINE: Mary?

10 MS. CULNAN: I would just make one other
11 argument for this again, more on the lines of process
12 in terms of -- and I agree with Dan's point and people
13 should be able to I think indicate whether something is
14 a rock or a piece of gold, but this argument was made,
15 again, when we did the study last year, that when
16 people get to comment, it helps to create buy-in,
17 because they get to state their views, as opposed to
18 everybody voting and then going out and discrediting
19 various parts of the report in public or to the press,
20 and I just from a process point of view, I think it
21 would make things proceed much better.

22 And again, people feel they have a chance to
23 air their views and voice is very important. Without,
24 again, adding new options, it's just the idea of
25 talking about what's already there.

1 MR. MEDINE: Okay, I think we're at the point
2 now where we're going to -- I think we've aired our
3 views, and again this is your report, so when you
4 proceed to your subcommittees after this, you can craft
5 it the way you want to, we're not going to tell you how
6 to do it, you can make a decision.

7 Ron?

8 MR. PLESSER: There's no decision for
9 concurring reports or dissenting comments?

10 MR. MEDINE: This is your report, you will be
11 able to put in anything you want in the report,
12 including individual comments.

13 MR. PLESSER: But you're doing the calendar,
14 and if you're going to have dissenting report --
15 dissenting, there should be some provision for that,
16 and that's all the proposal is. I'm not -- I think
17 this conversation has gone far beyond, but you're going
18 to have some people who are going to vote against the
19 report that have 100 percent is not likely, some people
20 who are going to vote yes with conditions or
21 qualifications, and not to give that a voice, and not
22 to -- I mean, I'm going to look at the Advisory
23 Committee Act.

24 I can't imagine -- I just can't imagine that
25 you're really -- the intent of where you're going is

1 really where you wind up, because all we're -- all I'm
2 talking about here is a process so that if -- if
3 somebody has a dissenting view, that they have an
4 opportunity to voice it along with the report that they
5 were appointed to. I just -- you have that at the
6 Commission level.

7 MR. MEDINE: But again, there will be at least
8 two opportunities for that. The first opportunity will
9 be from the period of time from the 19th to the 24th
10 where you will comment on the draft report.

11 Again, I was going to suggest that we have a
12 couple of days after the meeting on the 28th where
13 people can submit additional comments for the report as
14 finalized and then have a final email vote on the final
15 report. And then so if the group is amenable to that,
16 there would be the opportunity from the 28th, and I'm
17 proposing -- I guess I'll propose until May 3rd to
18 submit final comments, either on the report or
19 additional statements, and then I would propose that a
20 vote commence -- that we have time, I guess, to
21 incorporate those, and that on the 5th we trigger an
22 email vote to conclude on close of business on the --
23 close of business on the 10th of May.

24 Yes, David?

25 MR. PLESSER: Can somebody retype the schedule

1 while we're sitting here? That would be great.

2 MR. MEDINE: That will be redistributed.

3 MR. DAVID HOFFMAN: David Hoffman from Intel.

4 It seems to me there's a lot of value at least in
5 having consensus come out at this meeting on at least
6 the shape of the report. Lance did put a proposal
7 together and I wonder if we could just take a quick
8 vote on that, if that being the direction we could
9 take.

10 MR. PLESSER: As a separate issue.

11 MR. MEDINE: Deirdre?

12 MS. MULLIGAN: I would like to respond to two
13 issues. Deirdre Mulligan. The first is, you know,
14 Ron, I completely agree with you to make sure it's
15 appropriate that everybody's views are expressed and I
16 think the only thing I am trying to emphasize is to the
17 extent that that can be done in the body of the report,
18 I think it will make the report a better document. I
19 think if we are, you know, that --

20 MR. PLESSER: You have that pledge?

21 MS. MULLIGAN: Yeah.

22 MR. MEDINE: I would also make it just a more
23 persuasive comprehensive document as opposed to having
24 to read 40 or 50 --

25 MR. PLESSER: If that doesn't work, you need a

1 safety valve, and I can't imagine no resistance.

2 MR. MEDINE: I think it would be more powerful,
3 having a comprehensive statement of the pros and
4 cons.

5 MS. MULLIGAN: I would like to propose that
6 since we are envisioning, it appears additional
7 appended comments, that we make a commitment right now
8 to say two pages, three pages, you know, I would like
9 to make sure that they are finite documents so that we
10 don't have an appendix that's longer than the report.

11 So, I would like to put on the table that maybe
12 we suggest -- I don't know, Dan, how many pages do you
13 think it would take you to get your views in, two,
14 three?

15 MR. GEER: I want -- let me be clear about
16 that, I want all of us to do that.

17 MS. MULLIGAN: Yeah, I hear you, but how many
18 pages do you think would work?

19 MR. LANE: I think it should be words, not
20 pages. Real small type.

21 MS. MULLIGAN: 250?

22 MR. GEER: I knew how to do that in high
23 school, right, 22 point fonts did a good job. Well, I
24 don't know how to answer that, Deirdre.

25 MS. MULLIGAN: Lance, you read papers.

1 MR. GEER: As a point of information, I would
2 ask that the comments that are being sought, are
3 themselves part of the public record.

4 MR. MEDINE: The comments of the committee
5 members?

6 MR. GEER: Yes.

7 MS. MULLIGAN: Of course.

8 MR. MEDINE: Everything is part of the public
9 record.

10 MR. GEER: So they will all be available in
11 some sense?

12 MR. MEDINE: They will all be incorporated into
13 the report that's sent to the Commission.

14 MR. GEER: And bits are free, so this is not a
15 question of length.

16 MR. MEDINE: You have to consider, again, that
17 the audience has to read the report and having --

18 MR. GEER: Well, those who are paid to read it,
19 have no sympathy. Those who are reading it out of fun,
20 who will we have left? I'm sorry, I'll shut up now.

21 MR. MEDINE: Lance?

22 MR. LANCE HOFFMAN: There is a solution to
23 this, I agree with you, pick a finite printed page
24 amount, like one page, 600 words in whatever type,
25 whatever you want. Those of us who have done this for

1 any time at all know you can always put a bunch of web
2 addresses in there to expand your comments if you want.

3 So, then it's only a matter of arguing about
4 what is the size you're going to limit people to, and
5 then you don't detract from the main report, you could
6 say here are these other things, and if you want to
7 hear more about my opinion or anybody else's opinion,
8 go read this website.

9 MR. GEER: Right, and you can log those.

10 MS. MULLIGAN: Mary, what did we decide on,
11 five or three?

12 MS. CULNAN: This reminds me a lot of teaching
13 and you have the same issues in the classroom and Lance
14 is nodding his head. A page limit, a font size,
15 margins that are appropriate to keep people from -- I
16 think two to three pages would be plenty and then
17 whatever the format specification is so somebody
18 doesn't have to re-edit everything in a standard what
19 it looks like at the top of the page and where your
20 name goes and whatever.

21 MS. MULLIGAN: There we go, two or three pages,
22 and the question on the format of the report, I
23 actually agree with David that we think about format
24 but I propose that we do that at the end after having a
25 sense of going through the documents what format makes

1 sense. Lance's format sounds attractive to me, but I
2 think we might want to think about it at the end of the
3 day.

4 MS. CULNAN: I think to make the work easier
5 for Deirdre and the rest of the people who are going to
6 put this all together is to publish the format so again
7 it does look nice, even when you change the title of
8 these things when you have 40 of them gets to be a real
9 hassle.

10 MR. MEDINE: The question is do we want to put
11 Lance's -- I'm hearing a suggestion that we may defer
12 Lance's specific recommendation, I don't know, you mean
13 until the end of today or defer it until the next
14 meeting?

15 MS. MULLIGAN: To the end of today.

16 MR. MEDINE: Do people want to move or make a
17 motion?

18 Larry?

19 MR. PONEMON: I'm sorry, was this a motion here
20 that you're making?

21 MR. MEDINE: I don't make motions, but I can
22 invite a motion.

23 MR. PONEMON: I have something to say.

24 MR. MEDINE: The question is whether the group
25 wants to have a motion at this point or defer a

1 decision until later.

2 MR. PLESSER: Lance, does it ought to have a
3 comment?

4 MR. TORRES: I make a motion to defer a comment
5 until then.

6 MR. LANCE HOFFMAN: Lance Hoffman, it's always
7 good to defer binding time as a programmer, maybe as a
8 lawyer, too, I don't know.

9 MR. MEDINE: Larry?

10 MR. PONEMON: Larry Ponemon,
11 PricewaterhouseCoopers. I'm actually pretty concerned
12 that maybe process and form is killing our ability to
13 make an intellectual contribution. I know it's very
14 difficult because this is a citizens group and, you
15 know, we all have -- we all do other things in our
16 lives, and a lot of us have worked very, very hard to
17 kind of get our viewpoint in the report, but I also
18 think we're missing some critical elements.

19 I'm not sure if you asked most of the people in
20 this room whether their full point of view, their full
21 intellectual contribution is reflected here, so is
22 there any opportunity in the next couple of weeks for
23 us to say now what's missing? What are the bigger
24 issues that I can incorporate?

25 MR. MEDINE: I think again you have the

1 opportunity both as the subgroups reconvene to draft a
2 report and then that if you're not on a particular
3 subgroup, you have that opportunity either immediately
4 to let that subgroup know your views or most certainly
5 during the period again between the 19th and the 24th
6 to express your views and then even if then they're not
7 expressed, you have the period as we're proposing from
8 the 28th to the 3rd of May to express your views.

9 So, there are really three opportunities that
10 you have to make sure that your views are fully
11 represented in the report.

12 Let me also just note some recent arrivals,
13 including Larry Ponemon. Josh Isay is here?

14 MR. KAMP: Yes, he's here.

15 MR. MEDINE: Richard Bates is here. Jonathan
16 Smith is here. Richard Smith is here. Okay, just to
17 keep up.

18 Okay, I guess I would propose that we perhaps
19 move into the substance of the discussion, unless
20 people -- yes?

21 MR. KIRKPATRICK: Can I make a comment?

22 MR. MEDINE: We have one more. Yes, Roger?

23 MR. KIRKPATRICK: I just wanted to make a
24 comment about the role of pros and cons and it seems to
25 me that being viewed in contradictory ways based on the

1 comments that I have heard.

2 One role is that there's a way for people to
3 express different opinions, but they're not just that,
4 and then it seems to me that the Commission would be
5 losing a lot of nuance if that's all they became,
6 because even, I think, as Rick indicated, a half hour
7 ago, people who -- even people who agreed on the
8 overall conclusion of a particular proposal, can also
9 agree that the cons are important, and especially in
10 this committee, it seems to me that inherently we have
11 absolute conflict between access and security. They
12 just conflict, completely.

13 So, it seems to me that it would be if at all
14 possible, extremely useful for the Commission to get
15 the committee's sense on the extent to which the cons
16 reflect this agreement, or the extent to which they
17 actually reflect agreement from the committee on the
18 price to be paid for some of the proposals.

19 MR. GEER: Hear-hear.

20 MR. MEDINE: Again, I'm going to suggest we
21 move on to the substance and keep these things in mind
22 and revisit perhaps at the end of the day. Maybe from
23 Lance or somebody else about any particulars, and if
24 we're in agreement on that, why don't we move into the
25 access I group's efforts, which is the degree of access

1 in terms of the condition of access, and the group,
2 again, has done an excellent job in laying out a series
3 of options for the approach to access, including the
4 focus on categories, types of uses, complete access,
5 and I guess I would be happy to entertain a particular
6 discussion on this, or suggest is there a way to
7 simplify the approach suggested again in an operational
8 sense so that the person who has to implement this has
9 a clearer idea about how they go about making access
10 decisions?

11 But I'm also happy if we want to delve into the
12 particular categories of information, if that would be
13 helpful to try to flesh out when access -- people have
14 access is appropriate or not and there's a split
15 between access to personally identifiable information and
16 not personally identifiable information, drive
17 information, transaction, upstream.

18 I don't know if anyone wants to -- Dan?

19 MR. SCHUTZER: I found some of the categories
20 confusing and overlapping, so I would like to just
21 discuss what confused me. When I looked at
22 non-personally identifiable information and
23 non-personally identifiable information linked to
24 personally identifiable information, for example, I got
25 a little bit confused with that, because all

1 non-personally identifiable information could be
2 linked, it all depends upon how you do it and where.

3 So, I started thinking maybe of a different
4 distinction that might be helpful to you.
5 Non-personally identifiable information that couldn't
6 be linked is perhaps information where the information
7 stored only is an aggregate, that could be information
8 that you could never link back or anonymous data would
9 be information to which I could never link back, but
10 anything else, I mean hair color, click behavior and so
11 forth, could be linked back, and therefore as far as I
12 would be concerned, it should be -- if it could, it
13 should be treated as such.

14 MR. MEDINE: So, just a distinction from that,
15 to state further, then, if it's linkable, but not
16 currently linked, would you then suggest that the
17 subject of the data ought to have access to it, and if
18 so, how does that play with the fact --

19 MR. SCHUTZER: I'm not talking about the
20 recommendations yet, they all have pros and cons and
21 everything, so the clearer way of stating that is that
22 information could never be linked to identity to
23 information that is necessarily behavioral, not
24 necessarily linked to identity, but it could be.

25 MR. MEDINE: So, really create three

1 categories, personal identifiable, impossible to
2 identify and then --

3 MR. SCHUTZER: It's either how you link the
4 personally identifiable information or can't be, as far
5 as we can see.

6 MR. MEDINE: Okay.

7 MR. SCHUTZER: The next thing with the
8 interactive as opposed to the transactional. Interactive
9 can use transactional information. I don't see much of
10 a distinction there.

11 So, the distinction I think I was seeing being
12 drawn out there was account based versus non-account
13 based. Because there is something fundamentally
14 different between account based versus a non-account
15 based.

16 So, if I have an account with somebody then I'm
17 actually most likely going to be storing information
18 about that, maintaining a relationship, if I have a
19 non-account based, I still may store information for
20 the duration of the session, but I won't necessarily be
21 expected to want to maintain that information.
22 Somebody who comes and visits me, but they don't stay
23 with me. So, -- but I still might have identifiable
24 information.

25 For example, I could be a web merchant, a web

1 service provider, I see an email, yes, they have an
2 account with an ISP but they don't have an account with
3 me. They come visit for the purpose of that
4 interaction of storing information to try to customize
5 it during that whole session, I don't maintain that
6 information so it's unreasonable to necessarily ask me to
7 provide it back, so I think a better statement might
8 just be account based versus not account based.

9 And computer information, I mean that's -- all
10 the stuff is computer information, if it wasn't on the
11 computer, we weren't storing it, you can't make it
12 accessible. So, I would submit to not even bother with
13 that. Navigational or click stream data is, again,
14 transactional data. It's just not necessarily identity
15 linked information, but it could very well be identity
16 linked information. And derived data I think is an
17 important distinction, because we all have to talk
18 about derived data, there's lots of complex issues from
19 derived data leading to proprietary models and the like, so
20 I recommend keeping that one, I understand that one.

21 And then all the other ones get a bit confused
22 to me also in terms of distribution, PII, but let's
23 say, I think, the only thing I can draw out of that
24 next set of categories is that if we're talking about
25 merging the identifiable data that we're collecting

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 online and keeping online databases with let's say
2 other information we may have access to that is
3 fundamentally offline, you know, stored on tapes or
4 other kind of data, that may be complex for not
5 maintaining it online to make it readily accessible.
6 So, that's probably worth some distinction.

7 MR. MEDINE: Lance? Okay, first Lance and then
8 Richard.

9 MR. LANCE HOFFMAN: I'm sorry.

10 MR. MEDINE: Oh, you're not up. Richard?

11 MR. PURCELL: Just to respond directly to your
12 inquiries, the first two categories of non-PII and
13 non-PII linked to PII, explicitly talks to the
14 distinction you're trying to make. We considered
15 non-PII to be that data which is not or could not be
16 linked to personally identifiable information. It
17 exists as an anonymous blob, if you will, or set of
18 data. To the degree that that data has linkage to
19 personally identifiable data, it then is characterized
20 differently because it becomes incorporated into the
21 set of PII.

22 So, I don't know that the distinction -- I'm
23 not clear that this distinction is not clear, I guess,
24 is what I would like to say.

25 MR. MEDINE: Can I just clarify that in again,

1 what about the potential of linkage? I mean there is
2 data that is maintained in aggregate form that
3 essentially can't be reversed back to an individual,
4 then there's data that's maintained in separate form,
5 but not identifiable to a particular individual that
6 could be identified to a particular individual, like
7 account-based information.

8 MR. PURCELL: Then it's linked.

9 MR. MEDINE: Okay.

10 MR. PURCELL: If you have a master key that
11 says Richard Purcell's key to his PII is this, and the
12 same key to a bunch of click stream data, then that
13 click stream data is no longer PII data, it is linked.
14 Whether you've done the linkage or not, it is linked,
15 because you have a master key.

16 We have to be careful to distinguish database
17 terms from behavioral terms. A master key links data.
18 Whether you have actually taken the action of doing
19 that linkage is immaterial to the fact that a key
20 exists.

21 MR. SCHUTZER: So, if you're profiling an
22 individual as opposed to an aggregate group, for
23 example, then it's linked to you?

24 MR. PURCELL: Well, it depends entirely on
25 whether or not the keys that you use to identify

1 personally identifiable records are used in the
2 aggregated data as well. In order to unlink those two,
3 you actually have to destroy or rewrite the keys in the
4 non-PII data set and make them so that they can't ever
5 be restored to that original PII data.

6 In the account and transactional data --

7 MR. JAYE: Richard, before we move on.

8 MR. MEDINE: That's Dan Jaye.

9 MR. JAYE: Daniel Jaye. Just one point. I
10 think that David's question was inherently if you have
11 a unique number, is that by definition linked to PII?

12 MR. PURCELL: Yes. It would be.

13 MR. JAYE: Any unique number?

14 MR. PURCELL: No, if the unique number is used
15 in the PII set to identify that.

16 MR. JAYE: Yes, that's --

17 MR. PURCELL: And is the same master key that
18 is linked -- that identifies the non-PII --

19 MR. JAYE: But if you just have -- if there is
20 no PII, and you just have a unique number.

21 MR. PURCELL: No.

22 MR. JAYE: Then it is not by definition linked?
23 I just want to clarify that.

24 MR. PURCELL: Yeah, by no means. There's non
25 and there's PII. On the account based transactional

1 data, there is a distinction that says this is a subset
2 of transactional data. I don't want to be confused.
3 We did break out the two sets. But we intended account and
4 transactional or interactive data to be contained
5 within the same definitional set.

6 Computer information isn't the computer
7 information on the server, it's not your PII, it's not
8 -- it's specifically identified -- identifies the
9 users, the data subjects, computer hardware platform
10 that can be discovered through tunneling kinds of
11 protocols. So, often times that's disguised.

12 MR. MEDINE: That's information about the
13 computer, not computer information?

14 MR. PURCELL: About the computer that the user
15 is learning -- is using that is typically not
16 explicitly presented by the user, but is presented by
17 the computer.

18 MR. SCHUTZER: That indeed can link them in
19 that case?

20 MR. PURCELL: Oh, absolutely.

21 MR. WHAM: Not necessarily.

22 MR. PURCELL: Absolutely, but not necessarily.
23 The potential exists. And again we get back to whether
24 a master key has been issued that links all of this
25 data together. Navigational and click stream data is

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 undoubtedly a subset to the discussion we've just had
2 about non-PII and PII data. The dependency is whether
3 a master key, a primary key, has been issued that links
4 this data to the personally identifiable data. The
5 best way to get out of this discussion is to master
6 your personally identifiable data in a manner different
7 and irresolvably different from the non-PII data. If
8 you would choose to do that.

9 Finally, the PII merged from other databases
10 indicates data that is linked through whatever access
11 point you have from other sources. So, to the degree
12 that my online database receives not only interaction
13 from users online, but also takes data from other
14 sources and incorporates that into this data, again the
15 key discussion, then that data has to be addressed as
16 being one of the points -- one of the discussion points
17 around whether access should be provided.

18 So, if I have a system of -- where my, you
19 know, my -- a customer support center takes telephone
20 calls and I batch copy all of that stuff and put it
21 into my online database and link it to records by that
22 manner, that's what's indicated by here. And it could
23 be from third party, it could be from internal sources,
24 it simply means the data that's brought from other
25 systems and merged into the online identity data. I

1 think those are the points I wanted to make.

2 MR. MEDINE: Thank you. I think it's helpful
3 to clarify, I hope we'll then come to the question of
4 so what in the sense of how do we treat each of these,
5 now that we understand it, what are the access
6 implications and is this a useful method of
7 distinguishing.

8 Deirdre?

9 MS. MULLIGAN: Yeah. There are two things that
10 struck me. First, it was very interesting that there's
11 no discussion, you used all the categories, except for
12 globally unique identifier attached to data or locally
13 unique identifier attached to data, and that was kind
14 of surprising because that, in fact, I think has been
15 the flash point in defining what is PII versus non-PII,
16 and so the absence of that, I was wondering if you
17 could talk about why that isn't discussed.

18 And I think that in order to move the
19 discussion forward, we've all been kind of tap dancing
20 around the question of what does it mean for
21 information to be identified to an individual. Does it
22 mean that you have the name and address or does it mean
23 that you're tying data and making decisions about them
24 based on that data? And those are two very different
25 pictures of whether or not data is identifiable. And I

1 -- we've skirted around that enough and I think that's
2 what we have to address.

3 MR. MEDINE: Lorrie?

4 MS. CRANOR: Yeah, back to the question --

5 MR. MEDINE: Can you speak into a microphone,
6 please?

7 MS. CRANOR: Thanks, Lorrie Cranor. To the
8 question of linked data, I also wanted to point out
9 that even if you don't have a key, data can still be
10 linked. For example, if you have somebody's zip code
11 and date of birth, 95 or 90 times, some very large
12 percentage of people are uniquely identified that way.
13 So, I think just saying that it's tied to a key may not
14 be enough.

15 Now, we may say that that's good enough and say
16 for our definition, that's what we want to use, but I
17 think we should be very clear that that's a line in the
18 sand that we have drawn and that doesn't necessarily
19 mean that there isn't other data that could be linked
20 to an individual.

21 MR. MEDINE: Ron?

22 MR. PLESSER: Yes, one of the models that went
23 around in my mind when Richard gave his review was I
24 think in light of the health care industry where
25 there's a trusted third party holding the key,

1 particularly on longevity studies and things like that,
2 there's a third party that could get the various
3 information together, and then gives it a unique
4 identifier, but that -- and then would supply it to
5 somebody who then uses it. The company who uses it
6 can't identify who the person is.

7 We're not -- we're not -- I mean I want to be
8 careful that we're not saying that party -- maybe this
9 gets back to the entity discussion -- but that that
10 party has an access requirement, because then you're
11 essentially breaking apart a trusted key system. And I
12 don't think there's, you know, it's again one of these
13 areas where in this sea of searching for access, you're
14 really going to force propagation. So, I think we
15 ought to be very careful that making these lines will not
16 destroy your system where you can have some longevity
17 information, longevity studies, but linked through a
18 trusted key that the user really can't break through,
19 and so I just hope we do it -- we talk about the key
20 being held by different people, it's whether or not the
21 person who has the record can provide -- identify and
22 provide the records, not that there's a key existing.

23 MR. PURCELL: Absolutely.

24 MR. MEDINE: We have three Daniels with flags
25 up. So we'll start here, here and there.

1 MR. SCHUTZER: I would like to address the so
2 what. When I read this report, what I sensed was that
3 -- which I agree with, that you have to look at this by
4 many different dimensions, and what we've been talking
5 about so far is one of the dimensions you bring to
6 bear. So, for this particular dimension, you know, I
7 would say to myself, so why do I make these
8 distinctions, I'm trying to make these distinctions to
9 provide options as to what data I might need to make
10 accessible to an individual or not.

11 And so it seemed to me that there's only three
12 things I care about. One is if I have aggregated the
13 information in a way so it's not tied to an individual
14 profile, in any way whatsoever, or it's totally
15 anonymous, then don't expect me to provide access to
16 the day that to an individual, there's no way I can,
17 okay?

18 The other thing is that if it's not stored
19 online, in a way that's reasonable to expect me to
20 provide access, and I'm not maintaining it, other than
21 transitory, don't expect me to access it, it's not
22 reasonable, practical for me to do that.

23 Now, there's many other aspects that you get
24 into later on, the use and the nature of the data and
25 the sensitivity and some data like financial data, is

1 there any slapped on with lots of regulations and so
2 forth and is treated differently, and I agree with all
3 those other distinctions that you touched on, other
4 dimensions, but I'm just trying to cut loose for more
5 simplicity in terms of do we really need all these
6 categories for that one dimension?

7 MR. MEDINE: Daniel Geer?

8 MR. GEER: Yes, as a point of information
9 question, were you in this discussion explicitly
10 treating data fusion as a risk management problem? Is
11 that the core of this?

12 MR. PURCELL: Richard Purcell. No, Dan, I
13 couldn't say that that was the core of this. The
14 purpose here was to generate the kind of discussion
15 we're having today. We felt that what we wanted to do
16 was try and provoke as much discussion across as broad
17 a range of issues, so we didn't want to actually
18 establish a core issue, we wanted to establish as many
19 -- a broad platform of issues that require resolution
20 because this then becomes -- I mean we only have six
21 weeks to run, so we wanted to get as much on the table
22 at this meeting as we possibly could.

23 MR. GEER: I understand that, though forgive
24 this. When you don't know where you're going, any
25 direction will do. The risk management question, which

1 I think is what is at the core of the entire privacy
2 discussion, in turn requires us to think of well, what
3 are the risks?

4 MR. PURCELL: Um-hmm.

5 MR. GEER: And I would bet we have some measure
6 of consensus on the question of fusion, and I think
7 you're speaking to that here. I mean many of these
8 things here are about if you fuse this, if you fuse
9 that, if you fuse the other, recognizing, of course,
10 that the cost of fusion is near zero these days, that
11 there is absolutely no restraint on fusing data other
12 than the good will and taste of those who would
13 otherwise do it, and the world is full of people with
14 no good will or good taste.

15 Hence, my question is if that is the core idea,
16 if data fusion is the core idea, which I submit spoken
17 or not, it is as I read this document, then in turn, I
18 ask, what can we do to make that less? And because I
19 read nothing here about the value of pseudonymity whose
20 sole purpose is to throw off those who would follow, I
21 wonder whether this goes far enough.

22 That's what I'm getting at. You know, there's
23 nothing here about creating costs to the fuser, and the
24 only cost I can think of as a procedural issue is
25 pseudonymity for the purpose of misrepresenting

1 yourself so as to avoid the fusion. I think the logic
2 leads that way, and without knowing what the problem is I'm
3 trying to solve, it's hard to evaluate the mechanisms.

4 MR. PURCELL: Well, again, Richard Purcell in
5 response. Dan, what we tried to do is here to layout a
6 road map of pros and cons around each of these that a
7 careful reading of which none of us have probably had
8 an opportunity to take, does lead to increased risk
9 management issues as more and more data is mastered in
10 that central manner. And a decrease in the -- as data
11 is broken up into discreet usable sets, but sets that
12 cannot be restored into any master.

13 An example, click stream data is interesting
14 data, it's even used for aggregate analysis. To the
15 degree that's an exclusive use, there's no need to
16 identify that data in a linked manner to personally
17 identifiable data. And that delinking which often
18 takes the data step that says take this key and garble
19 this key or destroy this key in some manner or other,
20 you know, put them -- create a unique key within this
21 data set, but have it completely disable the ability to
22 link it back to the origin, then allows one to say this
23 is an analytical set, it's non-PII, it's not -- and as
24 such, I'm, you know, I can do a lot with this, but I
25 have reduced my risk because I can't necessarily point

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 any result of my analysis back to any known individual.
2 So, your risk is reduced in doing that.

3 Now, that does not help somebody who wants to
4 create user profiles that from that data that are
5 identifiable and can -- and the result of which can
6 produce more targeted advertising, or messaging or that
7 back to a known individual. But that decision made,
8 you have an increased risk, because what we're saying
9 here is that one of the issues is that that becomes
10 personally identifiable data through that linkage. So,
11 your risk does increase, certainly.

12 MR. MEDINE: Daniel, can I just ask a question
13 to follow up on your point which is another cost or
14 degree of ability of access to the fused data, so
15 therefore that the fuser has to be comfortable letting
16 the data subjects know that their data has been fused
17 and be comfortable with whatever steps have been taken
18 with the data?

19 MR. GEER: Fair enough. Because I work in the
20 security field, I tend to assume that all systems break
21 under some degree of strain. And the difficulty, of
22 course, being that data is never unrevealed. Hence the
23 question of for those things for which there is no
24 protection after the fact, one either prevents in
25 advance or one sets some high bar. I don't believe

1 it's possible to prevent aggregating some kinds of
2 data. I don't think it's possible. The more it is
3 aggregated, the more it is an attractive target, hence
4 the more -- the more attractive target draws more
5 attacks by definition.

6 Hence, my question about fusing, I think gets
7 to the heart of where the risk is, because in the act
8 of fusing, you create the target. And there's no way
9 around that. I believe this is a fact of nature, I
10 don't believe it's a matter of observation or opinion.
11 The more that it is concentrated, the more it is the
12 object of attack. Hence the higher walls you have to
13 put around it, and pretty soon you get a culture of
14 identity surveillance, and that's not where I suspect
15 any of us want to go.

16 MR. MEDINE: Daniel Jaye, the third Daniel.

17 MR. JAYE: Thank you. I just wanted to clarify
18 my understanding here that -- and people talked about
19 dimensions here, that fundamentally, it seems like we
20 have two dimensions here in the categories, one which
21 is whether something is non-PII, non-PII linked to PII,
22 and PII, and then the other dimension is specifically
23 then dividing up the different categories of data. I
24 just want to clarify that.

25 That was deliberately the approach or

1 accidentally the approach? Because obviously almost
2 any type of information here, I mean there's some types
3 that are inherently PII, but almost any type of
4 information here could be non-PII in a certain
5 circumstance, if you look at the categories on page 2
6 of our printout, pages 2 and 3 and 4 of our printout.

7 MR. PURCELL: Yes, that's correct. There is --

8 MR. JAYE: And the follow-on to that is just on
9 this issue of the handling of data and keys and data at
10 a summary level and data at individual level. We do
11 need to understand that there are different
12 implications of each of these data levels of data with
13 regard to access, but how it's processed, it -- you
14 know, this comment is just in general on the category
15 approach, the category approach I think has a lot -- a
16 lot of merits in some cases, but once again, I do think
17 that use is an extremely important dimension to
18 consider in combination with the categories.

19 MR. MEDINE: Greg, then Deirdre?

20 MR. MILLER: I am going to yield my time to
21 Deirdre because I think we want to make the same comment.

22 MS. MULLIGAN: Actually I think it makes sense
23 for you to make part of the comment. We have a cabal
24 over here.

25 MR. MILLER: We are obviously in heated

1 agreement about our caucus. Well, I'll just -- one of
2 the things I'm concerned about, Greg Miller,
3 MedicalLogic, is that as we know in both financial data
4 and health care data, there are regulations pending
5 already in other agencies to directly address these
6 matters, and the one thing I'm concerned about is
7 thinking about IDs and how -- what you can and can't do
8 with them.

9 For example, master patient index ID, protected
10 health care information versus non-protected health
11 care information. So, we're in a slippery slope here
12 and I just think we need to be mindful of what's
13 happening collaterally around us.

14 MR. MEDINE: Deirdre?

15 MS. MULLIGAN: Okay, I'm going to go back to
16 this issue that I can tell nobody wants to deal with,
17 which is what is non-PII versus PII, and what is the
18 scope of access, which I think underlies this whole
19 discussion. I think, you know, the statements that
20 we've heard around the table say well, non-PII, of
21 course I can't provide access to it, because there's no
22 way for me to authenticate, right? At least that's
23 been part of the -- I don't know who you are, therefore
24 I can't provide access to you.

25 And I think the "I don't know who you are part"

1 is where we're stuck. And I think if when we get to
2 the authentication discussion later, which I had the
3 privilege of working on that particular subcommittee,
4 what we found is that yes, there are streams of data
5 that are specifically connected to my name and address
6 and other things that everyone around this table would
7 say yes, that's identification information. We can
8 provide access to.

9 We've also found that there is data that is
10 account based that may not be identity based, but is
11 clearly account based, so the establishment of a
12 pseudonym, an anonymous email address, perhaps some
13 other tag that identifies a specific user, and that, in
14 fact, you can provide access to that data because it's
15 a longitudinally maintained file, and the question is
16 what is the appropriate level of authentication to make
17 sure that you're not providing access to the wrong
18 person.

19 So, you know, I think that this is the
20 important question, and this is where we get to: is a
21 unique identifier absent a name and address and phone
22 number, something that is identifiable or not? And I
23 want to kind of force this issue again because I think
24 it informs our discussion. So, I'm looking for some
25 more discussion on that issue.

1 MR. MEDINE: Then can I just ask you a further
2 clarification on that point? Because -- and it's
3 raised in the outline, is what about non-PII that's not
4 linkable to an individual but say to a computer that
5 could be used by multiple individuals? Is that a
6 situation where you would say no access because by
7 providing access you are essentially getting
8 information about other individuals or do you provide
9 access because there is a file or there is a profile
10 that links that computer, which clearly can be attained
11 and provided to the requestor?

12 MS. MULLIGAN: I think it's an important issue,
13 and part of that turns, if you look at, for example, in
14 the U.S., I have a telephone number, I happen to share
15 my phone with another person. I do get access to all
16 of the numbers dialed from that phone that are long
17 distance, despite the fact that that unique identifier
18 is not unique to me. It is still, in my opinion,
19 identifiable information, because it's identified to
20 me, but it's actually identified to two people.

21 In the U.S. in the phone context, we tolerate
22 that level of family disclosure of data in the
23 telephone context. Now, we can also say the telephone
24 numbers that I'm dialing are probably less revealing
25 than a URL or some other data that might be far more,

1 you know, nice and fuzzy. And so but if you look at
2 France, France actually doesn't tolerate that, they
3 don't want the numbers disclosed, you know, the family
4 doesn't have the right to know what the individual --
5 who the individual is calling, right?

6 So, I think that we have to think about that
7 question and I think for me, when you get to the --
8 this information is being used in a way to make
9 decisions about me. For example, while it may be
10 attached to the computer, my guess is that my
11 experience is still being influenced based on all of
12 that data, despite the fact that some of it is
13 inappropriately tied to me. Because it was actually
14 Greg using my computer, right?

15 So, I mean if that particular issue works in
16 both directions, and I don't think that the answer is
17 well, no, there's no access here, you know, blanketly,
18 because the risk is too great. I think we have to
19 discuss it. I don't think it's an open and shut case.

20 MR. MEDINE: Andrew, Ron and then Dan.

21 MR. SHEN: I agree with Deirdre and Dan that we
22 really need to discuss these issues about, you know,
23 very crucial definitions like non-PII and PII, but I
24 would also like to address a couple of broader issues
25 that I don't think were discussed in either of the

1 access outlines.

2 I think the first is enforcement. In the
3 security group at least, we considered this to be one of
4 the critical things that we should discuss. You know,
5 hopefully we come up with a number of serious options,
6 but unfortunately to get to the next step, we need to
7 decide how to implement those. I don't think I really
8 have a final answer on that. Maybe the final answer I
9 would prefer most people would disagree with. I think
10 that should be discussed in this outline.

11 The second issue is I think we really need to
12 go back and find out why is access so important. Why
13 is access so important? It's important for privacy. I
14 think the Federal Trade Commission fair information
15 practices of notice, consent, access and security, I think
16 those sort of limited articulation of fairness in
17 practices makes access do more work than it does in
18 other systems.

19 I think where there's no data use information,
20 there's no integrity relevant to principle, I think
21 access is more important in this limited rubric, less
22 we use access just to find out what companies have on
23 you. Not that it's accurate, but just find out the
24 full extent of what those companies have, the full
25 access to various data.

1 MR. MEDINE: Ron?

2 MR. PLESSER: I would break a little bit from
3 the PII/non-PII subject, but more in what Andrew said,
4 talk about the outline a little bit. I think A, B and
5 C were really quite well done, and I think they -- the
6 definition, and then the B and C choices, which were
7 really the fundamental choices, it seems to me, do you
8 have overall policy based on categories of access or is
9 it to all, and so I really like the progression of the
10 outline to that point, but then the outline seems to me
11 to go -- just go into 100 different directions, and one
12 of the questions as I think Andrew, you know, we may
13 disagree about it, but why is the relevancy issue in
14 here?

15 I just -- I first of all it just rings untrue
16 in terms of the outline, it's a wrong turn, and, you
17 know, if it's going to be handled, to be handled in a
18 different way, but I'm very unclear as to why, you
19 know, limitation on collection is in this -- in the
20 purview of our scope. I think that, you know, I just
21 don't think it is. And so I was surprised to see it.

22 The data retention issue, I don't feel quite
23 the same way, because I think data retention at least I
24 don't think access should drive data retention
25 policies, however I certainly understand that if you

1 destroy documents every five days, I mean I think
2 there's an issue that if you, you know, destroy
3 documents upon the receipt of a request, that that's
4 wrong.

5 So, I think data retention and the fair
6 practices approach in connection with access should be
7 here, but I'm not sure that this should drive an
8 overall data retention policy which it seems to me is
9 based on a lot of different issues.

10 Then the outline goes into access depending
11 upon use or purposes, and I -- it just doesn't make --
12 that I don't disagree with substantively, but I just
13 don't understand how it works in the outline. If you
14 already have your basic choices on categories, is this
15 now a matrix on top of that, and if so, how do we -- I
16 think we have to express that matrix in a more -- in a
17 clearer tree approach that okay, we're going to go in
18 categories against all, and then we're going to go to a
19 purposes or use.

20 Having experience in the Fair Credit Reporting
21 Act, I would rather go more to the categories of
22 information than the purposes of use, because I think
23 that creates a lot of problems, it's, you know, and it
24 becomes much more subjective, but I'm willing to have
25 it considered, but it just isn't -- it doesn't make

1 sense to me the way it's presented in the outline.

2 And then I think, you know, we could go on, but
3 I think the outline has to be broken up and clarified,
4 but the major concern I have, and Richard maybe you
5 have an answer, is why are some of these extraneous
6 things in here. At least in my view.

7 MR. PURCELL: As all of our subgroups probably
8 have realized, committee writing is a delicate art.
9 And, you know, I should and have and I'm remiss in not
10 commending Lieutenant Governor Jane Swift's office for
11 actually driving our subgroup during this process.
12 Jane is represented by David Veator today. These guys
13 did yeoman's work in taking an awful lot of information
14 that we were throwing at them in perhaps a random
15 fashion, and trying to digest it and put it into a
16 format that's digestible.

17 I think that what you're seeing here, Ron, more
18 than anything else, is a bunch of people who know too
19 much trying to tell a bunch of people who are not
20 intimately involved in the subject, and them doing the
21 best job that they're able to to hang it on a framework
22 that at least gets it on the table, if not elegantly,
23 at least in -- it displays --

24 MR. PLESSER: No, no, no, I think it's terrific
25 to see, but I think the first half of it is really very

1 fine. I think the question -- I think the purpose of
2 this conversation is to then kind of come up with the
3 logic that we're going to use it with.

4 MR. PURCELL: Yes.

5 MR. PLESSER: And I would like to see a logic
6 that was more decision tree than the outline.

7 MR. PURCELL: I think we all would.

8 MR. MEDINE: And again I think that categories
9 should drive the agenda or uses should drive the agenda
10 or both, but I think you should think about the
11 overlap that the website operator has to do at the end
12 of the day and obviously for the Commission to
13 interpret your conceptions, I think again how do you
14 put this into practice.

15 Frank?

16 MR. TORRES: Just a couple of comments. On the
17 categories of personal information, I think it's
18 important to be broader than less broad in this area,
19 because it's very informative, I think, for the
20 consumer to know how information is being collected and
21 what type of information is being collected about him
22 or her, or that's kind of out there or available, or
23 kind of open to collection, whether or not it's PII or
24 non-PII. At least in the first cut. That if you're
25 going to take it and aggregate it, shouldn't I be at

1 least able to know that that's what you're doing with
2 my information at the point that you're collecting it.

3 So, that brings me to my second point, which is
4 I think what's missing from some of our discussion is
5 the role of notice in some of this, which might help in
6 is something retained, not retained, how long is it
7 retained. I hate to see retention used to skirt -- to
8 skirt some of where consumers should get access to
9 data.

10 Oh, you know, the minute you request access to
11 data, all of a sudden it's erased from the system or
12 all of a sudden made non-PII so then if we choose to
13 make non-PII information nonaccessible, then, you know,
14 can you throw a switch and then move the information
15 back and forth into different realms to get out of
16 providing access.

17 And finally, I appreciated also the discussion
18 of use, and I think that's important, but maybe if we
19 are trying to simplify things, should it be not how the
20 information is being used, that's maybe not that
21 important, but the fact that the information is going
22 to be used for something. Why else are you collecting
23 it if you're not going to use it for a purpose, and if
24 you're using it for a purpose, then you're accessing it
25 for a reason, why can't that be the driving force for

1 saying well, if somebody is using it or accessing it,
2 then the consumer should get that same or similar
3 access to it.

4 MR. MEDINE: Jonathan?

5 MR. JONATHAN SMITH: Jonathan Smith, University
6 of Pennsylvania. I want to amplify a comment by Dan
7 Geer that I think is actually very deep and really not
8 addressed and should be, which is the role of active
9 countermeasures. I don't mean to go off on a complete
10 blue sky tangent here, but in fact, I mean one of the
11 key issues in preventing use of data is contaminating
12 it.

13 Or, for example, you know, thinking about many
14 ways that people in real life will take to mask their
15 privacy, and I mean we have not addressed that at all.
16 And I mean I don't -- I believe that probably belongs
17 in the access component of our analysis, because what
18 it essentially is doing, is, you know, making the
19 access futile.

20 So, it's a -- it's an active countermeasure
21 type technique, if you want to talk about it in terms
22 of information systems, but I really think we haven't
23 addressed that at all, and that's part of what I think
24 Larry Ponemon tried to bring up earlier is that, you
25 know, there's kind of some intellectual holes in what

1 we're -- in what we're doing that at least to some of
2 us are a concern.

3 MR. MEDINE: And again I would invite you to
4 submit your views on those and fill those holes and
5 that's the purpose of the discussion. Steve?

6 MR. COLE: Yeah, I would like to make a general
7 observation about personally identifiable information.
8 And the conversation proves to me that Deirdre is
9 absolutely right, that we really don't want to talk
10 about that yet, but I know that she's going to succeed,
11 so I want to make this general observation. We're a
12 group talking about access and security, and that
13 raises all sorts of important questions about
14 authentication and those came up earlier, but I just
15 hope we bear in mind that conceptions and definitions
16 of PII are going to govern more for the online
17 community than just the access and security issues.
18 The underpinnings of notice of what's collected and how
19 it's going to be used and choice and options and out
20 there is a whole underpinning of what policies and
21 procedures are about, is going to be dependent upon how
22 personally identifiable information is used. And it is
23 not clear to me that the complicated issues of access
24 and security should solely drive that -- the answers to
25 those questions. I don't have answers, but I'm worried

1 that we're -- the complications here may actually be
2 counterproductive to the openness and transparency
3 we're trying to create on the other side of the issues.

4 MR. MEDINE: Deirdre, do you want to respond to
5 that?

6 MS. MULLIGAN: If I could. I think I
7 completely agree with you, and what I would suggest, I
8 mean in thinking about this discussion, I would
9 actually start it from the other end, and say okay, I
10 have data about an account, I have data about an
11 individual, I have data. Could I provide access to
12 somebody who presented me with the token, whether it's
13 their name, or their email address or their cookie,
14 could I provide access?

15 Okay, that's the first question. Can you do
16 it? If the answer is, you know, no, because it's all
17 over the place, I'm not actually connecting it to a
18 single identifier, I could not. Okay, well, guess
19 what, go home, you can leave now. But if the answer is
20 yes, I could, then we get to the questions of well, are
21 there risks to providing that access, because we may
22 provide it to the wrong person? Are there costs to
23 providing that access that we have to think about,
24 because they may be, you know, burdens that the market
25 won't bear. And then what are the interests that that

1 access would serve?

2 And so, you know, my -- my preference would
3 actually be to start from the what can we provide
4 access to question, and then think about of the scope
5 of things that we can provide access to, what does this
6 group think it's appropriate to provide access to. And
7 that gets us out of the is it PII or not, and probably
8 into the is it account based, is it attached to
9 something, could somebody present me, you know, the
10 telephone card and I can say oh, yeah, I don't know who
11 you are, but these are the calls for that card.

12 MR. MEDINE: Yes.

13 MR. COLE: A narrow point. For what it's
14 worth, the way the business community that guided us in
15 the development of BBB online, this is precisely how
16 Deirdre is describing it. If it's information that is
17 -- is or can be associated with an individual, and it
18 is retrievable in the ordinary course of business,
19 access should be provided, unless, and the unless is a
20 narrow description of the balancing of costs and
21 benefit.

22 MR. MEDINE: Robert?

23 MR. HENDERSON: Bob Henderson. I think Richard
24 mentioned something that was sort of bypassed and I
25 can't remember his statement, so I'll sort of

1 paraphrase it. Basically I think we have to be careful
2 in terms of looking at these issues around how the
3 technology can execute the management of the data as
4 opposed to looking at how we want to help the consumer
5 control their privacy. And they're two distinct
6 activities, okay, and I think we have to keep that very
7 much in mind.

8 When we talk about fusion of data, when we talk
9 about some of the comments that Daniel made earlier
10 about online databases or offline databases, I think
11 those are secondary issues until you get to the point
12 of understanding the notice and the choice that the
13 consumer has, and then identifying what is PII and what
14 is not. Until we get to those identifications, I think
15 everything else becomes secondary and leads to a lot of
16 confusion.

17 Until I state very clearly to businesses that
18 are driving web sites what their requirements are, and
19 what standards or laws we're going to hold them to
20 around notice, I don't know how we can stipulate how
21 they should run their business. It doesn't make any
22 difference what technologies they use, it's a moot
23 point until you tell them the rules that they should
24 get engaged with.

25 Then when you give the consumer choices, now

1 you start getting into what rights the consumer has
2 around access. And then with those choices, you
3 identify what is PII. And until you identify PII, I
4 don't care how you store it. It doesn't make any
5 difference what technology you use to store that data
6 and you can fuse it all you want.

7 As a matter of fact, fusion is not the issue,
8 everybody can do that. So, the levels of
9 identification you have, and again, Richard talked
10 about master keys and we sort of got down to personal
11 identifiers, et cetera, they're all synonymous. The
12 issue is, what identifiers does a business have for a
13 particular consumer, and however they use those
14 identifiers around notice and choice is what we ought
15 to be managing. And then let the businesses use the
16 technologies in whatever way they feel they need.

17 MR. MEDINE: But are you then answering
18 Deirdre's question to say to the extent that the
19 business can identify it, that the flip side of it
20 ought to be that the consumer can get access to it?

21 MR. HENDERSON: Absolutely. If the business is
22 dealing anonymously, and following the rules of dealing
23 anonymously, they have no rights to provide access,
24 because in theory, they are not violating that
25 consumer's personal data, but if they're dealing with

1 identifiers, then that consumer has rights of access.

2 I don't mean to downplay it, but you have to
3 make it a simple equation before we can get into the
4 complexities.

5 If you start at the other end trying to develop
6 the complexities, I don't think we can ever identify
7 the simple equation. I'm a firm believer in all of my
8 discussions with anybody I deal with is first tell me
9 how I manage notice and choice, until I understand
10 those parameters, I don't know how to deal with this
11 issue. Because it gets too convoluted and too complex.

12 MR. MEDINE: Deborah?

13 MS. PIERCE: Deborah Pierce, Electronic
14 Frontier Foundation. I just wanted to go back for a
15 moment to the data relevancy policy issue, and we had
16 kind of a hard time finding a place for this, but we
17 noticed that it wasn't being discussed anywhere else,
18 and so we just thought that relevancy and retention
19 were both important enough that we wanted to include it
20 in our outline, and I know, you know, for us at EFF,
21 what we've been seeing with a lot of companies where
22 they're gathering so much information, you know, almost
23 like a vacuum cleaner and, you know, whether it's
24 related to what they're doing or not, just because data
25 is just easy to gather.

1 And so we really just wanted to get people to
2 start thinking about, you know, why are you using this
3 information, why are you gathering this information, is
4 it related to something that your business is doing.
5 And that's why we wanted to include it in our outline.

6 MR. HENDERSON: If I could comment on it, I
7 think that's a good point because it goes -- the
8 Europeans have handled it, they call it minimalization.
9 Okay?

10 Now, again it's tied to notice. If you state
11 your notice, then you can't go with this broad search
12 and accumulation of data, because you violate your own
13 de novo statement and you should not be violating whatever
14 definitions are put forth through the business. So,
15 notice, minimalization, data relevancy, all those are
16 explicitly tied.

17 MR. MEDINE: Alexander and then Dan.

18 MR. GAVIS: Alex Gavis, Fidelity. I think what
19 we were really trying to do here was to sort of lay out
20 a list of categories to really see to how we could
21 understand the categories of information that may be
22 collected. Because from the consumer's standpoint, as
23 was mentioned earlier, I think a lot of consumers
24 aren't necessarily aware of all these different types
25 of information that are collected, and how they link up

1 together.

2 So, I think it was important to actually put
3 down a longer list. We may want to pare that back, and
4 then from the list, it's then important to sort of
5 assess the normative value of each of these categories,
6 and that's really the sensitivity analysis. And then
7 to assess the risks involved, and you have to assess
8 the risks involved both from a consumer standpoint and
9 from the corporation or company's standpoints, and then
10 ultimately come up with sort of a reasonably practical
11 approach, which can kind of at least balance the
12 interest of the consumer, the normative values that the
13 consumers have, and the companies' business interests
14 and the cost of access.

15 So, I mean I think what we may want to try to
16 do is reframe this, but I do think that we need to
17 start with categories because that's really the area
18 that I think is most obtuse to the customers. The
19 customers don't necessarily know that all this
20 information is being collected about them.

21 MR. MEDINE: Dan?

22 MR. SCHUTZER: Four points I would like to
23 make. I agree with the distinctions that Deirdre made,
24 that if I'm collecting something that I have kind of an
25 index or a way of providing access to it, independent

1 of whether I know the entity, and when I say an entity,
2 bear in mind a very valuable entity is a household.

3 So, a household means an address without
4 knowing who that person is or a telephone number, you
5 know, just a resident, occupant. That alone can cause
6 privacy violations if you're not careful, because I'll
7 end up sending you all sorts of mail that you don't
8 like, or telephone calls during dinner time that you
9 don't like, so but I can provide access to that.

10 In the Internet, there's analogs to that
11 access, the address and the telephone number, there's
12 ID addresses, email addresses and PC numbers and
13 software registration numbers and a variety of other
14 things that would allow me to provide access.

15 I think the second point is that although I
16 think it's important to understand the distinction
17 between whether that entity has an account with me or
18 not, because if they don't have an account with me,
19 that changes the nature by which I provide the access.

20 In other words, anybody that gets onto that ID
21 number or that computer can have access to that
22 information I profiled, and I have no other way of
23 safeguarding it. That's a little riskier than if I had
24 an account with somebody where I could actually have
25 passwords and other times have stronger identification.

1 So, that makes us be mindful of, you know, what
2 kind of information I collect and how I provide access
3 and what kind of safeguards I provide access to.

4 The third point is the retention area. I just
5 wanted to comment about the deleting. So I wanted to
6 point out some of the things that we like to do
7 sometimes, is that we'll collect data, sometimes we
8 like to retain a lot of this history data on tapes
9 because it's not practical to retain this when we're
10 talking about years and years of it. Sometimes we're
11 required to retain it by law, but I'm saying ignoring
12 that, we may want to retain it for years and years
13 because we're not trying to track somebody that way,
14 but we're trying to understand people's behavior in
15 buying decisions and credit decisions over different
16 life cycles, different economic cycles and to build
17 models based upon that. But it would be impractical, I
18 think, to ask me, even though I might be retaining, I
19 don't want to delete it, all of this data that's kind
20 of massive stored offline, which I will run
21 occasionally to generate a model, which then has a --
22 the only thing I do store is the parameters of the
23 model, which has nothing to do with any individual
24 profile of any entity, to have to delete it just
25 otherwise I would have to provide access to it.

1 So, I wanted you to think about that. Then
2 later on, later on you talk about the distinction of
3 real time. I think what you mean by real time, I mean
4 I think the important distinction there is not real
5 time to the extent that when I ask for information, I
6 get it necessarily in real time, you know, the
7 performance, because you talk about other ways of
8 providing information. I think what you're addressing
9 is the issue of when I -- when I collect the
10 information, can somebody indeed access it instantly
11 after I've collected it. And that's not always
12 practical to do, because we don't always -- we do have
13 batch processes in some of this information that we
14 collect and we cannot make it available online in real
15 time.

16 For example, if you look at many of your
17 banking information, what we will do at real time is we
18 keep a running tally of the outstanding balance there,
19 the outstanding line of credit, as we debit it, but we
20 don't necessarily have available the transaction ledger
21 online available the next morning. So, if that's what
22 you mean by real time, that's an important decision,
23 what's reasonable for that company, if they are
24 updating that data in real time and have access to real
25 time, like your available balance and credit line you

1 should be able to see in real time, that is to say as
2 soon as you've made a purchase, you can now see a
3 balance again and it's decremented, but it would not --
4 it would not be capable of providing you a transaction
5 ledger that last bill that you just paid until the next
6 day, then we can't give it to you until the next day.

7 MR. MEDINE: Thank you. Lorrie then Ted then
8 Stewart.

9 MS. CRANOR: Lorrie Cranor. Several points.
10 First, a few people have made comments about things
11 that are sort of beyond the security and access, and I
12 think while in many cases it would be nice to look at
13 the privacy issues from a more comprehensive sort of
14 holistic view, that doesn't seem to be the scope of the
15 committee.

16 So, we might want to make a note about that in
17 the report, but I don't think we can look too much at
18 things like use limitation, which I would love to look
19 at, but don't seem to be related to the scope of what
20 we're supposed to be doing.

21 Back to Deirdre's comment about defining
22 identifiable data, I would urge us not to try to do it.
23 I've been trying to do it for three years now in the
24 context of the PPP project, we gave up, we finally just
25 removed it from the spec. It's something that

1 doesn't seem to be doable. I think that instead we
2 focus really on the question at hand, which is what
3 data do you have to provide access to and under what
4 conditions. And not worry about for all time whether
5 we consider that identifiable or not.

6 The third point is that we've come up with a
7 few different lenses of looking at data. One is the
8 category of the data. Another is how the data is used,
9 and this idea of whether it will be identifiable.
10 There might be another kind of lens which I think is
11 raised by the ideas that the Better Business Bureau
12 says if the data is used -- is accessible in normal
13 business practice, we may want to look at sort of a
14 business practice lens.

15 I can think of off the top of my head four
16 different kinds of business practice. One where I have
17 people that I identify, but not ongoing accounts or
18 relationships. Two where I identify them as part of
19 ongoing account relationships. Three, where I don't
20 identify them, and I don't have ongoing accounts. And
21 four is I don't identify them, but I have this ongoing
22 relationship, although not identified. And we could
23 probably think of others. But trying to come up with
24 those types of lenses to look through might be a
25 constructive thing to at least try.

1 Okay, and another point a few people have
2 raised is we don't want to get into the position where
3 we have some sort of rule where that allows companies
4 to say I'll just delete things when somebody requests
5 access. I think we should make a note that whatever
6 the Commission decides to do, they should make sure to
7 close those kind of loopholes. I think that's just
8 worth a note in there.

9 And finally, when we think about access, we
10 should definitely think -- remember that there are
11 different kinds of access, different costs, different
12 times. I know like in the telecommunications industry,
13 even though I work for a phone company, I'm not up on
14 all the regulations, but my understanding is that long
15 distance companies are required to provide access to
16 telephone records, and depending on how old the records
17 are, there's a different amount of time that they have
18 that they have to be able to provide it. And so
19 records that are less than a certain length of time
20 old, have to be provided like immediately or something
21 when you call, and if it's like five years old, you
22 don't have to find it immediately, but within some
23 other time. So, I think it's reasonable to say that
24 different kinds of access is appropriate under
25 different terms.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 MR. MEDINE: Thank you. Before we move on to
2 Ted, just to note that David Ellington, Stewart Baker
3 and Jim Tierney are here as well.

4 MR. WHAM: Ted Wham, Excite@Home. I have
5 several points that I would like to make. First of all
6 -- sorry. I would like to echo the comments that
7 Deirdre made earlier and that is that a great place to
8 start is the question is it accessible and if it isn't
9 accessible, you know, you go home. Unfortunately most
10 things are accessible, including online profiles, as 65
11 million anonymous profiles, but if I can get on to the
12 computer were that anonymous profile is tied it's in
13 the cookie data and I can go to Match Logic and
14 conceivably get that.

15 It poses a real risk whether we would want to
16 do that because there's no authentication mechanism
17 other than the fact that I know the cookie number.
18 Perhaps I can even mask that put it on my computer and
19 my company setting, for instance, if you have a cubicle
20 environment such as we do, my neighbor could get on and
21 see what they know about you or even worse all the
22 places you have visited. Or using the same type of
23 theory that employers have access to email, access to
24 their employees, they probably have equal access to all
25 the profiles of their employees, creating a black hole

1 instead of better privacy for consumers.

2 Second thing, uses. There's been a discussion
3 about having to explain and limit the collection of
4 information to reasonable, you know, and known uses of
5 the information. I would suggest that that's an
6 extremely difficult charter to give to any type of a
7 business.

8 An example I would use is that if I gave you my
9 business card and you took that out of here, would you
10 be able to categorically identify every use of the
11 information on that business card that you ever
12 conceivably could use. I think that's an almost
13 impossible standard for somebody to have. And tied to
14 that is that there is sometimes from the information
15 that businesses collect, they may not have an immediate
16 use of it, but there may be a serendipitous use out of
17 it that is beneficial to the consumer and to the
18 business.

19 The example I would use is how data mining
20 has identified how there's a real link between grocery
21 shopping purchases of diapers and beer that individuals
22 -- absolutely true, individuals -- depending on the
23 type of thing -- has been identified and in fact in
24 many grocery stores, they are now proximate to each
25 other so that people can buy them more easily. And it

1 was only by looking at the individual --

2 MR. TORRES: Thank God that information was
3 collected for that purpose.

4 MR. WHAM: But for a business that's trying to
5 eke out, you know, every penny, I think that's really
6 something to focus on.

7 MR. MEDINE: We can speculate as to why the
8 correlation exists.

9 MR. WHAM: We don't want to go too far down
10 that path.

11 Next point, in terms of access to information,
12 businesses especially when you've got back-up tapes and
13 you've got an environment which by its very nature
14 reports every transaction, Excite@Home, for instance,
15 will take the transaction logs and so forth and back
16 them up onto tape and throw them into some musty
17 warehouse some place for a long time.

18 We don't make a lot of specific effort to say
19 that we're not going to keep and back-up this type of
20 information and we are going to keep this type of
21 information, so we don't minimize information
22 along the way and so forth. It all gets this. Because
23 it's sort of expensive to determine and make
24 modifications in the back up process saying I am going
25 to keep this, I am not going to keep that.

1 If a consumer came to us and said we want to
2 know all the click stream data that we have done over
3 the past six months, is that technically possible to
4 achieve, yes. Is it something we do in our normal
5 business practices, no, I as an employee probably
6 wouldn't be able to get my hands on it because it's
7 frighteningly expensive to do that.

8 The last point I want to bring up is in regards to
9 the minimalization of information and the rights of access.
10 Again, I would like to posit that in no part of, you
11 know, government actions that I'm aware of is there
12 this demand that companies pull back in terms of their
13 features and pull back in terms of, you know, the
14 information that they collect, actively go and have a
15 responsibility as mandated by law that there's an
16 access right or that there is a requirement to collect
17 only a little bit of information, and are we going to
18 treat this as this completely different medium and
19 we're going to say you because you happen to be doing
20 business via this one communication technique have to
21 treat your business data and your business by a
22 fundamentally different set of rules than somebody else
23 out there.

24 Until somebody tells me why Nordstrom has to
25 tell me why they're giving me 10 percent off and my

1 colleague here 20 percent, why bother having that same
2 burden of having to say this is the data we collect and
3 this is why we collected it on you in that environment.

4 MR. MEDINE: Just as an example, you said
5 determine uses of access, does that suggest to you in
6 the earlier discussion of a matrix that we ought to be
7 focusing more on categories of information than on uses of
8 information because it's hard to anticipate even
9 present if not future uses of the information?

10 MR. WHAM: I'm more comfortable personally with
11 the categorical approach. I think uses is a very, very
12 slippery slope. I think relevancy is actually
13 slipperier, and to echo on a comment made probably 45
14 minutes ago by Dan Jaye, I see data as being of three
15 basic types. Data which is not PII, and can never be
16 associated with PII, data which is PII, that we would
17 all agree with that, and data which can be linked to
18 PII.

19 So, for instance, by that the fact that you,
20 David, are male, is never PII, even if I put it with
21 your name and so forth. It's an attribute about you,
22 but it is not definitionally a PII element.

23 MR. MEDINE: Stewart?

24 MR. BAKER: Thanks, Stewart Baker from Steptoe
25 & Johnson. I've got three points. The first is there

1 are a couple of issues that I think we could probably
2 safely drop from this part of the outline.

3 I agree with Ron that data relevancy is not a
4 question we are asked in the context of access. And
5 data retention, while as Ron points out there might be
6 some data retention issues that would be relevant to
7 access, the issue that's discussed here is not, it says
8 a company should delete information after a specified
9 period of time. That's an anti-access provision,
10 that's not an access provision. It's not a question we
11 were asked, I don't think, since we have plenty of work
12 to do just answering the questions we were asked, we
13 probably shouldn't get into that.

14 The second thing that I would raise here is I
15 think there's a missing piece of analysis running
16 through these categories. I mean, we shouldn't kid
17 ourselves. We're writing a regulatory program here.
18 We want to impose these rules on people who don't want
19 to follow them. Because if you want to follow them,
20 you can just follow them, you can do anything you want.

21 So, this is a regulation imposed on unwilling
22 persons, and there ought to be a pretty good reason to
23 do that.

24 So, what's the reason for imposing the access
25 requirement? It seems to me there are two reasons to

1 impose an access requirement. One so that people can
2 correct data that's wrong. This is the Fair Credit
3 Reporting Act requirement. It's understandable in that
4 context, that people would say you're making these
5 important decisions and you've got inaccurate data
6 there, somebody stole my credit card and made these
7 purchases.

8 And let's be honest, there's a second
9 reason to do this, and it's what at least in the
10 sixties we called consciousness raising. It's so
11 people will request this, and be shocked at the amount
12 of information that particular party has gathered on
13 them. And then they'll vote for candidates that want
14 more restrictions on data.

15 Now, it seems to me that the first is a lot
16 more legitimate than the second. And so I think that
17 the question that's not asked in this discussion is so,
18 how likely is it you're going to be correcting this
19 data? And when you start asking that question, a lot
20 of the stuff starts to look a lot less attractive as an
21 access environment.

22 I mean, am I really going to stay no, The Story
23 of O' was not in my shopping box for at least 30 seconds
24 and I want you to take that data out? Well, I guess
25 you could do that, but am I really going to say this is

1 not my cookie that you put on my hard drive? I mean
2 you're just not going to correct that data. I don't
3 think you're going to be doing much about correcting
4 click stream data, because what you're saying is
5 somebody might have used my computer, but they couldn't
6 possibly have gone to that site.

7 So, it would be useful, I think, in analyzing
8 each of these, to say so, what is it that we're going
9 to do with the access? And if we're not going to -- if
10 all we're doing is consciousness raising and helping
11 the fund-raising of EFF and CDT and the privacy
12 organizations, that's a useful thing to do, I think,
13 but we should know that that's the principal value of
14 the requirement.

15 The last thing is just a suggestion for adding
16 an option. We have a lot of discussion in the terms
17 and conditions about a whole bunch of rules about
18 storage and reform and legacy systems and it seems to
19 me that there's an awful lot of specificity to this
20 rule and we're writing a very specific -- a very
21 detailed set of rules. One of the options ought to be
22 to focus on requiring businesses to do for consumers
23 requesting access what they do for themselves in the
24 ordinary course of business.

25 If in the ordinary course of business they pull

1 this data out once a year and run it, then they ought
2 to run their consumer requests once a year in the
3 ordinary course of business. If they use it every day,
4 and they have it online and it's accessible that way,
5 then they ought to make it accessible in that fashion.
6 It creates a lot of flexibility and it says we're only
7 going to impose costs on business when the business has
8 already shown it's willing to accept those costs for
9 its own business purposes. And I think that's an
10 option that ought to be in here somewhere in the terms
11 and conditions discussion. Thank you.

12 MR. MEDINE: Well, let me sort of ask about the
13 reasons for access not only shock value but
14 accountability as a benefit as well, but maybe Andrew
15 can address the fund-raising aspects of the question.

16 MR. SHEN: Well, I was actually just going to
17 go ahead and talk about that. I think it is important
18 to talk about data minimization, deletion, use
19 limitation, data relevancy.

20 Well, the first reason I really think that's a
21 point is I don't know of another place to talk about
22 it. I think you can sort of address those issues in
23 notice and sort of address those issues in consent and
24 you can sort of address those issues in access, but
25 since that's really not articulated as a separate

1 principle, I think since you have a panel of experts
2 here, you might as well have discussion on the issue. And
3 that kind of leads me to my second point. I think it
4 does play an instrumental role in access, because I
5 think one thing we all considered is what is the actual
6 cost to businesses of implementing whatever
7 recommendations are made.

8 And clearly if information -- clearly if
9 companies are not collecting personal information or
10 don't have enormous profiles, and are thus minimizing
11 the data, those costs would be decreased, and I think
12 that's really how it comes into the current discussion
13 we have going on right now.

14 And specifically in response to Stewart's
15 questions --

16 MR. BAKER: I didn't mean to leave you out.

17 MR. SHEN: That's all right. I think I agree
18 with David that, you know, access is a right, because
19 this is information about other people, and I think
20 those people whom that information describes always have
21 a right to know what is being done with it and where
22 it's going and where it's being collected.

23 MR. MEDINE: Dan Jaye? Daniel Jaye?

24 MR. JAYE: Thank you. A couple of points that
25 get specifically to this issue of as we look at the

1 scope of access, and I hope that we would really wait
2 until we got into the security and authentication area
3 to deal with it, but since you just brought it up that
4 it's probably sort of fundamental to defer until that
5 part of the conversation, but one thing that I just
6 throw out, and once again since as Dan put it, we --
7 when you don't know where you're going, any direction
8 is good, that that gives me the model that what we're
9 doing here is we're coloring in a circle. Because
10 we're going in all directions and filling in all the
11 possibilities.

12 So, if we're coloring in a circle, I would
13 just throw out that the definition that we operate by
14 at Engage as one option, and one of the ways that we
15 define what is known PII versus PII that is linked to
16 PII, is when we can't figure out who a consumer is.

17 And the example of telephone numbers that was
18 brought up is interesting, but there are a couple of
19 points about it that I would like to point out a couple
20 of differences. First of all, when you're asked who
21 else has made calls. First of all, you have to be the
22 account holders. You are an identified authenticated
23 person and maybe even you can tell whether you're
24 authorized or not to access what calls are made by the
25 phone number you pay for.

1 Second of all, if I dial up the phone company,
2 that's actually more analogous than going to your ISP
3 and asking your ISP, what sites has my browser visited,
4 as opposed to going to a website and asking for what
5 data has been collected.

6 Third of all, I can't dial a cookie. I can
7 dial a phone number. You can actually contact a -- the
8 phone number is actually an identifier that is a
9 contact mechanism as opposed to a cookie which in the
10 non-PII case is used to distinguish one visitor from
11 another as opposed to specifically identify a
12 physically identifiable individual.

13 I think I would like to agree with Deirdre,
14 specifically on her concept, though, that she's
15 introducing and I think it's introduced on the document
16 an account holder as I think one term that might be
17 used is synonymous data, synonymous data, which is the
18 case where someone is not particularly identifiable but
19 does have a persistent relationship. And I think
20 that's actually in a very useful case so there
21 absolutely is a case where data might be non-PII, but
22 there would be reasonable mechanisms to provide access
23 in that case and I think that's a very important point
24 to bring up.

25 So, certainly the absolute statement that you

1 can't provide access at all, if there's non-PII data, I
2 think that when there is a persistent account, that
3 makes sense.

4 And then the final case I just want to bring up
5 is that we talk about the security risk and the fact
6 that well, any data could be breached, so you have to
7 assume what is the privacy risk if the security was
8 breached. And there's another principle I think in
9 security which is sort of the straw -- the needle in
10 the haystack analogy that if the data is in a pile of
11 thousands or tens of thousands or tens of millions or
12 even hundreds of millions, soon, records of data, and
13 you don't have any meaningful way to go out to look
14 into that data, that is there really a privacy risk
15 about the fact that there is data in there that might
16 be in the future upon a subsequent information
17 disclosure linkable to an individual, but at that time
18 is not linkable to an individual.

19 You know, the point that I would make is that
20 what we really have in this case is a straw in a
21 haystack, not a needle in a haystack, and I think
22 that's a very important distinction to make.

23 MR. MEDINE: One thing. One issue that was
24 raised over here in terms of the costs of the company
25 providing the access, it would be helpful if people

1 want to consider addressing the costs that might be
2 imposed on the consumer, transferring those costs to
3 the consumer and the outline talks about that to some
4 extent, but if the group has a view of what's
5 appropriate in terms of charging for access, and David
6 has a flag up, I don't know necessarily to address that
7 point, but --

8 MR. DAVID HOFFMAN: David Hoffman from Intel
9 corporation. It actually wasn't to address that point.
10 I wanted to -- I think we've unearthed one of the
11 dichotomies that has appeared in every single subgroup
12 meeting that I've participated in, and it is the
13 dichotomy between the members of the committee, those
14 who believe that the function of why we're here is to
15 protect the consumer from harm. And others who believe
16 that the reason why we're here is to make sure that any
17 information that's collected that might be valuable to
18 someone falls under the scope of what we're doing.

19 And I feel that that was actually pointed out
20 very well by Deirdre in her analogy with the phone,
21 which I was originally confused by, because I agree
22 with Dan that I think the real issue of when that's
23 harmful to the consumer is when that is matched with
24 some other personal information, my name, my address,
25 my billing mechanism.

1 And the problem with that is I think inherently
2 the issue of harm is the ability for me to separate
3 myself from the data at some point, whether that's by
4 destroying a cookie, or whether that's by chopping up a
5 phone card that isn't connected to me in any other way
6 than I happen to have it on me at this time.

7 So, the issue that I believe we need to address
8 is are we here to protect consumers from harm, and if
9 so, then the document, Richard, or I don't see -- maybe
10 the underpinning of some of the categories that we have
11 here, such as the one -- the use tax that we call out,
12 may get to the point of whether it's causing harm or
13 not, but it's not called out explicitly.

14 I think we ought to call that out explicitly at
15 least as one of the options that we think is important.
16 And then we ought to recognize that there is a spectrum
17 of harm. And I would like to hear Deirdre and other
18 people's response and Frank I think has also commented.
19 I don't necessarily see a tremendous amount of harm
20 that could come to the consumer from situations where
21 it's not linked to personally identifiable information.

22 MR. MEDINE: Did you want to respond to that,
23 Deirdre?

24 MS. MULLIGAN: I'm so pleased. That is so
25 nice. What a good set-up. Actually I wanted to make a

1 personal point with respect to privilege with Mr. Baker
2 over there. I mean if we're going to go down the line
3 and the realm of sarcasm, I would suggest that the
4 people who would have the most interest of these people
5 having committees come up with regulation is the
6 lawyers.

7 MR. BAKER: The lawyers?

8 MS. MULLIGAN: The lawyers who have the database
9 clients or the access companies who provide the
10 infrastructure to provide access. And as a point, no,
11 CDT isn't really having a funding problem. In the
12 current market.

13 But yeah, I think the question -- Stewart said
14 what we should really be talking about is why are we
15 providing access, and in fact I think very early on, a
16 committee that Andrew was on and some others,
17 documented some of the reasons for access. I see that
18 as part of our task, whether it's to prevent harm, to
19 ensure accountability, but I really think that there
20 was a -- I put a model on the table for thinking about
21 how we approach access.

22 First, is it possible, right? If it is
23 possible, I completely agree with you, Ted, are there
24 other risks, are there costs, is it inappropriate, you
25 know, Steve Cole, does the business access it, is it

1 sitting in the back? How do we look through these
2 issues?

3 But we have to start with a framework first,
4 and I really want to push and say that if we could
5 start with a framework and say that access can be
6 provided to data in a certain -- if it has the
7 following attributes. It's tied to an identifier.

8 Now, there's a question about how do we
9 authenticate the individual? Absolutely. If you look
10 at the authentication section, there's no direction
11 that I present an email address and you give me access.
12 There's suggestions that you perhaps combine this with
13 a password, perhaps you combine this with the last
14 three people you've sent an email message to. You're
15 trying to provide access back to the person. However
16 there's no way to authenticate other than
17 identification.

18 All of the security people in the room I'm sure
19 here can tell me that that's not true. Those aren't
20 the same things. And so I want to push a little bit
21 and say let's come up with a framework at the front
22 end. And I was actually really heartened, I had NCR, I
23 had Mr. Schutzer, I think I got Ted Wham, I had Steve
24 Cole, I was feeling a lot of buy-in, so if we could
25 move forward on that, I would really -- I think it

1 gives us a good place to start.

2 MR. MEDINE: Why don't we take Rob and then we
3 could take -- I should take a break and then we can
4 resume with all of the flags that we have up and go for
5 quite a while, and give the court reporter a chance to
6 have a break, if nothing else.

7 MR. GOLDMAN: Rob Goldman, Dash.com. Sorry for
8 not continuing along, I've been sort of collecting
9 these comments as we go. So let me try and get them
10 out.

11 We've been talking about various continuums to
12 consider, and we did it on the subcommittee that I was
13 on and I see that it was done here on the access one
14 committee, and I think everyone has commented or many
15 have commented on how complex these get, and difficult
16 to discern one item from another and there's a lot of
17 overlap and lot of blending. Business practices, which
18 Lorrie just suggested as a potential lens to look
19 through this could conceivably be part of the use lens,
20 and the question is to where the two are separated is
21 difficult.

22 Even within use itself, if you try to quantify
23 sort of no use on one end and use for life impact
24 decisions on the other end of the spectrum, it's not
25 exactly clear where, for example, employment use --

1 used in making employment decisions versus health
2 decisions versus financial decisions, where exactly
3 those fit along those continuums. So, why does that
4 matter, I guess?

5 I think use is great because it's a more
6 relevant to the consumer, I think it's more important
7 distinction. Factual information that may seem sort of
8 trivial can be used in important ways. So, I think
9 it's a more relevant continuum than the time continuum,
10 but again you get back to this issue of how do you make
11 distinctions that are clear to use and practice. And
12 both with use and type I think we run into this same
13 rat's nest around derived data, inferred data. You can
14 use inferred data to make important decisions, but
15 should we require access to that?

16 There are certainly passionate opinions on both
17 sides of there, and certainly with type. Some derived
18 information is factual. Some information can be
19 summarized, counted and shown totals. Other derived
20 information are essentially inferences, and inferences
21 are a different type -- I mean inferences aren't right
22 or wrong, they're inferences. So, it's hard to say
23 whether they're correct or incorrect.

24 Given that, I guess there are -- there's one
25 piece of language that's occurred to me as we have been

1 going through this which I would like to offer, and
2 that is factual information used to make important
3 decisions, which I think is -- it does a good job of
4 dodging the problems with both continuums. Factual
5 information includes some derived information, but of
6 course only information of fact, not opinion, and not
7 inference.

8 So that's on the type continuum. And on the
9 use continuum, important decisions is broad and vague,
10 I know, but I think for the -- in the mind of the
11 website operator of the future, trying to decide
12 whether or not the information is being used to make an
13 important distinction, I think it's a valuable question
14 to ponder. Is this important and who might consider it
15 important, might it be considered important by a body
16 or an agency, or a regulatory authority.

17 And I guess that brings me to Stewart's point,
18 and the points others have made in the same area, which
19 is that what is the point of the recommendation? This
20 is a very emotional issue, and I think we've seen that
21 going around the room here, and I've certainly seen it
22 outside in between our meetings when I discuss what's
23 going on in here with the friends and family, and it's
24 not clear to me where -- I mean certainly we may
25 address it, just because it's an important issue, and

1 emotional in the minds of many people, but it's not
2 clear to me that we have tried to quantify this as a
3 public bad in any real way.

4 To Stewart's point, the sort of consciousness
5 raising aspect of this, does speak to the emotional
6 side, and maybe there's a place for that. Maybe this
7 is that place, I don't know. But certainly to the --
8 to the more practical allowing people to correct
9 information so that it's correct, and used properly, I
10 think it's a little bit harder there, or I heard anyone
11 yet make an argument as to where the market would fail
12 there or why, and I'm curious to hear and I'm not
13 convinced that it won't, but it certainly doesn't seem
14 obvious to me that it will.

15 Whatever businesses, at least people from
16 industry in the room are operating and working, they
17 will always in every case, make a correction for
18 information if it adds value to the business. There's
19 no case where I won't make a change if that creates
20 value for the company and for the world and so I guess
21 the question is, where it won't. And then the only
22 times I won't voluntarily change data is where that won't
23 add value to the business and won't in my self interest
24 improve my position.

25 So I guess the question then is why has the

1 market failed there? If I have information I'm using
2 and I'm holding offline for auditing purposes and other
3 purposes and that information is not being used to make
4 important decisions, not being used at all perhaps, and
5 there are consumers or customers or entities of any
6 sort who want to correct that information, it will be
7 positive costs to me, and I guess I would argue
8 insignificant benefit to them, why is that -- where did
9 the market fail there? Why do we need to regulate? I
10 mean I would certainly like to hear that argument,
11 because it's not clear.

12 MR. MEDINE: Thanks. Why don't we take a
13 15-minute break and convene at about 10:40.

14 (Recess in the proceedings.)

15 MR. MEDINE: Okay, thank you, if we could
16 resume the discussion. We would like to turn next to
17 the issue of entities --

18 MS. CULNAN: Is there anymore on the final
19 comments?

20 MR. MEDINE: I was going to get to that. I
21 would like to start focusing on entities, although I
22 know that some people had their flags up who wanted to
23 try to make some closing comments on the prior
24 discussion, and why don't we start with Dan here and
25 then Mary.

1 MR. GEER: Thank you, yes, Dan Geer. This is
2 sort of like a chat room in that this conversation is
3 -- there are several in the room and this goes back a
4 long way.

5 MR. MEDINE: Do you have to provide access to
6 the chat room record?

7 MR. GEER: Yes, but incursion comes to mind.
8 The question of mine what was and what wasn't known
9 personally identifiable information, and, sir, your
10 request for things that people could follow without
11 confusion, I suggest that anything that's not
12 personally identifiable test for that is could we
13 publish it without harm. In other words, if it's
14 non-PII, you can put it on the net. If that isn't a
15 hurtful number, it must be non-PII. This is an
16 operational thing, if you can publish it, it must be
17 non-PII.

18 Secondly, I would like to raise one small issue
19 here. Not raise, I guess, I'll tell you how I was
20 thinking, and it might be at odds to many, I was making
21 no distinction between a real person and a legal person
22 in this discussion, because it seems to me as a small
23 business, for example, we take great steps to make our
24 web browsing anonymous so that our competitors don't
25 know when we visit their site, et cetera. I would make

1 no distinction between a legal person and a real person
2 with respect to this discussion.

3 Third, and last, this argument about well, what
4 happens to the data, and how do I know what appears to
5 the data, and how do I know that it went away? I would
6 suggest that, again, as an operational rule, perhaps
7 ugly and blunt, but as an operational rule, you could
8 say to a web operator, or whoever else, you can't
9 collect data unless you're prepared to keep it forever.
10 I will now shut up.

11 MR. MEDINE: Thank you. Mary?

12 MS. CULNAN: Okay, I would like to make some
13 just general points before we move on. The reason for
14 access, this is the first principle, and the original
15 fair information practice is that there should be no
16 secret systems, the basic idea is that people have --
17 should know if information is being collected on them,
18 that that is essential in a free society. Independent
19 of the operational issues of providing access.

20 And so what I think that means is, to go to
21 something Frank said earlier, is the idea of how much
22 of this can we accomplish with notice, and I would say
23 it's not -- consciousness raising maybe the nineties
24 word for the -- the 2000 word for this is consumer
25 education, but the idea of not just telling people we

1 collect information from X, Y and Z and what we do with
2 it, but you provide some samples.

3 And if people understand what it is and what it
4 looks like, perhaps that may help them understand and
5 they wouldn't actually go and ask to see their record,
6 maybe they would. That's a good question for research
7 to study at some point in the future.

8 But I'll give you an example. Browsers pass on
9 information about us, and there are web sites, CDT has
10 a website that does a good job of this, the Pentagon
11 even has a website and people can link to this that has
12 a page that explains this is what your browser says
13 about you when you visit a website and it gives an
14 example. And people see that and then they can decide
15 okay, I understand this, I want to know more, whatever,
16 but I think for most people, that would make them
17 comfortable and say fine.

18 Another example would be where information is
19 acquired from a third party source, a marketing
20 example, again, a lot of this is aggregate data or it
21 may not even be right because it's census data or
22 whatever, but the idea of providing people with what a
23 sample record would look like for a hypothetical
24 individual, and these are the fields and this is the
25 kind of information that might be provided again, that

1 might be enough for a lot of people, maybe it wouldn't,
2 but I think that's something worth pursuing and to try
3 to do a better job of seeing to what extent notice can
4 address some of these issues versus where I would agree
5 that an important decision is made about a consumer
6 might be another way to phrase that it's a material
7 decision where it affects them in some significant way.

8 And then finally, since we're moving on to
9 terms and conditions, or rather to entities, I think
10 one of the things that requires some attention and to
11 get some in this document is what is actually returned
12 to the person who requests the information, the format
13 of the information that's provided as the result of an
14 access request and you can look to credit reporting.

15 That is an example where there are lots of
16 different ways to do this. It used to be about ten
17 years ago, if you got your credit report, a lot of that
18 would be unintelligible to the consumer. There were a
19 lot of codes. For example you couldn't tell who really
20 had requested your credit report because at the bottom
21 there was just a code that referred to the
22 organization, and there was no way for a consumer to
23 know exactly who that had been. And so I think in
24 terms of operationalizing our recommendations, there
25 need to be some clear rules about the format of an

1 access request.

2 MR. MEDINE: Lance?

3 MR. LANCE HOFFMAN: Lance Hoffman, George
4 Washington University.

5 I would like it not to be lost before we go on
6 to entities because I think it's going to affect the
7 other discussion on entities and other items as well,
8 that we have an appropriate framework to describe this.
9 I've been listening for the last couple of hours, and
10 I'm a little bit disappointed that we have this
11 taxonomy which is sort of just left in the cold.

12 On the other hand, some of the discussion in
13 particular that Steven raised and other people raised
14 about is it possible to get it at all, what is the
15 harm, what are the risks, what are the costs and so
16 forth, and even Mary's most recent discussion about
17 examples, are much more down to Earth and to the point.

18 I would much rather see a discussion when we
19 finally put this out, the next time around, be framed
20 in such a way that there in essence can be a decision
21 procedure for the website operator to invoke and say
22 okay, the FTC has said this, here's some reasonable
23 guidance, and I can read this, I can understand it, and
24 then can address all of these items.

25 And so I would just suggest that not getting

1 too based on taxonomies but rather on decision
2 procedures. At the end of the discussion, what am I
3 supposed to do. And let's keep it simple.

4 MR. MEDINE: Okay, thanks. Frank?

5 MR. TORRES: A couple of comments, but first, I
6 just have to respond to the earlier comments by
7 Stewart. I was actually -- I know they were hopefully
8 a little bit tongue in cheek, but at the same time, I
9 was a little bit disappointed that they were made.
10 It's not just the ability to correct data because I
11 wouldn't want to see an environment where a marketer
12 who's collected all this data sends a questionnaire
13 saying we want to market even more to you, or we
14 haven't gotten any responses from you recently, so
15 could you please correct this data for us so we could
16 send more junk mail to you or so that we can make sure
17 that we're charging you the right amount for your loan.

18 It is an issue of accountability. It's not
19 just an issue of getting in and correcting it. And one
20 of the reasons why I think we're here is because people
21 care about this issue. And the harm -- perhaps that
22 we're talking about is the harm to e-commerce, because
23 people care about the privacy and the security of their
24 information when they go online and in other aspects.

25 I mean maybe the answer is to give consumers

1 the choice about whether the information is collected
2 in the first place. I know that's not why we're here,
3 but maybe that should be part of the discussion as to
4 whether or not you should -- I mean, if we can't even
5 get agreement on allowing access just because you've
6 collected it, and not have to -- and have to try to
7 justify why a consumer should get access to
8 information, then maybe we shouldn't let e-business
9 collect it in the first place.

10 I mean Trent Lott and some others came out
11 yesterday arguing about the census, you know, how dare
12 the government ask these questions, you know, how dare
13 the government ask how many bathrooms you have. Well,
14 I would submit to you that you could probably figure
15 out a way, if it's not done already, you may not be
16 able to tell the number of bathrooms, but you could
17 probably tell me the brand of toilet paper that I buy
18 and how many rolls a week that I use. And yet that's
19 considered perfectly all right and let's protect the
20 interest of the business community to collect that
21 information. I mean why shouldn't -- you shouldn't
22 have to justify to us why consumers shouldn't get
23 access to that information.

24 MR. COLE: You have two bathrooms and a powder
25 room on the first floor.

1 MR. TORRES: Actually you're right.

2 MR. MEDINE: Work our way down, Larry, Richard,
3 Bob and Andrew. And again if we can start moving the
4 discussion, at least amongst some of you, towards the
5 issue of entities and the access II group has a lengthy
6 list of entities and connotations and permutations of
7 entities and again if we can try to bring this
8 practical application simplicity to that approach, that
9 would be helpful.

10 Larry?

11 MR. PONEMON: I did the unthinkable, I actually
12 talked to a couple of consumers, I talked to my
13 nine-year-old son and my 80-year-old mother about the
14 issue of access, and quite frankly, they helped me
15 frame what I am going to refer to as the first ethical
16 proposition of our committee. Let me just go right out
17 here and say it. I have a right to know how much a
18 company or organization uses or plans to use about me.
19 I have a right to know how a company or an organization
20 uses or plans to use information about me. With
21 appropriate redress, and enforcement, I think that is
22 doable by every organization around this table. It
23 doesn't kill the Internet space, it's doable.

24 And here's the important issue, it's not being
25 done today. After we frame this high-level ethical

1 proposition, we went shopping at a toy store, this is
2 not my 80-year-old mother, but my nine-year-old son,
3 and at that toy store, they wanted to collect personal
4 information about me, and even though I was going to
5 pay in cash, they still demanded it and they wouldn't
6 let me out and when I asked what are you going to use
7 this for, and they said no clue, okay.

8 I have a client, and this is a more serious
9 issue, that actually says well, we just collect
10 anything we can get our hands on, because we don't know
11 how we're going to use it in the future.

12 That's pretty scary. So, I think if we start
13 off with a high-level ethical proposition and then
14 start working our way to other propositions that may or
15 may not be costly or harmful to different
16 constituencies around this table, I think that would
17 lead to a more robust framework, to not only access,
18 but also secure it.

19 MR. MEDINE: Could you translate that into
20 access? I mean it's one thing for the store to tell
21 you how they're going to use your information, how does
22 that translate into what you're entitled to get access
23 to?

24 MR. PONEEMON: Again, in talking to my nine year
25 old son and my 80-year-old mother, they both said I

1 want to know how they're going to use this information.
2 That's what Mary said. I don't necessarily need to see
3 the report. It's not like the FCRA world, I don't need
4 to see it, I just want to know how it's going to be
5 used. I don't want companies to be profiting from this
6 information if they don't have a clear reason why they
7 have this information, then I don't want them to have
8 this information. So, with redress and enforcement, I
9 think this is a very workable solution.

10 MR. MEDINE: Richard?

11 MR. PURCELL: Richard Purcell. Quickly now, I
12 encourage us all to begin thinking in the sense of the
13 interdependencies of all of these principles that we're
14 talking about and how notice and choice has a direct
15 and significant effect on not just the access issues
16 but also security and enforcement.

17 We've been beginning to think about an emerging
18 matrix of if you can think about a matrix of two
19 dimensions, with the type of data being one dimension
20 in increasing sensitivity, so it may travel from
21 non-PII to PII to derived to financial and health and
22 children's data as it increases in sensitivity, against
23 another axis, which would be use, which would be of
24 increasing distance from the primary purpose.

25 So, at the non-PII primary purpose junction, it

1 would move out through primary purposes, secondary
2 purposes and even through distribution to third
3 parties. That's really what we're talking about in
4 terms of saying here's what we're going to collect, and
5 here's how we're going to use that data. This is the
6 principle of notice.

7 Choice, access, security, and enforcement, all
8 fit within the matrix that's drawn out from that in
9 that there are varying levels of need for all of those
10 different areas, depending on their location on that
11 chart. If you're gathering non-PII data in order to
12 deliver a primary purpose, I, you know, I've said I
13 like blue as my background when I go to your website,
14 boom, it's done. That's the only purpose it has, it's
15 right at the very corner. The level of security around
16 that data, the level of access around that data, the
17 enforceability of the, you know, of the use of that
18 data, is minimized.

19 If you're asking for financial information,
20 health information, children's information, and you
21 want to distribute it to third parties, it's at the
22 opposite diagonal. It's out in the most sensitive,
23 most protected, most secured, most accessible kind of
24 area. If we think about it in that way, we begin to
25 get a flavor of how you kind of get a chart and some

1 location on that chart that gives you information about
2 how to treat that data.

3 MR. MEDINE: Can I to keep you on your chart
4 for a moment and put you out in your last category of
5 sensitive personally identifiable information that's
6 transferred to a third party, which third -- should
7 that third party be required to give you access to that
8 information, and how do you analyze the question of
9 which parties along that spectrum of transfer should be
10 providing the access?

11 MR. PURCELL: Well, a company's policy, under
12 which data is gathered, has to travel with the data
13 that is distributed. In other words, if I gather data
14 from David Medine, under a certain policy, and I
15 transfer that data to another entity, the data
16 protection that I am providing at a minimum, has to
17 travel with that data.

18 MR. MEDINE: Now, so just to clarify, so that
19 the end result would be the receiving entity would also
20 be required to give access if it's personally
21 identifiable information that at least fits in the part
22 of your chart where the first party that collected it
23 would give access, the third party would also give
24 access, assuming the data is maintained in roughly the
25 same form?

1 MR. PURCELL: Yes.

2 MR. MEDINE: Bob?

3 MR. HENDERSON: Bob Henderson.

4 I want to comment on a couple of comments that
5 were made before the break. One came from Rob that I
6 interpreted his comment to ask how was industry being
7 impacted by privacy, and I think there are some very
8 explicit examples, both in the legal sector, where
9 several state attorney generals are bringing legal
10 action, or have brought legal action against some
11 financial and health care institutions for misusing,
12 misappropriating personalized information.

13 You also have examples on the social side,
14 where one of the states was selling driver's license
15 information for commercial gain, and there was an
16 outcry. GM had an outcry because they had a black box
17 technology in their car, and didn't tell anybody. One
18 of our colleagues here at the table, their company had
19 had an outcry because they had a tracking in their
20 process or tape billing. So, this is a real issue, and
21 it is impacting business.

22 Also, Ted made a comment about minimalization,
23 minimalization and the fact that there were no laws,
24 and I would beg to differ. There are laws. And the
25 laws, if you're in the e-commerce business, or

1 international, that if you do, you know, with
2 e-commerce, there are no international boundaries.

3 So, in Europe, there are specific laws. And
4 interestingly enough, the Federal Trade Commission is
5 involved in enforcing the negotiated Safe Harbor
6 principle that the Department of Commerce is
7 negotiating with the EU Commission, and if they get
8 agreement on that, the FTC is going to have
9 responsibilities for enforcing a self-regulated
10 activity that will be supportive of the EU directive.

11 So, this thing is beyond just looking at the
12 things we see in our own domain. This is world-wide
13 and it is real at the consumer level.

14 And finally, I would comment that Lawrence's
15 example of his nine-year-old son and 80-year-old mother
16 is very appropriate, because those are the things that
17 the consumer is asking, and I think when we get into
18 the entity discussions, and look at some of the other
19 discussions we have to go through with the subgroups,
20 if we don't position ourselves with the mentality of
21 concentric attitude, I think we're going to miss the
22 boat in what we're trying to do.

23 MR. MEDINE: Andrew?

24 MR. SHEN: I would also like to respond to
25 something that Rob brought up earlier, not to jump all

1 over you, but, you know, just in response to how the
2 market has failed in terms of privacy protection, I
3 think clearly e-businesses will also operate in their
4 interest, if it's within their financial interest to
5 provide access, then clearly they're going to do so.

6 But I'm really concerned, maybe I didn't
7 understand the full impact of your comment, but I'm
8 concerned about providing access even if it's not in
9 the business' financial interest.

10 Now, you can make an argument that what we see
11 right now in the public realm is an incredible interest
12 the privacy, that groups like EPIC, CDC, they're trying
13 to do.

14 A lot of fund-raising to point out what
15 companies are doing with personal information. But
16 honestly we don't want to surprise anyone. We think
17 that there should be standards out there that all
18 consumers should expect from companies and that
19 companies should provide. A lot of the problems with
20 privacy is that a lot of the data collection is so
21 invisible to the average user. I think it's very
22 important to think outside of this room. We throw
23 around terms like derived data, inferred data, profile
24 scores like they're just in the normal course of
25 business. For us it is, it's normal business. But for

1 most consumers out there, they have no idea that this
2 stuff is going on. And that's what we have to be
3 concerned about.

4 MR. MEDINE: Stewart?

5 MR. BAKER: Thanks, maybe I can be less
6 inflammatory. Or maybe not.

7 First, just to return to the -- briefly to the
8 question of consciousness raising. Other people have
9 suggested other names for it, consumer education, or
10 accountability, but I think it is the same value that
11 we're talking about. We think people will be
12 surprised, shocked, and unhappy to see what the actual
13 records are, and that will result in pressure on the
14 company to gather less data, or to -- will educate
15 consumers about the nature of their privacy rates or a
16 lack thereof.

17 I don't deny that that is a value of a sort. I
18 think it has more value to some than to others.

19 And I think we should recognize that, but we
20 have to recognize that to impose a significant
21 regulatory burden on people, just in order to serve
22 that purpose, is a pretty heavy responsibility. And I
23 think Mary made a very good point. If what you're
24 trying to do is tell people what kinds of data are
25 gathered on them, why not put it in the notice? The

1 only reason not to rely on the notice is either you
2 think a correction is appropriate, or you think people
3 will be more shocked by seeing the actual data than by
4 reading the notice. And I think the shock value is a
5 much less valuable consideration for regulation.

6 To turn to the section that we're dealing with
7 now, I would just raise this question about correction
8 of data. You know, we had five years of debate over
9 ISP responsibilities for chat rooms, for web pages, for
10 statements that are made there. Should they be
11 required to take down statements that are libelous or
12 that otherwise infringe on the legitimate rights of
13 other people, and the argument which has been quite
14 persuasive thus far to policy makers is that is putting
15 an enormous burden on people. What happens if somebody
16 says this statement about me on a public chat room is
17 libelous? Do you take it down or not? Do you
18 investigate it? Do you hire people whose job is to
19 investigate and find the truth of claims over libel?

20 I think exactly that risk is being run in this
21 context. If somebody says no, Story of O was never in
22 my shopping basket. What do you do? Maybe it was,
23 maybe it wasn't, are you going to conduct an
24 investigation? Are you going to change it even if you
25 think that they're lying because what the hell, it's

1 easier to change it than to argue about it? I think
2 this is going to create significant obligations on
3 people to investigate the accuracy of data that they're
4 not relying on for anything very important, just
5 because the consumer has asked that it be changed, and
6 yet they're afraid to change it in case somebody else
7 might rely on it in a way where the truth is important.
8 Thank you.

9 MR. MEDINE: I guess just to follow up on the
10 correction issue. How would you weigh in on the
11 concern that the consumer would have of getting further
12 communications from the company on Story of O as
13 opposed to Barney and his friends? Would that --
14 whether true or not true, that affects the consumer's
15 ongoing interaction with the company, is that a
16 benefit?

17 MR. BAKER: I think Rob Goldman is right, what
18 is the point of sending stuff to somebody that they
19 don't want to get? It's another piece of data that
20 they object to getting, this email on, you know, the
21 story of, you know, P, and you would be a dumb
22 company not to act on that additional piece of data.

23 MR. MEDINE: Steve?

24 MR. COLE: I would like to make three
25 observations or state concerns on three issues that

1 have come up in the last ten minutes or so. When I
2 heard Larry's formulation, I said right on, I really
3 liked it, it was very helpful, and I then I started
4 thinking about it and I started getting a little
5 concerned with where we were going here. Not with your
6 observation.

7 I have taken for granted by joining this group
8 and thinking about this issue that certain consensuses
9 have already developed, and the issue of what
10 information is collected, and how it will be used, is a
11 given. The business community has accepted that. The
12 government has accepted that. The media has accepted
13 it.

14 I would rather not see a lot of conversation
15 about that issue in this committee, unless the
16 committee wants to decide that good notice obviates the
17 need for access, and I would bet my next week's salary
18 no one is going to come to that conclusion, or at least
19 a majority won't.

20 So, I'm a little concerned that notice keeps
21 coming up as if it's still in question. And I think if
22 there's one thing, either self regulation or other
23 context, that has worked nicely in the last couple of
24 years, is that the business community gets it on that
25 point.

1 The second observation was on the transfer of
2 third party data and how that affects, and we were
3 talking about the original policies will move with the
4 data. I just want to remind you, I think that's
5 probably right, and I think it's consistent with our
6 own program standard, but enforcement is going to be
7 very, very difficult for the business community, and
8 for the government, or anyone else who gets involved in
9 this issue, because with the difficulty of enforcing
10 your terms on a third party who may not have the kind
11 of relationship with you that makes that easy.

12 And lastly, the Safe Harbor came up, and it
13 made me think about something, what was on the front
14 desk here, all the different work papers here. This is
15 very heavy and very good work, all our committees have
16 been doing. Have you all noticed that two government
17 regulating organizations got together and in about two
18 pages defined the access principle? I just leave that
19 thought to you all. I mean, and I don't know where
20 we're going in this committee, but that was a very
21 concise statement of agreed conditions of access,
22 whether it's the best one or not is fairly debatable,
23 but it wasn't quite as drilling deep into the bowels of
24 all these issues, it kind of stayed as Deirdre was
25 talking, a basic fundamental framework and it left the

1 different organizations and people a way to implement
2 the fundamental framework.

3 MR. MEDINE: Ted?

4 MR. WHAM: Ted Wham with Excite@Home. I want
5 to touch on a couple of comments from, you know, Mr.
6 Ponemon and some other people who have talked here
7 about the rights of access, Frank and so forth. And I
8 want to say that we're talking about some concepts of
9 rights of access rather airily that are -- we're
10 talking about them within the context of the online
11 world, and I want to think about if I made a purchase
12 at Bob's company and purchased some hardware and I had
13 some service contracts over time and I did an upgrade
14 and I came into the store and purchased something with
15 a check and so forth. Over time, I think he would have
16 a damn hard time telling me everything his company knew
17 about me and that certainly there's no right to access
18 of that information today.

19 If I was an audit customer of a, you know, KPMG
20 or Rick, and if I was a corporate customer, since they
21 don't typically offer their services to individuals to
22 my understanding, if I went through and said, you know,
23 when have you received all of my checks, what's the
24 history of my late payments to you, what have been all
25 of the, you know, filings that have been done, not SEC

1 filings, but other types of internal files done on you,
2 what's everything you know about me as a company, that
3 that would be an extremely difficult thing to do, and
4 that there's absolutely no right for me as a client to
5 get that information right now.

6 If I were to go to my colleague here at IBM and
7 say tell me everything that you know about me as a
8 customer, based upon my purchases and uses of your
9 services, I couldn't possibly get that information, and
10 there's no expectation on the consumer's standpoint
11 that they have a right or that companies have a
12 responsibility to provide that.

13 Yet we talk about within this context that
14 suddenly if a transaction is done online, and Larry's
15 seven-year-old goes into Toys 'R Us, that suddenly
16 there's a right of access to all of that information.
17 And I hate sounding like this, because I think I'm
18 sounding like the guy who wants to get no information
19 whatsoever. That's not the perspective that I would
20 give. On Excite@Home, there is access to a substantial
21 amount of consumer information. Effectively, most of
22 the information that we use in a decision making
23 capacity ourselves, all of the registration information
24 is available for access, it's available for change,
25 it's available for de-activation and so forth and we

1 support those types of rules. But we are talking about
2 online access and security. And I believe it is a
3 fundamental mistake for this group to suggest rules and
4 implementation that don't have an analogue in an
5 offline world.

6 If the FTC wants to say as part of fair
7 information practices that all companies at all
8 communication methods must make all the information
9 known about the customer available to that customer,
10 that's something very different than saying for online
11 activities you have to do that. And I fundamentally
12 reject the notion that there is an inherent right to
13 all information that a company knows about it, because
14 I don't see it anywhere. And until that's out there in
15 the marketplace, what are we doing trying to impose the
16 substantial cost and the substantial new burden on
17 companies that is so completely advanced beyond what
18 we're seeing in the traditional marketplace.

19 So, I thump this drum enough, I think you've
20 heard it enough from me, but before we go down that
21 path, I would look at the companies that are within
22 that business. I would look at, you know, Mary Culnan
23 and I would say Mary, can you tell me everything you
24 ever did with a student you had two years ago or five
25 years ago or 17 years ago, and you probably could, but

1 do you have to today?

2 You know, does Consumers Union have to tell me
3 everything about the address changes I have done for
4 my, you know, Consumers' Report, and all of the
5 different problems of misdelivery that I called in? Do
6 they have a responsibility to do that today? I don't
7 think so. And we should be -- tread very carefully
8 before we impose that type of burden categorically upon
9 the constituents.

10 MR. MEDINE: I would like to try given an eye
11 to the clock shift us to the access of entities and
12 really focus on that group. And again they have laid
13 out a lot of different entities who could existentially
14 provide access, data collectors, subsidiaries, parents,
15 agents, data recipients and so forth. And I guess it
16 would be helpful to start focusing people's views on do
17 all of the people in the chain have to provide access
18 and what are the criteria by which they provide access,
19 because again, it's going to be one more question to
20 focus on what kinds of information and what kinds of
21 uses, but I think it's critical to also understand,
22 again from let's get back to the point of view of the
23 website operator who may have received information from
24 a third party, what are your access obligations with
25 regard to the transfer data.

1 Rick, do you want to address that?

2 MR. LANE: Yeah, I mean I think if you look at
3 -- you know, their outline, I think it's great, because
4 it shows how many possibilities there are. And you're
5 talking about looking at it from a website provider.
6 And you look at this, and you think there are so many
7 different possibilities, and so many burdens. Heck,
8 I'm not even going to do it. And it's just too
9 overwhelming. And the concern I have, and someone was
10 talking about we need to focus this on the consumer, I
11 don't think there's a business out there that is trying
12 to sell a product or do something that isn't focused on
13 the consumer.

14 So, they're not focused on the consumer, they
15 don't have a business.

16 So, just de facto, that's the way businesses
17 think. And so privacy is being talked about by
18 everyone. It's not -- no matter where you go, no
19 matter where you read, it's privacy, privacy, privacy,
20 and with \$2.9 billion sitting on the table last year
21 because of people's concerns about privacy in the
22 online environment, a lot of businesses are looking at
23 that and they want a piece of that \$2.9 billion because
24 that's only going to increase as more and more people
25 get online.

1 So, there's a need for folks around the table
2 to realize that this is a business issue to its core.
3 It is fundamentally how we're going to deal with our
4 customers in the 21st Century.

5 The one concern I do have, we keep talking
6 about cost, you know, and we have this cost of
7 business, is that, in fact, the higher you make the
8 cost, the more burdens you place on the business, the
9 less that a customer is going to have choice of
10 services.

11 If you have so -- if I want to give all my
12 information to Excite@Home, because they -- because
13 they can provide me great products, customize, color,
14 everything so I don't have to think about anything
15 again, that can be a wonderful thing. And but the fact
16 is, if you have these burdens in place, these
17 regulatory burdens, or I happen to be able to access
18 Excite@Home, they won't offer that service.

19 So, as a customer, I'm being denied a service
20 because of the burdens of trying to protect some
21 information that no one will really care about, and, in
22 fact, you're hurting my choice of going in and using
23 all the potential services where the marketplace will
24 allow. Because if there is an opportunity for a
25 business to provide complete service, concierge

1 service, so to speak, there will be people who will
2 want that service and then give information willingly.
3 If people and your eight-year-old feel uncomfortable
4 and your grandmother feels uncomfortable or your mother
5 feels uncomfortable going places where they don't know
6 where information is being used, then don't go to that
7 site. I mean to me it's common sense, if you're not
8 comfortable with the site, then don't go. You don't
9 walk into a business that you don't feel comfortable
10 with.

11 And so the concern that I have is that we're
12 going to try to create standards in a place where
13 standards really should be determined by the
14 individuals and what they feel comfortable with. And I
15 think the Cathy comic strip was a perfect example. A
16 few weeks ago when she was running the thing on
17 privacy. She was talking to her friend, and kept
18 seeing all this information that this website had, and
19 the friend didn't care, but then she said they also
20 know you're a size seven, and the friend went oh, my
21 gosh, you know, people know that about me. And it's
22 all relevant, and so she thought people were selling
23 her size seven to other people, she'll say I don't want
24 that information being sold, and you opt out or you
25 don't go to that site. And so we have to look at some

1 personal responsibility here and not just look at let's
2 mandate everything from the top down.

3 MR. MEDINE: Again, how would you translate
4 that into the downstream uses of the data? I mean,
5 again, that focuses -- this group is -- this discussion
6 is -- let's assume perhaps that the person you do
7 business with is going to provide you access to your
8 data, how do you translate those principles or those
9 concerns into the entities that receive the data down
10 the line? And the consumers not necessarily having a
11 direct interaction with those entities?

12 MR. LANE: Well, I think that's the problem.
13 If they're not having a direct -- if I have opted out,
14 and I don't want certain information used, and they go
15 ahead and use that downstream, then obviously there's a
16 course of action. You can go to the FTC, there's other
17 ways of going about, and there are groups out there
18 that did check this out, thank goodness, like the CDTs
19 and others out there are constantly monitoring this
20 type of activity. So, if you're -- if they're giving
21 that they said that they wouldn't give, then obviously
22 there is a problem there, and I think we all agree with
23 that.

24 Now, if you have agreed to that and you know
25 where the information is going, it's going to be kind

1 of impossible to say here are all the places we sell,
2 because that's also a confidential proprietary list.
3 So, if you don't feel comfortable that it's going to
4 third parties, then you can obviously, and we talk
5 about choice and everything else, opt out of that or
6 not go to that site.

7 MR. MEDINE: Alex?

8 MR. GAVIS: Alex Gavis from Fidelity. Tim, you
9 had talked earlier about the cost of access and whether
10 it would be passed on to consumers, and I think it's
11 important to focus on that, particularly in light of
12 this area.

13 I think ultimately if we put too much in the
14 way and really put the tremendous number of
15 requirements in this space, there will be costs that
16 will be passed on to consumers.

17 In particular, I think it's important to focus
18 on the scope of access. It seems to me it would make
19 sense that there should be one single point of access,
20 that the customer should go through with a company, one
21 pipeline in which to get information, and then from
22 that, there should be a sense of what the means of
23 access should be, because that can drive the costs.

24 In other words, if access means being able to
25 call up on a telephone and interview the company for

1 every piece of information, that will have a much
2 different cost than actually having a format, for
3 example, where there's a specified format that can be
4 conveyed to the customer through a website, that would
5 be much cheaper.

6 And then in terms of dispute resolution, how
7 should the consumer actually dispute something or
8 correct their data, and what kind of costs are
9 associated with that. So, I think as we define each of
10 these areas, ultimately, it's going to result in costs
11 being borne by the company, which ultimately will be
12 passed on to the consumers.

13 And it's important to think about that,
14 particularly since if we adopt something that goes on
15 -- that actually is too complicated, or allows a large
16 amount of access rights, not all consumers may want
17 that, and the few consumers who want it will be placing
18 burdens on the rest of the other consumers.

19 MR. MEDINE: So, translating that into this
20 particular discussion, are you suggesting, then, for
21 efficiency's sake, that such a one-stop-shop for
22 consumers, and that is that the data collectors, the
23 entity that provides access, or who in the stream in
24 light of that discussion ought to be providing access
25 to information that may be transferred to subsidiaries,

1 parents, agents and so forth?

2 MR. GAVIS: I would think that the entity to
3 which the consumer does business with within the
4 corporation should then be looked to provide access for
5 information, and then the question is, how far along
6 the stream does that entity have to reach, or how far
7 or to what other entities does that entity have to pull
8 information from to give to the customer, I think
9 that's the question that we need to think about.

10 MR. MEDINE: Tom?

11 MR. WADLOW: Tom Wadlow, Pilot Network
12 Services. I wanted to react to something that the
13 gentleman from the Chamber of Commerce said about
14 personal responsibility and if you don't like what --
15 how the information is being used, don't go to that
16 site. Deirdre mentioned earlier about the phone
17 records in Europe, and how, in fact, a great amount of
18 that information was protected, you didn't have the
19 right to see who else called on the phone and in fact
20 they do a great deal of protection there, and I don't
21 know if anybody -- I'm sure, actually, quite a number
22 of people in this room are aware that the reason for
23 that is the way the phone records were used in World
24 War II. And I don't think it was the case that the
25 people before World War II thought that using the phone

1 would have the impact on their lives that it did.

2 And so I think it's very important to realize
3 that, you know, one of the reasons why I participated
4 in this, and one of the reasons why I'm sure a lot of
5 the other people did, is that we in this room have a
6 much better sense of what the problems are with things
7 like that. It's easy to say don't go to that site, but
8 you don't really know the implications of going or not
9 going in either case, and because we are here doing
10 this, we think about these things every day, as Andrew
11 said.

12 You know, we have a much better sense of what
13 the implications of those decisions are, and also how
14 -- how widespread they can be, and I think if nothing
15 else came out of this but a sense of how widespread
16 some of the implications of what you type into a
17 browser can be, I think we would have served our
18 purpose.

19 MR. LANE: If I can just respond to that. I
20 agree with that. Because if you think about how -- I
21 mean obviously, what is happening in the EU, obviously
22 they have a different mindset, because of what they've
23 gone through compared to the U.S. But from the
24 business standpoint, and again, I think we all are
25 aware, and I think it gets back to the education. If

1 people understand, and that's why I think this is a
2 good process, understand how the information is being
3 used, I think we're on the same page. Because if you
4 understand that, you may not want it to be used. And
5 then you won't go to those sites, because of concerns
6 that you may have.

7 And I think what we don't want to do is if you
8 think about somebody who comes from France or Germany
9 where they're used to having really high levels of
10 privacy, they're going to react differently to sites
11 and go to the sites that they feel comfortable with,
12 because I don't think we want to go to AT&T or MCI or
13 anyone else and say we don't want you to have anymore
14 listings of phone numbers, because it's a concern of
15 some other folks.

16 Because I know from a business standpoint, we
17 like those listings, because we like to argue with the
18 phone company on our bills. And so there is a
19 difference, and that's why from market standpoints, you
20 allow that sensitivity. If I'm oversensitive, again,
21 from my standpoint, I like customization, but there are
22 others in this room who do not. Let those people, you
23 know, kind of decide, and obviously you want to have
24 notice and we all support, you know, some of the
25 guidelines out there, but we don't want to have it so

1 restrictive that you're denying my choice as an
2 individual to go places that I would like to have a lot
3 of customization because the costs are so high that
4 they just can't implement it.

5 MR. MEDINE: I'm getting the sense that people
6 don't want to talk about entities as much. Good, let's
7 hear something from Deirdre.

8 MS. MULLIGAN: I actually promise to talk about
9 entities, but I think that the first question, which
10 entities are required to provide access to data should
11 actually be which entities can provide access to data,
12 again going back to the okay, if you can, then there
13 may be some mitigating reasons why you should not.

14 This may sound really bizarre coming from me,
15 but I'm really not interested in micromanaging the
16 decisions of a business, whether or not they provide
17 access at one point or multiple points, I don't care.

18 And I think to the extent that we can allow
19 people to maintain flexibility over whether they
20 centralize an access point or provide multiple access
21 points, I would like to see it migrate in a way that
22 it's easy for consumers, but I don't think it would
23 serve us very well to micromanage a business practice
24 as to how access is provided, other than to say it
25 should be simple. There should be an access point.

1 But I think that if you can provide access,
2 right, so if I have -- if I'm a bank and I have
3 transferred some information and Greg now has
4 information about the customer with their name and
5 attached to it and the customer now comes and says what
6 do you have on me? Well, they clearly can, so are
7 there reasons that she should not?

8 And I want to push back once again and start
9 from the if you can do it, let's acknowledge it, and
10 then let's talk about are there costs that need to be
11 thought about, okay, so maybe the costs favor Greg
12 sending people back to me in a simple way. Maybe the
13 costs say provided at every single point. He's using
14 the record, he is, you know, sending it out to other
15 people, it's easy for him to pull it up and give it to
16 me. Maybe he charges me the cost of the paper.

17 Are there risks? I think when we -- the area
18 where the which entities are required, it's which
19 entities are required to correct. Now that's I think a
20 real issue. I think there are real risks to allowing
21 him to correct data that might have originated with me.
22 They're not the same risks. If I happen to be a doctor
23 and I've transferred information to the insurance
24 company, the patient might get access there, but they
25 can't correct my diagnosis. You know, they have to

1 come back to the doctor.

2 So, I think there are risks that we have to
3 acknowledge, but if it is possible, we should say yes,
4 it's possible, and then look at what are the mitigating
5 factors.

6 MR. MEDINE: Greg, you had your flag up. Do
7 you have an entity comment?

8 MR. MILLER: Actually I do.

9 MR. MEDINE: Good.

10 MR. MILLER: Greg Miller, MedicaLogic. Just
11 kind of in furtherance of that. If we determine that a
12 recommendation is that there is some sort of definition
13 for a covered entity, that is an entity that would be
14 subject to follow these guidelines, then we need to
15 cover what happens when there's a recipient who isn't
16 otherwise a covered entity.

17 A quick example that we ran into at HHS that
18 was sort of bizarre. Let's suppose that you decide
19 that you want to go pay for health care services at a
20 clinic and you really do not want to involve your
21 insurance, and you decide that you're going to pay
22 cash, but you unwittingly decide to use your debit card
23 at the counter to pay cash for these services rendered.
24 A bunch of data is sent off to the merchant bank that
25 receives that information.

1 Is the merchant bank now subject to the same
2 rules and regulations with regards to receiving that
3 health care data that a covered entity is, thus has
4 borne the beginnings of a business partner.

5 So, in addition to the covered entity, you have
6 a business partner. And then the question to
7 enforcement becomes do we create this so-called chain
8 of trust, in which we require that business partners
9 and covered entities agree to conduct themselves in a
10 reciprocal manner, such that unfortunately the downside
11 is, I become liable or responsible for the bad acts of
12 my downstream partner, and as Dan would enjoy,
13 recursively so.

14 So, I think that one of the things we may want
15 to look at with regard to entities is do we come up
16 with some sort of a notion of a covered entity and a
17 business partner, and then do we recommend that there
18 is some notion of a chain of trust that's built that we
19 will all conduct ourselves in a reciprocal manner so
20 that the consumer has some sort of a certainty as
21 potentially a third party beneficiary that they may
22 have some recourse, if somebody breaks the chain.

23 MR. MEDINE: Roger?

24 MR. KIRKPATRICK: On Deirdre's question of the
25 costs, I would just like to give one example of a cost.

1 I'm in Time.Inc., and certainly at Time-Warner
2 generally, but just certainly a lot just in Time, Inc.,
3 we have many different data centers. It's not just one
4 monolithic data center. And those data centers
5 generally correspond to the business operations. And
6 those data centers are not merged because the business
7 operations are not merged.

8 One of the concerns that we're constantly hit
9 with, or not we, the company, but we constantly hear,
10 is that people, privacy advocates don't want those data
11 centers merged all the time necessarily, especially
12 over big companies. If we're required to define access
13 to mean everything Time, Inc. has is okay, or even out
14 further, everything that Time-Warner has, the only way
15 we're going to be able to give that access is to merge
16 the data centers, which on the other hand people don't
17 want us to do.

18 So, I would propose that the best way to look
19 at it is from the reality of the business operations,
20 and one of the lenses that can be put on that, to
21 take an analogy from other FTC experience, is who does
22 the customer think they're dealing with? I mean, when
23 somebody buys People magazine, they don't think of
24 themselves as dealing with Time-Warner, they generally
25 don't think of themselves even as dealing with Time,

1 Inc., they think of themselves as dealing with People
2 magazine. And I think that's a good way to look at it.

3 MR. MEDINE: Thank you. Dan?

4 MR. SCHUTZER: I was on the group, and so I
5 want to say what we would do is we would just stream of
6 consciousness with a view towards a draft and as I look
7 at it, you know, I have some of the same confusion you
8 have. So, I'm going to suggest a framework, after
9 thinking about it for a while, and throw it out and see
10 what you think. Why were we doing entities when it's
11 really about the question of who has to provide access,
12 and also who gets the ability to correct or question.

13 So, I agree with a lot of the things you said.
14 By saying who can provide access, we're addressing the
15 issues of in terms of two things, one is if there's
16 companies and subsidiaries of companies and so forth,
17 at what level do we want them to provide access, and
18 that's a complicated question, and indeed in many of
19 our instances, like in my company, we have to have
20 Chinese walls between some of these, so it would not
21 even be possible to give you a central point where you
22 could come into an insurance company and see access to
23 your brokerage account, for example, because we're not
24 mingling the information in that way.

25 But if that's not an issue, you know, in other

1 words, if we're -- if we have a consensus that says
2 that within this group, it's up to the corporation to
3 decide that they're maintaining the information,
4 whether they provide you a consolidated or a
5 suborganization level or so forth, then it's not
6 necessary to define that as an entity.

7 If we have something to say in terms of
8 options, about whether it's maintained at a corporation
9 or a subsidiary or a department, then it's important to
10 define that distinction.

11 Another distinction is intermediary, again, if
12 we have something to say or not, what we meant by that
13 is if you have a third party where the information is
14 passing hands, but they're not maintaining it, they're
15 just somehow in the process of transposing it or
16 distributing it, they probably don't have to maintain
17 access, but if they are also storing this information
18 in some way, then they -- then they're a legitimate
19 company that would have to have access, whether a
20 partner or affiliate or not.

21 So, that's one issue. An entity class that we
22 didn't talk about, Frederick brought up, are the
23 entities and who has the right to access the
24 information. And there I would say the issues there
25 when we talk about entities, we're talking about legal

1 entities, corporations, individuals, households and the
2 like, and I would think there that some of the options
3 would be that if people have the right to access that
4 information, that's the degree to which we could
5 distinguish who they are.

6 So, I'm only collecting the information at a
7 telephone number level or an email level or an ID
8 level, all those who could share that have the right to
9 access that information.

10 And now we have to get down to well, who has
11 the right to collect the information, and I would think
12 that we want to ask two questions. Who has the right
13 to question the information. If you have access to the
14 information, I think you have the right to question the
15 information and get back to substantiation from the
16 person maintaining the information as to why they
17 maintained it. I don't think you necessarily have the
18 right to correct the information. In the sense that
19 you could get on and correct the information.

20 So, who has the right to correct the
21 information? I guess it would be if I can authenticate
22 myself properly, that I -- that I'm certified the right
23 person, that I don't not only see it but correct it,
24 and that is the kind of information that's information
25 that I have provided, not that it was inferred or

1 derived from it, and I can certify the information, you
2 know, then sure, I have the right to correct it, but if
3 it's someone who cannot authenticate it and can't
4 certify the information you're providing, they could be
5 corrupting my database, they have a right to question
6 it, to provide alternative data that I would have to
7 respond to, but not necessarily online to correct it.

8 So, I don't know if you agree with all those
9 things, but that would be the nature in which we would
10 have to want to define the entities, and only for those
11 purposes.

12 MR. MEDINE: I'm glad you mentioned the word
13 authentication, because I hope there are a few more
14 comments on entities and we can also transition into
15 the authentication discussion as well. John?

16 MR. KAMP: Yes, I was also a member of the
17 subcommittee, and I wanted to share with the committee
18 some of the thoughts that I had as I went through this.
19 Because as I -- if we -- if we look at many of these
20 wonderful and fine distinctions, I was reminded of the
21 days that when I first came to Washington for the first
22 couple of years I was a rule-making attorney. I was an
23 attorney in an agency very much like this who had to
24 take the piles of documents, I remember my first
25 rule-making had 20,000 comments, and then draft

1 something for the agency to look at and then decide,
2 make the public policy choices.

3 And I'm worried. As I went through this
4 process in my subcommittee, I actually like all the
5 rest of us really, really was sort of delighted to make
6 sure that we had the full range of all the
7 possibilities and machinations that ever could be in
8 there so that we made sure that the Commission knew
9 everything it could possibly know about this issue
10 before it made a decision.

11 But as a rule-making attorney, I can tell you,
12 it doesn't help. This is very complicated stuff, and I
13 think that we as a committee have to start thinking
14 now. I think we're finished with the stage of
15 broadening all of these ideas and getting all those in
16 there. I think we have to do the best we can now to
17 help the Commission make this simple.

18 And in fact, I think Frank Torres of our
19 subcommittee who brought to me something I had actually
20 read and paid attention to and I think it's -- I
21 recommend for the reading of all of you in this
22 committee, and that is the material done by the
23 Commerce Department, and partially with the Federal
24 Trade Commission on these very issues that it's
25 essentially the policy of the government in its

1 discussion about access and security and notice and
2 other things, stemming out of the OECD guidelines, and
3 its EU negotiations on these matters. And they're all
4 available on the Department of Commerce website and
5 there's a tremendous amount of intelligence there about
6 these issues, and as Steve Cole said just a few moments
7 ago on access, the FAQ part of it is only three pages.
8 And I think there's a lot of intelligence there and I
9 think it's a very useful point of departure for us or
10 at least a point of reference for us because it is the
11 stand of the government on these issues at least in one
12 context and I think it helps instruct us.

13 It also should help instruct us that we have a
14 very difficult job ahead of us in the next four to six
15 weeks, because we've got to make this material
16 intelligible to the government, so that they can write
17 rules that not only business can understand and
18 implement, but the choices that consumers make are
19 choices that are real, intelligent choices, but they're
20 choices that they're going to be willing to make with
21 the mouse in their hand, while they're trying to get
22 some place else.

23 And they're only going to want to make --
24 they're going to make these for the most part, they're
25 going to inform themselves of what the general

1 principles and stuff, but they're going to want to make
2 most of these choices in seconds or milliseconds,
3 perhaps. And we've got to now help the Commission
4 simplify and clarify these matters. We've got to make
5 -- we've got to take this stuff that we've got here and
6 put it in a page and a half or two pages.

7 MR. MEDINE: Since you used Frank's name,
8 Frank.

9 MR. TORRES: Thank you. Frank Torres from
10 Consumers Union.

11 Just a couple of comments that were most
12 recently made. I had never thought I would see the day
13 when I actually agree with somebody from the banking
14 industry, I actually appreciated those comments because
15 they were very reasonable in their approach. And I
16 think that's something that the issues do get kind of
17 complicated and I think now we're getting more back
18 into the reality of the situation, and I don't think
19 Dan's comments were any different from what Deirdre was
20 saying a little bit earlier in does it really matter
21 who is providing access, as long as access is provided.

22 And it's meaningful and it's complete and I'm
23 perfectly willing to leave that to the entities that
24 are collecting the data and then sharing it amongst our
25 affiliates or with others to make that determination.

1 As long as it's simple for the consumer to understand,
2 you know, how the information is flowing, to allow one
3 access point, if that's reasonable for you to do, or to
4 say go to the People magazine site that first collected
5 the information, and they'll be able to help you out.
6 However the determinations are made so that it's
7 complete, I think that's good.

8 When it comes to the ability to correct
9 information, it strikes me as any information that you
10 can have access to, or that is out there that's wrong,
11 should be corrected. Now, that brings up the
12 authentication question, which is important and in
13 addition to the Safe Harbor, I think the Fair Credit
14 Reporting Act can -- the documents related to the Safe
15 Harbor, I think the Fair Credit Reporting Act can
16 provide some guidance into reasonable approaches to
17 correct the information and who should be responsible
18 for assisting in that process.

19 What I like about the safe harbor, and we don't
20 necessarily agree with everything that's in it, but it
21 strikes me as it takes a reasonable approach, it says
22 things like cost is a factor, but it's not the
23 controlling factor. When it comes to things like
24 financial information or information used to make
25 decisions about how much something costs a consumer, or

1 medical information, then cost really doesn't matter.

2 Consumers should have access to that
3 information, and it should be fixed if it's wrong.
4 When it comes to other things, then, you know, maybe
5 cost comes into play. If it's going to cost you a lot
6 of money to provide me access to my name and address
7 that you've got somewhere aggregated. Well, maybe it's
8 just enough that you've got my name and address. I
9 don't need to -- and so there's some balancing that
10 goes on there. And I think that's important.

11 MR. MEDINE: Thanks. Jerry?

12 MR. CERASALE: Thank you, Jerry Cerasale. I
13 wanted to respond to the -- just respond to the example
14 that Greg gave on the medical information, and say that
15 it's -- it may not be the best example to try and think
16 of, because it raises a question I don't think anyone
17 has talked about. We're talking about going to the
18 clinic, wanting to pay cash, but somehow paying with a
19 debit card, and then that information goes off to the
20 bank, and then does the -- all the limitations on the
21 medical record go downstream with that.

22 He entered into another customer relationship
23 with another notice requirement and another agreement,
24 because I chose to make a -- an agreement with the
25 bank, and I chose to use the bank, and I had some

1 information agreement with the bank so that there's
2 that type of example raises a second round of separate
3 customer relationship in the same single transaction,
4 and I don't know if that raises another complication as
5 you look at entities and access and what type of
6 access, and so forth down that way. But I think that
7 that's -- it's important to understand the agreement
8 that you have and go down at the end and look at it.

9 I also think we have not discussed, and I'm not
10 going to raise it, it's going backwards, but I don't
11 think we discussed use well enough that was in the
12 first group, nor have we discussed access costs and
13 charges that you might want to apply. We haven't
14 discussed that at all. I think those are important
15 factors, factors wherein even the Fair Credit Reporting
16 Act allowed people to charge, but suddenly laws are
17 being made that it all has to be free, so we have to
18 think about that so that there are significant added
19 burdens that say that you can charge the cost of what
20 it takes is one thing.

21 Another idea on cost is what happens if you --
22 if Jerry Cerasale goes out to write everybody you
23 probably can to look at what kind of access you have --
24 information you have on me, and you get a lot of nulls,
25 that nobody has any access. And I constantly ask

1 should there be a burden on me for harassing somebody
2 who doesn't have information on me to try to get access
3 to the information, should there be an additional cost
4 and things of that sort. Thanks.

5 MR. MEDINE: Stewart?

6 MR. BAKER: Thanks, Stewart Baker. I think
7 we're down to the point on the end of these questions
8 where we really have the three options, thinking in
9 terms of simplifying this, which entities should be
10 providing access, one option is nobody. I've kind of
11 gotten my sense that I think this right of access has a
12 lot of costs for privacy and for business, and some
13 rather dubious public policy values, maybe it should be
14 available when someone feels that they are actually
15 suffering a harm as a result of incorrect information,
16 they have some reasonable basis for believing that
17 these Story of P promotions are based on inclement data,
18 but a very limited access is a possibility.

19 The other is the data collector, and there's an
20 awful lot of consensus for that, that whoever collected
21 the data is the place you would go and if they have
22 access to it, then they provide it back to you. And
23 that matches what business practices are, you know, if
24 you've got access to it, then you ought to produce it,
25 and it doesn't add to your cost.

1 And the third is somebody else, too. And this
2 is the business partner issue, or the subsidiary issue,
3 here I think that we haven't explored the costs of
4 saying somebody else, too. This is a circumstance, at
5 least in my taxonomy, where the party who originally
6 gathered it no longer has access to this information,
7 or it's been mixed up with other information by
8 somebody else.

9 In those circumstances, to say if you enter
10 into a business relationship that involves data with a
11 website that's covered by this rule, you're screwed, is
12 a way of discouraging people from entering into
13 business relationships with web sites that are covered
14 by this rule.

15 You kind of create a class of typhoid Mary
16 data, that cannot be shared, that has to be
17 quarantined, so that it can be provided back to
18 customers as a result of these indirect requests. I
19 think that's a substantial risk in an area of
20 regulation that we've never explored before in pursuit
21 of benefits that are a little dubious. And so I
22 suggest that we might be able to break it down into
23 those three options in this area.

24 MR. MEDINE: Ron?

25 MR. PLESSER: Well, three points. One is I

1 think Ted Wham made a good point about how this isn't
2 in the electronic media, why not the nonelectronic
3 media. I think we have to face the reality that if we
4 do this and the Trade Commission does this and calls
5 for access, that it is almost -- it will be impossible
6 to distinguish between the, you know, the nonelectronic
7 and the electronic.

8 The New Yorker had this wonderful article about
9 clicks and mortars and about how the two worlds are
10 absolutely united and anybody who hasn't read that
11 article should, because it absolutely makes the case
12 that you can't distinguish, you know, there's not two
13 worlds out there.

14 And so I think that we're even really Ted
15 looking at a worst scenario, because not only are we
16 driving electronics, but I think we have to be clear
17 that we're probably going to drive what's going to
18 happen in the nonelectronic world as well, and I think
19 that's why there's a lot of sensitivity on this.

20 Number two, I think we do have to talk about
21 entities that are required or should provide access. I
22 think to just simply say can you provide access, and
23 deal with it in the cost, sweeps away a lot of issues
24 that I think a lot that Stewart was alluding to in
25 terms of, you know, do you want the data process or to

1 provide access, does Federal Express, who's delivering
2 on behalf of L. L. Bean, do they have what we call the
3 food chain line? Do those people who are simply really
4 agents of the first collector or the first, do you
5 really want them each to have it, it seems to me those
6 are qualitative decisions. Federal Express probably
7 could provide it very easily, it's probably the cost is
8 very low to it, but it seems to me there's some issues,
9 because then do they get to create independent client
10 relationships, what is the -- there's a lot of
11 implications from a commercial and privacy prospective
12 if you're L. L. Bean, do you really want your customers
13 going to FedEx to make the inquiry.

14 Cost may not be an -- I'm not speaking for
15 either of the companies, I'm just using them as
16 examples, but Fed Ex is pretty sophisticated, they can
17 find out most information pretty quickly.

18 So, cost is not a factor. I think we have to
19 deal with whether or not, you know, this is desired,
20 required, appropriate, we can't just totally eliminate
21 the subjective, you know, judgment here and make it
22 only a cost judgment.

23 And then finally, I think this whole entity
24 issue and the subsidiary and the policy and this whole
25 thing that we keep on coming back to, it's always been

1 to me fairly straightforward in looking at this over 25
2 years, that basically, and I think that my friend from
3 Citicorp essentially said the same thing, it's self
4 defining. You know, everybody should have a right of
5 access. The question of, you know, is Citicorp going
6 to take responsibility for everything under its
7 umbrella, or Time-Warner is a better example that
8 you're familiar with, or do you say Warner Brothers has
9 an access position or title?

10 It's really self defining, and I think that --
11 and it's part of the notice. I think to sit down and
12 try to make governmental decisions on corporate
13 structures is going to be extremely difficult and
14 controversial, and I think the easier way is to say
15 every consumer has to have a right of access to this
16 data, as related to the transaction, but then it's kind
17 of up to the collector to decide how they want to
18 define themselves, and that has a lot of implications
19 in terms of who they can disclose it with and when and
20 under what circumstance, but I think basically it's a
21 self defining operation.

22 MR. MEDINE: I assume you agree with that, but
23 going back to your point before that, what is the
24 principal basis on which you decide how far down it
25 line you go with transfers to subs and third parties

1 and affiliates in terms of providing access to the
2 data? You said not FedEx, but what other kinds --

3 MR. PLESSER: Well, Fed Ex is an agent, but I
4 think if you look at Time-Warner, I think it's self
5 defining. If Time-Warner wants to say that it will
6 provide access to every subsidiary, that's their
7 choice, or if they say the subsidiaries alone. But
8 then, you know, they may be limited in how they can use
9 it internally.

10 MR. MEDINE: No, if you accept that -- accept
11 for argument that you -- the entity that the consumer
12 has interacted with, whether it's People magazine or
13 Traveler's Insurance, is the one that provides the
14 access to their data, their part of the company, the
15 question still is if they transfer data to third
16 parties, what principles do you apply to which third
17 parties do you get to go to for access or do you have
18 to go back to People or Traveler's to get your access?
19 How do you decide how far down the line, assuming your
20 data is being transferred?

21 MR. PLESSER: There has to be a principal point
22 of responsibility, and I think that you can define that
23 in the notice, but I -- and I don't have so much
24 problem, you know, that people can define it, and they
25 can define it as themselves, or they can define it as

1 Time-Warner, but what I'm more concerned is, that
2 they're not required -- that FedEx, who is a different
3 -- that they don't have an independent requirement or a
4 processing company, if somebody is -- EDS is processing
5 data for a hospital, you go to the hospital, you don't
6 go to EDS. It may actually be cheaper for EDS to do
7 it, but you want to force it back to the institution in
8 which at least there was some level of consumer
9 relationship.

10 MR. MEDINE: David and then Alex, but let's
11 also if we could try to blend in the authentication
12 discussion, and one of the -- as we move forward,
13 because one of the issues that seems to come up in the
14 authentication discussion is a balance between
15 gathering more information from the data subject in
16 order to authenticate them and how do you -- is there a
17 privacy concern constructing the balance between
18 properly authenticating somebody and comparing the
19 information that they have already provided to you.

20 MR. WHAM: A schedule clarification.

21 MR. MEDINE: I am going to propose we break in
22 about ten minutes for lunch. There was a proposal that
23 we try to be back in an hour to try to expedite things
24 and even try to get out early, so I propose we break
25 for about ten more minutes and then break for an hour

1 for lunch? Are people agreeable to that?

2 MR. DAVID HOFFMAN: Yeah, I think that I can
3 make the connection that you asked for, David. First,
4 I would like to commend Rob Goldman, by the way, who
5 did the bulk of the work to pull together this piece,
6 and I actually think we found in our subcommittee this
7 is extremely difficult, this area, and I actually think
8 there is a tremendous amount of guidance hidden in the
9 commentary here. We need to flesh it out more, but I
10 think it's there.

11 The key area, or one of the most key areas that
12 we had the most difficulty, and I think Stewart pointed
13 this out, and I like the way he defined his subgroup as
14 the somebody else, too. And the somebody else, too, I
15 have a lot of concerns that if we take what I will call
16 the Richard Purcell and Greg's idea of the chain of
17 trust, which is what I think the question you were
18 asking Ron, I think it's impossible. I don't know how
19 -- I don't know how you would do that, where you define
20 how far they have to go. Once you -- when we looked at
21 third parties, we said one of the things that makes it
22 hard -- difficult to deal with third parties is their
23 -- we can separate it into two different categories,
24 and Ron talked a little bit about this. Agents, and
25 other -- and other third parties that you are

1 transferring information to.

2 And the way that we defined agents was to say
3 that when you have an agent, you don't have online
4 transfer beyond the agent, because you have obligated
5 the agent not to transfer to someone else. You have
6 also obligated the agent not to use the information
7 other than for the express purpose that you have
8 already disclosed to the data subject, that that
9 information is going to be used for.

10 Agents is much easier in my opinion, my
11 personal opinion there, is that the data collector that
12 has hired the agent has the obligation to go back to
13 that agent, find the correction and if a correction
14 needs to be made, make that correction. The other
15 difficult task is this whole idea of this chain of the
16 onward -- now that the onward transfer has been allowed
17 to someone else.

18 My opinion there is that we shouldn't even go
19 down that road, given the fact that I think under the
20 current principles that have been adopted by the OPA
21 and by the -- EU's data collection directive, if notice
22 is given that the data is going to be transferred to
23 another entity, then once the understanding has been
24 given to the consumer, data is going to be transferred,
25 and where it goes from there, no one is going to have

1 any idea.

2 To try to put an obligation upon the entity
3 that first transferred that data to have to track down
4 the chain of trust, and then to put an obligation on the
5 entities that receive that data. Number one, unless
6 we're going to -- which I am not recommending, to
7 increase the scope of this to also include offline
8 data, that they have to categorize what was obtained
9 online versus offline, but then to try to figure out
10 some way to authenticate data from someone that they
11 never received the data from themselves I think is too
12 hard of a task to take.

13 MR. MEDINE: Alex?

14 MR. GAVIS: I would like to say that one point
15 is that came out of the Gramm-Leach Bliley, which
16 recognizes that corporations have a number of
17 affiliates that they may share information with and
18 that they may also share information with third
19 parties. In both cases, you have a specific obligation
20 to provide notices to what you're doing with the
21 information, and then particularly with the third party
22 sharing, if it's for marketing purposes, or for onward
23 transfer purposes, the ability to provide the customer
24 with an opt-out.

25 If, in fact, it's for agency purposes, for

1 example, for servicing accounts, or for processing
2 transactions, or even, perhaps, for marketing purposes,
3 where you're hiring an agent to fulfill for you or to
4 actually help you understand marketing information, you
5 don't necessarily have the need to provide an opt-out
6 in those circumstances.

7 I think that model, and it focuses on the
8 notice, but then it does provide rights later on with
9 respect to the onward transfer is a fairly powerful
10 one.

11 MR. MEDINE: And how would you translate the --
12 those rights into the access context, that is if you --
13 if you are subject to a notice and opt-out about the
14 transfers and the transfers take place, then what with
15 regard to access from the onward transferred company?

16 MR. GAVIS: Well, particularly on the first
17 part with sharing among affiliates, the context that I
18 would put out earlier where the customer actually
19 contacts the corporation and then there is other
20 information that the corporation can share, that would
21 be provided through that entity. If possible, if there
22 aren't regulatory barriers for sharing that
23 information.

24 With respect to third party sharing, to the
25 extent that the information is being used in an agency

1 or servicing capacity, obviously the corporation would
2 have an obligation to reach into that entity, if
3 necessary, and provide the data back.

4 If it was going to be used for onward transfer,
5 simply sold to a third party, given away, whatever,
6 bartered, clearly the obligation is -- that's where I
7 think we need a discussion, which is how do we treat
8 that, should we find the corporation to be a little bit
9 more responsible and go to that third party and try to
10 correct things. Or is it really just a question of the
11 notice is good enough, the customer knew when they
12 entered the transaction or when they entered into the
13 relationship that, in fact, this was going to happen,
14 they were given the ability to opt out, they didn't opt
15 out, and therefore now the information is with that
16 third party. It's their responsibility to go to the
17 third party.

18 MR. MEDINE: Okay, let's take Lorrie, Steve and
19 Deirdre and then we'll break and can pick up on some
20 loose ends on authentication before quickly moving to
21 the security discussion after lunch.

22 MS. CRANOR: Lorrie Cranor. So, back to what
23 you just said, if the notice is good enough, I think
24 that may be an issue in that somebody said we're
25 assuming that notice is a given, we're already doing

1 notice, but in fact notice about sharing data with
2 particular affiliates and third parties and agents is
3 not, I don't think, very good.

4 And I think there is -- the Fed Ex one is
5 actually a great example, because while there may be
6 some companies that enter into agency agreements with
7 FedEx, there are other companies, especially small
8 businesses, that just drop the Fed Ex thing into a box.
9 And I have actually gone to the Fed Ex box and looked
10 for information about what they do with data, and they
11 don't tell you. I don't know, there are other shippers
12 that actually in their privacy policies explicitly say
13 that they have the right to use data about who's
14 shipping to whom for other purposes, and there's no way
15 to opt out of that. And so I think sort of this up
16 front notice is not actually happening. If we had the
17 notice, the access might be a lot less of an issue.

18 MR. MEDINE: Steve?

19 MR. COLE: This third party transfer discussion
20 is harkening me back to our conversation about the
21 by-laws the first week and I will tell you why in a
22 second. I've heard the term rights about a half a
23 dozen times. Greg mentioned the word liabilities a few
24 times. We're talking about whether the companies are
25 bound or not. And I'm sitting back thinking after

1 today, we're going to be drafting a committee report,
2 and we really don't know what the purpose of the report
3 is.

4 And it matters into what the recommendations
5 are. If it's best practices, that's one thing. If
6 it's giving advice to self regulatory organizations
7 about what their standards ought to be that companies
8 voluntarily opt in or don't, that's another thing. If
9 it's regulatory requirements, that's another.

10 And to me, it has a very practical
11 significance. If we're talking about proposed
12 legislation, the company's inability to bind its
13 partners can be taken care of. Congress could bind the
14 partners, or the Federal Trade Commission, arguably, if
15 you have federal rule making power.

16 So, we're going to be drafting recommendations,
17 and without knowing the answer to what this report is
18 for, you can't answer any of these questions.

19 MR. MEDINE: Deirdre?

20 MS. MULLIGAN: Okay. I guess I want to respond
21 to two pieces of what I consider to be slightly perhaps
22 inaccurate statements.

23 First, I mean referring to Gramm-Leach-Bliley
24 is kind of ironic, since there are absolutely no access
25 provisions in the Gramm-Leach-Bliley bill so I want to

1 know we have on the table that there is absolutely no
2 right to access and in fact there's a very limited
3 right to notice.

4 The EU directive, in fact anybody who has
5 personal information, whether they bought it, got it
6 from the consumer, regardless of how they got it, is
7 governed by the directive. Which includes access
8 rights. So, it doesn't matter. And I find it kind of
9 ironic that a business who purchased data, imagine it's
10 a long list of information with individuals' names, a
11 huge marketing list, and they purchase it, versus
12 another company that collected it directly from a
13 consumer.

14 The company that purchased it would be in a
15 better position, because they wouldn't have to provide
16 any access to consumers, because they bought it from
17 somebody else, versus I mean this is the scenario we're
18 setting up, that if you purchase the data from another
19 business and you are, in fact, a secondary user of the
20 data, but you wouldn't have to provide access,
21 potentially, versus the person who actually collected
22 the data from the consumer, probably did give them, if
23 we set up the perfect scenario, a notice and a choice,
24 and they would have to provide -- I mean, I find it a
25 little ironic, and I think it would be pretty important

1 to look at the business implications of treating two
2 businesses that have the identical data set at their
3 disposal with different rules based on what the source
4 of the data was. I think that might be a little
5 problematic if you think about the economic
6 implications.

7 And then the third, I do want to just go back
8 to the question of I completely agree with Ron, that
9 there are issues that go beyond cost that need to be
10 explored in thinking about is this the appropriate
11 place to provide access, do we provide access at all,
12 itself. But I think the first question you have to ask
13 is can you provide access. I think there are entities
14 that purchase data and then merge data and take out all
15 the qualifiers, so I think they provide access.

16 And so framing the discussion is it possible?
17 Are there reasons not to? Are there business
18 implications? Are there costs? Are there interests?
19 You know, all of this factual stuff, we need to put
20 down in a consistent way. And I think it can inform
21 our discussion about access, about correction, and even
22 about security, if we stick with a -- with a consistent
23 framework.

24 MR. MEDINE: Thanks. I was again informed that
25 the -- informal pol suggested that we would like to

1 have a shorter lunch break than an hour so we can get
2 back to business quickly. So, along those lines, I'll
3 see everyone at 1:15. Thanks.

4 (Whereupon, at 12:15 p.m., a lunch recess was
5 taken.)

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 AFTERNOON SESSION

2 MR. MEDINE: If we could get started, please.
3 Thank you for coming back. We want to relatively
4 briefly finish up the discussion on access so that we
5 can save some time to discuss some very important
6 security issues.

7 John Kamp has asked for recognition and will
8 begin the focus along with a couple of other folks
9 before we move on to security.

10 John?

11 MR. KAMP: Yes. Apparently I led people to
12 believe that the Federal Trade Commission was now
13 immediately at this time in the midst of writing rules
14 in this area, and I wanted to make sure that I knew and
15 everybody else in this room, including the press knew,
16 that that was not the case.

17 But since I've said that, I also want to respond
18 to Steve Cole's question about what are we up to here.
19 I think that we're being unfair here to say that we
20 don't have any rules, and we don't have any goals.

21 We are informing the Federal Trade Commission --
22 this advisory committee is informing the Federal Trade
23 Commission about this issue, and an issue that we all
24 know is, if not certain, certainly likely to be the
25 subject of law or agency rulemaking in the relatively

1 near future.

2 And what we do here is important and significant
3 to them, and we have to do the best we can to inform
4 them in ways that helps them do what they asked us to
5 do, and that is ensure that these rules work for the
6 American people as well as for the American business.

7 MR. MEDINE: Well, I will definitely associate
8 myself with the first remarks that John made. I can
9 assure you the Federal Trade Commission is not in the
10 process of engaging in a rulemaking proceeding, but we
11 are, as we've said all along, examining self regulation,
12 and clearly the work of this group already has informed
13 the FTC staff and will ultimately the Commissioners as
14 well about these very important issues.

15 Do people -- we left off on access, and I don't
16 want to spend too much more time on it because we do
17 want to move on to security, but if anyone wants to make
18 some final comments on access issues, particularly
19 authentication which we didn't have a chance to develop
20 too much. Dan?

21 MR. SCHUTZER: I would like to say a little bit
22 about the authentication sections. When I looked at
23 it, here's some observations I make about it. I do
24 think it's important to have a section, and you do have
25 a section in there in terms of describing

1 authentication, defining it.

2 And some of the issues of definitions, key
3 points you want to make here and I think you did make is
4 that there's a difference between the fact you might be
5 authenticating identity but you don't necessarily to be
6 authenticating identity due to levels of
7 authentication. There are some applications of
8 identification other than that, and there's a
9 distinction between authentication and authorization.

10 And then to go into the different kinds of ways
11 -- technology ways can do authentication, there I
12 think -- I thought it was a little confusing. I
13 recommend we think about rewriting it somewhat. I saw a
14 section there that, at least to my mind, seemed to be
15 equating a Photo Card to a Smart Card, and they're not
16 the same thing whatsoever.

17 But I think that's important as a backdrop to
18 getting everybody up to the same level of -- some level
19 of understanding as to the different technologies, the
20 main part being that there is no perfect way of doing
21 authentication.

22 Even if you go into a two factor or even a three
23 factor system, there's risk and liability associated
24 with it, and there's trade-offs associated with it
25 because as you provide greater, more perfect

1 authentication, you have overhead and security costs
2 inconvenient to the consumer and the like.

3 And then I think the two issues you're talking
4 about in authentication falls into two areas. One is in
5 the issues of the trade-offs and who makes the
6 trade-offs, and you can propose all the alternatives and
7 options you want.

8 I might propose an option might be that the
9 trade-offs is something that's made mutually by some
10 combination of the person who's providing the
11 information. They certainly have a role in providing
12 what types of authentication they need, they require to
13 allow you to have access, and the consumer, the entities
14 in a way provide some of that trade-off too because if I
15 make it to onerous, they won't come to my service.

16 And the third thing that I think to dwell on and
17 where probably a lot of this really has to talk about is
18 in the area of the liability. That's to say, How do we
19 distribute the liability and what are the options
20 there.

21 There's where I think most of the work in
22 authentication should lie. In other words, I think some
23 of that is tied into notice. In other words, because
24 I'm going to be providing you the authentication through
25 secrets and passwords which is probably the most likely

1 way most of us will do it because it's less costly, it's
2 easier and so forth, then there's some liability I'm
3 taking, but there's some liability in the part of the
4 consumer.

5 And they have to understand that, that if they
6 were to share their passwords or be careless and
7 negligent in that process and as a result of that, in
8 that accessing the information the wrong party is going
9 to have access to it, then the corporation should not be
10 held liable in that case.

11 In other words, if somehow your information is
12 accessed by the wrong parties and we've done the most
13 reasonable thing we can do to safeguard it, but somehow
14 through negligence of the consumer, then there's some
15 liability on their part of those damages which you can
16 try to minimize and defect.

17 So there's those kinds of trade-offs and options
18 where I think is we probably would want to set here.
19 The backdrop on authentication is not perfect. There's
20 trade-offs, then the distinction between authentication
21 and authorization, and then really honing in on the
22 liability issue.

23 MR. MEDINE: And I suspect that the liability
24 discussion will also be mirrored in the security context
25 as well. Dan, did you have a --

1 MR. JAYE: Yes, I had one comment here on the
2 authentication considerations for access, which is that
3 one of the considerations when we look at the risks here
4 that isn't talked about is contracts, and in many cases
5 when there's some data sharing or there's some
6 relationship due to different parties involving data,
7 there are usually contractual requirements that restrict
8 what can be used for the data.

9 So, for example, at Engage we have contracts
10 that say that we will not allow data passed to us as non
11 PII to ever be combined with PII or to be turned into
12 PII, and so we see that we have a significant exposure
13 if that data was inadvertently revealed to someone other
14 than the data subject themselves.

15 So authentication has more than just these
16 issues we talked about here, which is the potential harm
17 to the consumer, but also could have a very tangible
18 impact on businesses who have contracts where the whole
19 purpose of the contract is to actually protect the
20 consumer.

21 So it actually might, in fact, be interpreted as
22 a desire, as an incentive for people not to have data
23 protection contracts because they might not -- it might
24 make it even harder for them to comply with it.

25 Thank you.

1 MR. MEDINE: I guess the question is: Which
2 standard would that then suggest for authentication?
3 Would the contract be implied, have a reasonableness
4 standard, or would there be some other suggested
5 approach to how much authentication you ought to
6 require?

7 MR. JAYE: Well, I think the issue there, once
8 it comes with the risk and what is the real consumer
9 benefit of allowing access to different types of
10 information or what's a potential harm of not providing
11 access, I think that I actually very much agree with
12 Deirdre's comment about we should be starting at the
13 point of what can we provide access to.

14 I think in this case we end up in a very similar
15 position, though, which is that in a case where we've
16 had contracts that are deliberately designed to actually
17 prevent the data from ever being used in an
18 inappropriate way, it becomes very hard to -- you end up
19 in the same situation where risks of inadvertently
20 sharing it with an inappropriate party are too great.

21 MR. MEDINE: Dan, the other Dan?

22 MR. GEER: Yes, Dan Geer. It's a small tentacle
23 point but it's important to catch, and this is about
24 data correction.

25 Since I'm assuming that we envision at least in

1 near term future in which primarily people identify
2 themselves by revealing a secret, whether it's a pass
3 name, pass name or mother's maiden name or what have
4 you, as a point of security, you cannot on the same
5 channel that you would use those secrets to prove that
6 you are who you say you are also correct those.

7 So if my Social Security number or my name or my
8 street address or my phone number or whatever it is that
9 you use as the secret to confirm that I'm Dan needs
10 correction, you cannot correct that over the same
11 channel.

12 Otherwise you're completely wide open for
13 breach.

14 MR. MEDINE: Fred?

15 MR. TORRES: I'm just curious as to something,
16 and I would appreciate the security and authentication
17 issues kinds of wrapped together because we don't want
18 people who shouldn't be authorized to get access to
19 things to have access.

20 But on kind of the flipside of that, what type
21 of authentication do you get or verification of
22 someone's identity do you get when you're collecting all
23 this data because I would hate to see the authentication
24 argument used as creating such a heavy burden for
25 consumers to really have to -- I mean, there's got to be

1 some balance here.

2 But I was wondering on the flipside, what steps
3 do businesses take to verify the information that
4 they're collecting in the first place?

5 MR. SCHUTZER: It depends I think --

6 MR. MEDINE: Dan Schutzer.

7 MR. SCHUTZER: I think it depends on the nature
8 of what I'm doing with the information. If I'm
9 collecting the information to maybe infer something
10 about the consumer for let's say marketing, direct mail
11 or something like that, I can be somewhat sloppy I think
12 because I'm not damaging the individuals.

13 That may be inconveniencing them by sending the
14 wrong marketing message that they're really not
15 interested in, but when it's something like dealing with
16 their financial records or balancing their funds, then I
17 have to be extremely careful in the authentication of
18 the individual, even in collecting of the information,
19 so I think it's the nature --

20 MR. TORRES: And how do you go about doing that
21 part of it, authenticating it when it's important
22 information?

23 MR. SCHUTZER: Well, as you know, in most of our
24 financial transactions, we require something at least of
25 a two factor nature, something that you're holding like

1 a card, for example, and then some kind of a --
2 something you remember, like a pin number or biometric
3 like your handwritten signature.

4 All these things are somewhat imperfect, but
5 that combination, plus looking at pattern recognitions to
6 detect out of -- unusual kinds of buying patterns will
7 come back in that case to another channel. It goes back
8 to the customer, and we'll say, We just want to verify
9 from you that you do have your card or you did make that
10 purchase just to make sure that it wasn't a fraudulent
11 transaction, those kind of things.

12 Then we follow with laws and regulations by
13 having to then send you, on a periodic basis, your
14 transaction records and your balance, which you get a
15 chance to see and correct and challenge, so we have to
16 go through all of those efforts for that.

17 We don't go through those kind of efforts, of
18 course, for our marketing, but we do absolutely have to
19 go through those kind of efforts with financial
20 transactions.

21 MR. MEDINE: Richard? Just speak in the
22 microphone.

23 MR. RICHARD SMITH: Richard Smith here. I was
24 on this particular group on authentication. I just
25 realized something that we kind of left out, something

1 that Dan mentioned, is one way that you can deal with
2 the authentication problem is if somebody's accessed the
3 personal records, and you have like an email you can
4 send out that access was made, and so if there -- if
5 that was done in error, there's at least this separate
6 channel back that says, Hey, somebody got into your
7 data.

8 MR. MEDINE: Ted and Stewart, and then let's try
9 to shift gears to security.

10 MR. WHAM: To address the questions that Frank
11 had from a different perspective and a lower security
12 type of business than a financial institution, the point
13 of entry, there are some rudimentary checks that can be
14 placed on the data integrity as it's provided to you so
15 you can, for instance, test that an individual's name is
16 all alpha characters as opposed to any numerics or you
17 can take and match the Zip Code against the city. Those
18 do logically make sense. You can't be in San Francisco
19 now with a 20001 Zip Code because you be the FTC.

20 Other information, once the custom has in his
21 the database systems to support, some of which supplying
22 a vast array of things with information provided by the
23 U.S. Postal Service.

24 Some other things that we do is once you've got
25 that information, if somebody comes through and says

1 they're Donald Duck and they have the password of Goofy,
2 presuming the code network has come out for that.

3 (Laughter.)

4 MR. WHAM: To us that individual is Donald Duck,
5 and there's no additional attempt to try and verify that
6 through a third-party scene, but nonetheless we have to
7 -- since we cannot on a prima facie basis know whether
8 there is in fact a person by the name of Don Duck out
9 there, we have to presume that that's accurate.

10 We have to have some type of an authentication
11 step through there because the next person could just as
12 easily have put in accurate information and will get
13 quite ticked off with us if we randomly allow access to
14 them.

15 MR. MEDINE: Stewart's promised to be
16 provocative and keep us going this afternoon.

17 MR. BAKER: I'm going to switch us over to
18 security in just a second but I thought I would touch on
19 liability.

20 MR. MEDINE: Good.

21 MR. BAKER: Security is going to be boring I'm
22 afraid. Deirdre and I agreed on this test.

23 (Laughter.)

24 MR. BAKER: On this question of liability, I
25 think it's important to recognize -- I think it's

1 different in authentication than it is in security.
2 Security, of course, you can be sued for bad security
3 and held liable, and there ought to be some protection
4 where you've done something reasonable.

5 But in authentication, it's a much trickier
6 policy issue because if you allow the wrong person
7 access to data and a harm results, and I think both of
8 those things are certain to happen if you're providing
9 access, you're going to get sued, and you're going to be
10 held liable in many cases, and that is an incentive for
11 people to be very demanding in the authentication that
12 they impose, maybe too demanding.

13 And I would have thought that it's also clear
14 that there are privacy violations in having
15 authentication violations, and there also could be
16 privacy problems with not allowing access to data, so
17 that you have privacy interests on both sides of this
18 debate.

19 I would have thought that everyone could agree
20 that if someone makes a reasonable effort to strike a
21 balance there, they ought not to be held liable either
22 way and particularly ought not to be held liable by
23 people who say, Yeah, but the wrong person got access to
24 my data.

25 And only the FTC can say, Yes, but in the

1 interest of allowing easy access, we're willing to live
2 with some of that harm and we don't think that people
3 should be scared off by it into raising the bar for
4 access.

5 MR. MEDINE: Mr. Mendorose (phonetic) of the
6 Fair Credit Reporting Act has a standard of proper
7 identification in which you can infer reasonableness as
8 opposed to a strict liability standard for giving out
9 improper access.

10 MR. BAKER: I thought I would just quickly go
11 through what we did in this paper. We set out a
12 continuum of options. We have five options ranging from
13 most stringent to least stringent. We actually have the
14 options in there twice, first by themselves, and then
15 later with pros and cons that are sort of in draft form.

16 But the continuum runs from the most drastic is
17 a sliding scale of securities standards that depends on
18 how much security you impose, tells you -- is related to
19 how sensitive the data is, and the idea that some
20 independent body or the FTC would set those standards.
21 It's going to require quite a bit of elaboration
22 regulation. That was one possibility.

23 Another possibility was to say to everyone, We
24 recognize that you have to have different security
25 standards for different data. We're just going to tell

1 you to do the right thing, to have an appropriate level
2 of security, and if you miss, we'll hit you.

3 The third way is to rely on industry standards,
4 and there are three different ways of generating those
5 standards from having the bodies that do it be
6 designated by a government body and subject to
7 government type regulation, notice and comment and the
8 like.

9 Another possibility is just to say any
10 third-party that adopts a reasonable set of standards,
11 and that would include a lot of these topics, can set
12 the standards, or it simply could be that any trade
13 association or standard setting body that wanted to get
14 into this business could, and that would be enough.

15 It would be akin to a seal program. Consumers
16 would decide how good a particular seal was from their
17 point of view.

18 The fourth option was, I think this is the Ron
19 Plesser option, you just maintain a security program.
20 You adopt one. Everyone is required to have a security
21 program, but they don't have to have a particular
22 content to it.

23 There's actually two sub options here. One is
24 where the government sets the content and tells you what
25 is a good security program, and one is it just says,

1 Look, you have to think about it, you have to write down
2 what you're doing, we're not going to tell you more than
3 that, and the last option is rely on existing remedies.

4 We have two options that we rejected that we
5 didn't -- anyone think they belonged in here. We then
6 talked about four ways of enforcing any rules that are
7 adopted and have about five additional issues that came
8 up that we are still trying to fit into the continuum or
9 into a preamble for this discussion.

10 Thank you.

11 MR. MEDINE: Thanks for that very helpful
12 overview. I guess one thing that would certainly be
13 useful for people to express their views about, which of
14 these various approaches is most feasible, is most
15 appropriate, what the costs and benefits of each of
16 those programs are?

17 MS. CULNAN: Before we move on, Mary Culnan, add
18 one comment to Stewart's excellent introduction which
19 would be, we didn't really I think reject notice and
20 consumer education. We rejected them as stand-alone
21 options for the reasons that are stated in the
22 discussion there, that they would be useful in
23 conjunction with appropriate security program.

24 MR. MEDINE: Deirdre, who agrees with all
25 Stewart's panoply of options?

1 MS. MULLIGAN: Stewart did an excellent job of
2 introducing the document.

3 I actually want to step back to the
4 authentication and access issues just for one second.
5 One second I promise. Lance and I think being concerned
6 about whether or not we can meet deadlines each drafted
7 a document that we thought might help move us forward.

8 One is a process document. One's a little bit
9 of a, Here's a draft outline for how we might deal with
10 the authentication section, and I just think we're going
11 to pass those around, no substantive comment.

12 MR. LANCE HOFFMAN: Well, I wonder -- I didn't
13 know you were going to do it right now.

14 MS. MULLIGAN: No, I'm just going to pass them
15 around, not actually do anything with them, just pass
16 them around.

17 MR. PLESSER: These are additional comments?

18 MR. MEDINE: We'll take them and pass them
19 around. I think they're suggested approaches for how we
20 move on from here. We can certainly take those up at
21 the end of the session. Dan?

22 MR. SCHUTZER: I think we did a pretty good job
23 on this one. The one comment I think we would like to
24 make from the financial service industry point of view
25 is that -- and therefore we think it's worthwhile your

1 noting that kind of distinction, probably health care is
2 the same kind of thing.

3 And you might consider that some of these
4 options, they might be different depending upon the
5 nature of it. For example, in the case of financial
6 services, we have a lot of standards, guidelines and
7 regulation and order bodies, and we are perfectly happy
8 with those kind of regulations and order bodies, and it
9 isn't necessarily the right thing for everybody else,
10 and you might -- even if there's another agency it might
11 be a different agency for those other people, but it
12 indicates financial services without asking for any
13 change unless somebody here thinks otherwise.

14 The only caveat you might be thinking about is
15 that we do on another front where we're working for
16 various regulators and the FTC and others, and we're
17 looking at the issue of aggregation and those people
18 that are touching financial information that are not
19 financial service firms and the issues that they're
20 wrestling with, I don't know how that will come out in
21 terms of what kind of Reg-E types of provisions or
22 regulations might be imposed on a non financial service
23 firm that is indeed handling financial information.

24 There, of course, if it turns out that they have
25 these kinds of security regulations or Reg-E regulation

1 and so forth, it's not clear they necessarily need to be
2 governed by the same agency as financial service firms.

3 MR. MEDINE: I mean, I don't know if another way
4 to translate that is to the extent that it's a regulated
5 industry and those regulations address security
6 concerns, I don't think that that fits under your
7 industry specific standards or it's a sixth option which
8 is to the extent that some of the otherwise regulated
9 security, those standards out to govern.

10 I don't know if people have views about whether
11 -- and of course the FTC and banking industries will be
12 issuing regulations in the future on Section 501
13 relating to security issues also.

14 I guess maybe do people have a view of sort of
15 across the board in general U.S. commercial web sites,
16 which has kind of been our focus, as to which of these
17 standards make the most sense in terms of the kinds of
18 security measures or if there ought to be again
19 regulations as we talked about in the access context
20 depending on the type of site it is or the type of
21 information it collects or the types of transactions
22 that it engages in.

23 Ron?

24 MR. PLESSER: To the extent that my name was
25 used as a reference point before, I actually think that

1 what my thoughts were, I don't even know if it's a
2 proposal, was a combination of I guess what is marked
3 here as 4 and 2. I did not mean 4 -- at least I did not
4 mean for it to operate separately.

5 I think it has to be -- you have to maintain a
6 security program that's appropriate under the
7 circumstances, that you define the standard of care of
8 reasonableness, appropriateness, whatever the right
9 standard. You then take reasonable precautions to
10 protect against those risks.

11 If then in the end you have a risk loss and
12 somebody -- just having the loss isn't enough but if
13 somebody goes back -- and be it the FCC or FTC or
14 whoever looks back and sees that, you know, you
15 didn't -- you didn't adequately consider the risks that
16 happened or you didn't take standards of care, then it's
17 a violation.

18 Then it would be a problem, so I think that what
19 I'm really talking about is I like 2, and I think -- but
20 2 to take it a little further step is to say that you
21 have to implement 2 in advance, have it written down so
22 that somebody can then consider it rather than have 2
23 kind of approved, preapproved European style.

24 This would be you would do it yourself, but that
25 standard would have to be there so I think that 4

1 standing alone doesn't make a lot of sense, but I think
2 4 standing with a combination of 2 makes a lot of sense,
3 so it's just a combination more than a criticism.

4 MR. MEDINE: We'll call Mary, but just to add to
5 the discussion, what about the relationship of
6 communications with consumers about which standard is
7 being applied? In other words, if there's an
8 expectation that standard is going to be applied to
9 security, should a website say in its privacy policies,
10 We use reasonable efforts, we use some standard so that
11 not only will consumers in the market know what's going
12 on, but there's also some essential commitment by the
13 web site even in the legal sense to follow some of the
14 whatever they say they're going to do?

15 MR. PLESSER: Well, I guess the focus is if I
16 can, Ron Plesser again, really the notice issue, take
17 the reverse of what you said, can you put on the site
18 there's no security here. We've taken no steps to
19 secure the information or is that adequate, is that
20 okay? If it's clearly and conspicuously notified to the
21 consumer or put in a petri pea click that there's no
22 security here, is that okay, is that sufficient, and --
23 or are we trying to really create some kind of
24 substantive standard for security or are we more
25 concerned about it as a notification issue?

1 MR. MEDINE: Mary?

2 MS. CULNAN: Actually I just had forgotten to
3 take my card down, but I will make a comment.

4 MR. WHAM: Cheater, cheater.

5 MS. CULNAN: I think the notice component is
6 very important. I would be very unhappy if we came away
7 without a notice requirement because consumers -- what
8 is a consumer or surfer to assume if their web site says
9 nothing? Are you just to assume everyone has
10 appropriate security procedures in place or not,
11 although I think we do agree that notice doesn't do the
12 job if you haven't really implemented the right thing,
13 and the issue is how to fit those two together.

14 MR. MEDINE: Lorrie?

15 MS. CRANOR: Lorrie Cranor, and this is
16 something we also talked about within our subcommittee
17 about notice, and I think that notice is good only if
18 it's tied to something very specific and concrete. I
19 think just having web sites say, We take good security
20 precautions doesn't really help.

21 And especially if we are operating under
22 something like number 2 where they all basically have to
23 be taking good security precautions. Whether they say
24 that or not doesn't really matter. If on the other
25 happened we're relying on something like number 3 where

1 we have industry specific standards, then disclosing
2 which industry specific standards you're following would
3 make some sense I think.

4 MR. MEDINE: I guess going back to how is the
5 consumer -- if the web site does all the right things
6 but doesn't say anything about them, how does that -- is
7 there a need to create consumer confidence about
8 security almost separate from what the web site is doing
9 but obviously related to it, but how do consumers know
10 that they're dealing with a secure web site and how do
11 they have confidence in e-commerce without some statement
12 to the consumer about what the web site is doing?

13 MS. CRANOR: So if all we're worried about is
14 consumer confidence, if a web site thinks it's in their
15 best interest to build confidence to say something,
16 they're going to do it, but the problem is actually
17 misleading the consumer, giving them false confidence if
18 every web site is just saying, We take good security
19 measures when they're just saying that.

20 They may not be doing that at all or there's no
21 definition of what it means to take good security. In a
22 privacy policy if you say, We don't share data with
23 third parties that's a very specific thing you can test
24 whether or not they're doing that, but we have good
25 security precautions is a lot harder a task, Mr. Medine.

1 MR. WHAM: Wham, with all due respect to
2 Business Week I feel like I'm back in an Alice In
3 Wonderland discussion of the notice component here. The
4 argument and tangentially to what you just said, David,
5 how is a consumer to trust e-commerce in the absence of a
6 notice requirement? I presume we can trust it in a way
7 not dissimilar to the way they trust a traditional
8 commerce environment.

9 When I order furniture and have it delivered to
10 my home, there's not usually in my experience a
11 conspicuous notice about how they're going to take and
12 keep that information. When I buy any type of a product
13 and they capture my name and address information, if
14 it's in an offline world, you know, if I go into Barnes
15 and Noble, I don't recall seeing a big broad notice
16 saying, This is the data that we're capturing about you
17 this is how we're going to --

18 MS. GAU: This is about security system.

19 MR. WHAM: Pardon me?

20 MS. GAU: This is about security system.

21 MR. WHAM: This is about security system, and
22 nonetheless the banking industry I don't recall -- there
23 may be, it's probably buried in some disclosures but I'm
24 not even sure that's the case, right? Certainly not
25 available within the branch and as some legislators have

1 recommended in the upper right-hand corner of the
2 bill.

3 There is -- where is the analog, where is the
4 analog, how does this tie to the real world? If we've
5 got a new economy and an old economy, the world works.

6 Now, that all said, I believe there should be a
7 disclosure. I believe it should absolutely be on
8 there. I think it's in the best interest to consumers.
9 I don't see that there's a lot of harm in doing it, but
10 to say that without it we're going to have this -- how
11 is e-commerce going to grow I think is absurd.

12 MR. MEDINE: Jonathan, then Richard and Andrew.

13 MR. JONATHAN SMITH: Jonathan Smith, University
14 of Pennsylvania. I was not going to say this in the
15 last session but I just have to point it out. The
16 big -- there's a very fundamental big difference between
17 the things that people are calling the old economy and
18 the new economy, and you probably know what it is, but
19 I'll remind you again of it, which is Moore's law.

20 And what it changes is the following: You have
21 costs that decline by 60 percent a year for doing the
22 things that you do, store information, process
23 information and move bits, 60 percent a year or better.

24 In the old economy you have oil, you have
25 salaries and you have real estate that don't change at

1 exponential rates, so what happens is the market
2 valuations of these new economy companies reflect the
3 fact that people have figured out that there's an
4 exponent on one side and there's not an exponent in
5 sort of the old brick and mortar economy.

6 That's what's going on here, and I think when
7 you're looking at a world in which things are changing
8 exponentially, I believe that things are very different
9 because human beings are used to things that change in
10 linear terms and a tempo that's human.

11 And when you're talking about these huge
12 exponentials, in fact things are very different, so the
13 cost of collecting information essentially is going to
14 zero or at least it's going down by 60 percent a year.
15 You can do the math as to how many years it takes to be
16 approximately zero.

17 So what's changing here is that you really do
18 have a very different world, and I don't think that I'm
19 living in wonderland to be able to look at a curve and
20 look at how those costs change, so I think what people
21 are asking about is, What happens when the cost of
22 getting every bit of information about you is zero.

23 And I think that's where a lot of the concern
24 lies on the committee, so I think it's unfair to say,
25 Well, we have to have an analogy because there is no

1 analogous physics of change in the cost in the
2 economics. It's just not so. We've never encountered
3 anything like this.

4 MR. WHAM: If I may, if I can respond directly
5 to that, I appreciate the perspectives there, and I'm
6 afraid I'm going to have to take issue with some of them
7 that are provided.

8 A company such as Excite@Home, 80 percent of
9 our total expenses are involved in head count, you
10 know. The pay that we have to pay for our heads, that
11 we have to pay for our offices is not dissimilar to --
12 and in some cases arguably is higher or substantially
13 higher than many traditional business have to pay for
14 their business.

15 A company such as Amazon has to have warehouses
16 and has to have employees to stock those warehouses. It
17 has to do all those things, and there's also a
18 misconception that you brought forth that could not be
19 more disruptive to actually understanding what's going
20 on.

21 The cost of processing information is going down
22 by Moore's law. The cost of collecting information is
23 not going down by Moore's law and the cost of collecting
24 information in offline business is very similar to the
25 cost of collecting information in an online business,

1 except for the difference in an online business you
2 absolutely, unquestionably have substantially more touch
3 points.

4 And as I was talking with somebody in the
5 audience here in the break, as part of my participation
6 in this committee and hearing a very broad spectrum of
7 ideas, my personal opinions have changed, and my
8 personal opinions are that there are differences within
9 the online world, and I believe that those differences
10 should be reflected in the type of actions that we
11 recommend and the nature of our report.

12 But to take it and say that we have in an
13 offline world not an ability to have a comprehensive
14 compilation of information about a consumer is to
15 just -- that's just not the case.

16 As a database marketer for 15 years I can tell
17 you I could go get a massive storehouse of information
18 about you that had nothing to do with new economy
19 businesses that was available today.

20 Yet we're talking about imposing a burden of
21 regulation on business based upon the communication
22 method they have as opposed to the underlying, quote,
23 problem. If there was problem that there is infinite
24 information categorizable and retainable about a
25 consumer and if the public policy decision is that we

1 want to do something about that which is absolutely an
2 arguable position I don't take exception to, if that
3 decision is there, then apply it to business but don't
4 apply it one sector of business because you put it at an
5 inherent disadvantage, and you don't solve the problem.

6 As long as I can go to a primary list of data
7 and buy your age, your income, the items that you
8 purchased, how long you have been in your home, what the
9 mortgage value is, all of those different things, I can
10 do that like this.

11 As long as I can do that, to solve the problems
12 within the online community is not to solve the
13 problem. Treat it in an equal and fair fashion.

14 MR. MEDINE: You want to respond to that at
15 all? If not, I would like to return back to the
16 security issue.

17 MR. WHAM: Disagree.

18 MR. MEDINE: I'm going to -- I'll go to Bob and
19 then go back to Richard.

20 MR. HENDERSON: I think Ted is bringing up some
21 very good points, and I said this during our first
22 meeting. Even though the title of our committee is
23 Web, Access And Security, this is about the
24 accumulation, the process, the distribution, the
25 accessibility of personalized data, and I think that a

1 fallacy that Ted's bringing up, and I totally agree
2 with, is that the web activity, the e-commerce
3 environment, the new economy is one element of
4 processing personalized data.

5 And if you think about it, in your daily lives,
6 how many of you actually provide information,
7 personalized information to businesses exclusively
8 through the web? You don't. You provide that
9 information many, many ways.

10 So the types of things that we're talking about
11 don't get lost in the issue that it only applies to the
12 web environment. It's across the board for any business
13 that collects data. I think Ted asked for an analog.

14 I'll give you a good analog, the traditional old
15 economy business, banking. Some of the major banks in
16 the United States are putting out notice statements
17 about privacy. They're spending thousands of dollars
18 with public relations companies developing these
19 statements so they can get, get this, explicit or
20 implicit opt-in for their customers so they can put out
21 the right statement of notice to get their customers to
22 agree with what they're doing with the data, and they're
23 spending a lot of money to do this right.

24 It has nothing to do with the web or the
25 e-commerce environment. It's the issue of providing

1 notice and protecting the privacy elements, so I think
2 Ted's absolutely right on this issue that what we're
3 talking about is web based activities, but everything
4 that we do, if you take it back to the consumer, to
5 managing personal privacy, is going to apply to any
6 business that collects personalized data and processes
7 it.

8 MR. MEDINE: Richard?

9 MR. RICHARD SMITH: Yes, this is not on
10 security, but I want to get back to Ted's remarks here
11 because he's made it twice. Interesting he made the
12 analogy of Barnes and Noble. I was just in Barnes and
13 Noble last week and picked up kind of a little card, you
14 can sign up now for getting email notices and also you
15 give them your name and address, and there's some
16 privacy disclosures on there.

17 So at the point where Barnes and Noble and the
18 offline world does collect personalized data or data
19 about you at all, they're going to know. They do --
20 they're getting into the web way of doing things of
21 disclosure.

22 The fundamental difference of course in the offline
23 world is when I walk around Barnes and Noble, I don't
24 have a cookie with me, and on the web, the level of data
25 collection is many, many orders of magnitude higher, and

1 I think that's why we're talking about this issue.

2 The Barnes and Noble, if I go read a book, The
3 Story of O off the book shelf, I don't believe there's a
4 camera in the ceiling of that building recording what I
5 am interested in, but if I go to bn.com that interest
6 might be recorded.

7 MR. WHAM: They only record The Story of --

8 MR. RICHARD SMITH: Yeah. The other issue is
9 even when I go buy a book, it's very unclear because of
10 there's no cookie there. They might need my credit
11 card, maybe that's being record, I hope not, but maybe
12 it's -- I just think the level of data collection is
13 much, much smaller in the offline world in the
14 particular example that you gave there, not of course
15 all industries of course.

16 MR. MEDINE: John?

17 MR. TORRES: Just one quick comment. Maybe I'm
18 dating myself a little bit here, but I kind of missed
19 The Story of O.

20 MS. MULLIGAN: Me too.

21 (Laughter.)

22 MR. KAMP: I'll explain it to you later. This
23 is John Kamp. We don't want to talk about it online.

24 MR. MILLER: I recommend a search of Yahoo.

25 MR. KAMP: Moving on this is John Kamp from the

1 AAAAs again. I too like Ted have changed my mind about
2 this issue. When we first came, in the first meeting we
3 talked about offline versus online, and I suggested that
4 we shouldn't go there, not the least of which had to do
5 with the scope of the authority of this Commission.

6 But listening to even the chairman's -- the
7 chairman of the FTC's comments or his quote in USAToday
8 a week ago Thursday and elsewhere, I think we all have
9 to be cognizant of the fact that what we do here, as I
10 said before earlier in this session, what we're doing is
11 informing policy makers about the public policy choices
12 before them.

13 And if online choices are made in this area, we
14 have to be at least cognizant of the fact that they will
15 be a template or at least a point of departure for those
16 people who want to suggest that this ought to go
17 offline.

18 These aren't -- I don't think -- I sort of agree
19 with both of them here that there are differences, there
20 are reasons to -- there are similarities, but we're
21 working in a public policy forum where these discussions
22 will have a tremendous amount of impact on the offline
23 world eventually as well as the online world.

24 MR. MEDINE: Tatiana?

25 MS. GAU: I would like to take the discussion

1 back to security.

2 MR. MEDINE: Great.

3 MS. GAU: And actually these were some comments
4 that I had made at an earlier meeting. With respect to
5 the issue of set standards, whether it's in the first
6 level sliding scale of security standards or industry
7 specific standards, I think that it's going to be a
8 continual source of, shall we say, amendment and
9 revision.

10 As threats change and the environment that
11 exists on the Internet evolves, the technology evolves,
12 it's extremely difficult to set some type of baseline of
13 standards which would even be appropriate for a period
14 of six months, so I again take objection to the idea of
15 trying to come up with some kind of baseline standards.

16 I would also like to take us back to the idea of
17 security as a process, that it's not just technology,
18 that it's also program, work force, policies inside a
19 company which goes to the Ron Plesser point number 4,
20 maintaining the security program.

21 And again as I suggested previously here I think
22 the use of external auditors could really help address
23 this issue. If companies similarly to having their
24 annual report attested to, their financial tested to by
25 an audit firm, would have a statement from an audit firm

1 indicating that they did meet certain, shall we say,
2 expectations and reasonable, shall we say, barriers
3 exist to prevent security breaches.

4 That would also help to prevent the disclosure
5 of information that would help hackers figure out what
6 kind of security exists at a company in order to break
7 in, so particularly with respect to the audit, external
8 audit which could be reflected through a statement by
9 the auditors in the privacy policy or a link from the
10 privacy policy to the statement of the auditors or some
11 kind of seal program again.

12 MR. MEDINE: Again just to clarify, are you
13 basically suggesting that the modified Plesser, which is
14 the combination of appropriate certain circumstances and
15 maintained program is the way to go in terms of
16 providing sufficient flexibility as new threats develop
17 and as technologies change, and yet require that that
18 company have some process in place to make sure they're
19 addressing those changes and threats?

20 MS. GAU: I would do that with the contingency
21 that the companies not be required to provide full
22 notice of exactly what their security program is on the
23 web site.

24 MR. SCHUTZER: Just a point of clarification is
25 that in some industries where we're talking about the

1 existing standards that you do, those are the kinds of
2 standards that we have, the standards that talk about
3 the process and the management and the personnel and the
4 audits and so forth.

5 And yes, they do in some cases point to the
6 current technical standards like this particular
7 encryption standard says, as those things become
8 vulnerable, they get updated, but the general standard
9 that you're talking about are the kinds you're referring
10 to, the process stuff --

11 MS. GAU: Yeah, but what I'm talking about also
12 though --

13 MR. SCHUTZER: The audit stuff, right?

14 MS. GAU: I'm also talking about kind of the
15 advisories put out by CERT on vulnerabilities in certain
16 server software and other things along those lines,
17 which, yes, there is an obligation for people to
18 maintain and constantly update the systems, and that's
19 part of a security program, you have somebody who is
20 actually implementing the fixes to the known bugs.

21 But that's my point to illustrate the fact that
22 the standards are --

23 MR. SCHUTZER: I agree with you, you actually
24 don't want to list those. I solved these patches but
25 they don't know which ones they didn't solve, right?

1 MS. GAU: Right.

2 MR. MEDINE: Steve, Rick, Deirdre, Larry.

3 MR. COLE: I want to speak to the question we
4 talked about a little while ago and it came up just
5 again now, the relationship between notice and security.

6 As a representative of the BBB, notice is
7 crucial to us. Our business is about informing
8 consumers, so I'm very gung-ho about everything we can
9 do to improve notice to consumers.

10 I have some real doubts that that's a big help
11 on the security, in fact, more than doubts. I don't
12 think it will be a help. I think it will be a harm.

13 Notice goes a long way to build confidence when
14 it's directly applicable to a range of some reasonable
15 choices a consumer could make, so what's collected on me
16 and how is it going to be used and can I see it and when
17 can I see it and how can I see it.

18 I think consumers either have an expectation or
19 ought to have an expectation if I give private
20 information, it's secure. I don't know what it means.
21 I don't know how to secure it, but it ought to be
22 secured, and I don't want to see a range of choices
23 about security measures.

24 What I think I want as a consumer is someone or
25 someones to set reasonable standards and then I'm going

1 to expect that those are met. Now, that could be by
2 industry practice that develops over time. It could be
3 by government doing it. It could be by self regulation
4 programs doing it.

5 I don't know that it matters precisely how, but
6 I would feel very uncomfortable if we put more than half
7 a percent of reliance on notice to accomplish anything
8 here.

9 MR. MEDINE: But how does that relate to the BBB
10 privacy seal where if someone has a seal, isn't there
11 some statement as part of that that they do have
12 security measures in place?

13 MR. COLE: That's right. If a consumer was
14 digging deep -- and by the way, one of the concerns we
15 all have in this business is we build a lot of
16 information for consumers but one of the reasons they're
17 looking for trust marks is they really don't want to
18 read all this information. They just want to know, Is
19 this okay.

20 And there's some danger attached to this. I'm
21 not saying that's really the best answer. Paula may
22 have a different viewpoint, but I see her nodding her
23 head up and down, but the way it relates to this is a
24 program, a self regulation program, whether it's PWC's
25 or TRUSTe's or ours has a set of standards.

1 Consumers can find out what they are if they
2 choose to and I guess could make some judgment, but the
3 standards themselves should provide adequate security,
4 and then we could debate which they do or not or whether
5 they could be approved or not.

6 But the consumer every time they got to a web
7 site is not going to be in a position to evaluate, Are
8 these securities measure good enough. They can
9 evaluate, Do I like what that web site does with my
10 information or when they let me see my information or do
11 they transfer it on to third parties but I'm going to
12 assume it's secure.

13 Now, whether our standards -- I'm learning a lot
14 here. We may have different standards here for now, I
15 don't know, as we're learning more about all these
16 issues but I think -- and maybe government will do it.
17 Maybe there will be a piece of legislation some day that
18 says, In these situations here's the minimum security.
19 I don't know. I'm not sure that's a good or bad idea.

20 So I just would like to see us pay more
21 attention on the security to what are the range of
22 reasonable security measures and not rely on consumers
23 to create a marketplace here.

24 MR. MEDINE: Rick.

25 MR. LANE: I'm concerned about standards is I

1 think as everyone agrees they're constantly going to
2 change depending on what the rate of attack is and
3 what's going on out there in the real world.

4 I think really what's critical in terms of
5 security is to find out or have a location -- I know
6 this kind of shifts the debate a little bit, but have a
7 place for businesses to go to find out how to secure
8 their network.

9 Especially for a lot of small businesses the
10 question is, Where do I go. I want to set up a secure
11 site. I can't afford to have a consultant come in and
12 pay a lot of money to tell me that, Oh, how you can buy
13 this \$35 software package and you're set and you spent
14 \$10,000 on the consulting fee.

15 And maybe the role of government -- and if there
16 is a role and I think a proper role for government is to
17 provide a place or provide a place for businesses to go
18 to educate the small businesses on process, on what do
19 you need to do, and I know Cisco has some small business
20 pages on their site that go to this point, but the more
21 that we can do that, I think that will help build
22 security.

23 In addition, what we're all trying to get after
24 which is consumer confidence. I think if you just have
25 here's a standard today, that doesn't provide security

1 -- especially if you pick up The New York Times or The
2 Washington Post or The Washington Times, whatever you
3 read, the following day and they say, Look at all the
4 sites that were hacked into with this minimum standard.

5 So then you've blown out any standard whatsoever
6 because then the trust is completely gone, and so the
7 best way to build trust is try to limit the amount of
8 attacks. I think that's the ultimate goal here, and the
9 ultimate goal is to limit the amount of attacks. The
10 only way you're going to be able to do that is have
11 information at your hands for small businesses and the
12 large businesses on where to go.

13 And I think if we're going to have a report, I
14 think education and a site that provides that I think is
15 reasonable and probably one of the best uses of the
16 government resources.

17 MR. MEDINE: Deirdre?

18 MS. MULLIGAN: Deirdre Mulligan. On the
19 security component, I would like to build a little bit
20 on what Tatiana said. I think the appropriate under the
21 circumstances combined with number 4 makes sense, but I
22 think in order to say what is appropriate under the
23 circumstances, I would want there to be some informed
24 process that helps to explain what a business could do
25 to be exercising reasonable care.

1 And that isn't, Here's a standard you have to
2 meet but what are the processes? What do you have to
3 monitor? Do you have to regularly install patches,
4 monitor the CERT alerts? Do you have to do tests? Do
5 you have to once a year, once every two years hire
6 somebody to test your security?

7 What are the processes that are going to make
8 sure that what you're doing is reasonable? And I think
9 the last thing anybody wants to do is create a bunch of
10 standards that are going to be outdated tomorrow, but
11 the question is , How do we ensure that the people who
12 are trying to do the right thing, and I'm going to act
13 with the assumption that everybody wants to do the right
14 thing, how do you help them.

15 And I think Rick just built upon that, but I
16 think the ability to put out some process points, these
17 are the things you should be doing to stay up to date,
18 would be a useful addition to informing number 2 in
19 combination with number 4, and I would certainly support
20 that as a good recommendation to the FTC.

21 Then I just wanted to make two comments.

22 MR. MEDINE: Just on that point, obviously your
23 report would be a useful starting point, and you've got
24 a tremendous amount of expertise at the table.

25 MS. MULLIGAN: Well, I'm hoping we can move that

1 to the recommendation in the report. I'm hearing a lot
2 of consensus so I would like to start building, and if
3 you don't like it, be quiet. No.

4 MR. MEDINE: Go for it.

5 MS. MULLIGAN: Come on, Stewart and I agree.
6 You're not going to get much luckier than that.

7 MR. BAKER: Yeah, but don't push it.

8 MS. MULLIGAN: I was pushing just a tiny little
9 bit, and the second issue is what's reality in the off
10 line world versus what are we doing to burden online
11 businesses?

12 From day one there's been a discussion there's
13 absolutely no definition of what online means, and I am
14 perfectly happy to pull a Donna Shalala and suggest any
15 information that ends up in electronic form is in fact
16 online, and I think that would solve your problem, Ted.

17 MR. WHAM: It would, yes.

18 MS. MULLIGAN: Accept? I have a motion on the
19 table.

20 MR. MILLER: I second it.

21 MS. MULLIGAN: We've been searching for a
22 definition, what is the scope of online access and
23 security?

24 MR. MILLER: I think it's a misnomer to say it's
25 web access. Web is certainly a big part of it, but

1 there's a lot of access portals into an online
2 information network that we call digital economy that we
3 need to think about, and one of the things that HHS did
4 was to prevent the notion of, okay, fine, I'll just keep
5 everything in paper because that was the alternative.
6 They said, Well, anything electronically --

7 MS. MULLIGAN: Or I won't collect it here, I'll
8 collect it somewhere else.

9 MR. MILLER: Exactly.

10 MR. MEDINE: James? Could you identify
11 yourself?

12 MR. ALLEN: James Allen. Having spent 20 years
13 in the online transaction processing world before I got
14 into the web world, I go along with this proposal
15 completely.

16 MS. MULLIGAN: I have a second and a third.

17 MR. KAMP: I'm not sure I understand what the
18 motion is.

19 MR. MEDINE: The committee can chose to --

20 MS. MULLIGAN: I'm being a little flippant, but
21 I'm just trying to suggest, Ted, that I don't think the
22 perception that what we're trying to do here is create
23 an uneven playing field doesn't have to be the
24 perception.

25 I think there's an opportunity to reform that,

1 and there may be dissenting views on this, but I think
2 it's a really, really important discussion, but I don't
3 want you to think that that's anybody's goal or at least
4 certainly not mine.

5 MR. SCHUTZER: Just a thought, I think there is
6 a distinction between being online in a behind the
7 firewall proprietary network and being online in a
8 network that's publicly accessible, so you have to bear
9 that in mind. You follow the distinction?

10 MR. LANCE HOFFMAN: Keep going. Do you
11 agree with that, Deirdre?

12 MS. MULLIGAN: From the perspective of access,
13 from the consumer's perspective?

14 MR. SCHUTZER: From the perspective of security
15 threat and everything else, if I am talking about a
16 behind the firewall enterprise network let's say.

17 MS. MULLIGAN: Yes, definitely I would say.

18 MR. SCHUTZER: It's not coupled. It's got an
19 air gap and it doesn't go through any kind of public
20 network access, then I think the security is a lot
21 easier, and the risk is a lot simpler and so forth, and
22 there is a difference.

23 Now, I'm not really sure exactly how you want to
24 treat it, but I think it's oversimplified just to say if
25 it's in a computer and it's on a network, it's the same

1 thing as being through a public network.

2 That said, you can get it through a telephone,
3 through a form pile, from any one of these standard open
4 public networks, then you're online whether it's the web
5 or not.

6 MR. MEDINE: I think that's why the challenge of
7 this group of security issues is because of the public
8 access to some extent to these databases, that it raises
9 a lot of these concerns. Larry's been patiently waiting
10 so let's give him a chance.

11 MR. PONEMON: I've been waiting so long that I
12 forgot what I was going to say. My view has changed
13 already here in the last 15 minutes. First, thank you
14 for your very kind words about auditing.

15 Second, one of the issues here that I'm
16 wrestling with is I think about, well, the tobacco
17 industry, right? Can you imagine being assigned the
18 task of helping to create an ethical tobacco industry,
19 and how would you go about doing that?

20 Well, let's see. You could take the point of
21 view that disclosure -- and you have to push
22 accountability down to the consumer so you disclose it
23 on every pack, and there's a little warning that if you
24 do this you die, or you create a new science and you
25 make cigarettes non habit forming and non cancer

1 causing.

2 So the question is where were we in that
3 paradigm? Are we saying that disclosure is good enough
4 and buyer beware or smoker beware, or are we
5 actually trying to create something, a new technology, a
6 new approach, new science if you will to ensuring
7 privacy.

8 And I think it's an interesting -- it's a weird
9 connection but it's an interesting connection not to say
10 that we're in the tobacco industry, but we're dealing
11 with issues today, going back to what Jonathan said,
12 that right now the issues that we're raising, we can't
13 even think, we can't even conceive of how it might be
14 used five or ten years out.

15 That's how fast this industry is changing, so
16 that's really -- it's more of a question to this group,
17 where do we want to take this? Is disclosure good
18 enough or conventional means, or should we be thinking
19 about five or ten years out?

20 MR. MEDINE: Let's hear from the third seal
21 program, Paula?

22 MS. BRUENING: Thank you. Paula Bruening from
23 TRUSTe, and I was having a moment like Larry. I almost
24 forgot what I was going to say, but I want to actually
25 build on what Steve said and what Larry said.

1 First of all, I agree with Steve that there is a
2 certain level of reliance that consumers have when they
3 see a seal standing alone, and I don't think that every
4 consumer looks at every word of every privacy statement
5 that gets posted behind the TRUSTe seal, and for that
6 very reason I think our subcommittee didn't look to
7 notice standing alone as a solution to this.

8 But I also think that -- and perhaps it's the
9 peculiarities of the people who happen to submit
10 complaints through the TRUSTe's program, but a lot of
11 the people who do submit those complaints really do want
12 information about a security system when they think
13 there's been a problem.

14 And I think that having some level of notice
15 will inform consumers and give them a little better
16 sense of what computer security is all about, and I
17 think it serves a couple of functions. One is to make
18 it clear to them that there are limitations to
19 security.

20 Everybody at this table knows that there are
21 limits to it, that there are trade-offs involved in it,
22 and there is no security system that's perfect, and also
23 that consumers have their own role to play in this, and
24 I think that that's important across the board as we're
25 building this web and creating this marketplace.

1 And the second point I wanted to make sort of
2 builds on what Larry said. There's been so much
3 discussion about notice today, and perhaps I beat this
4 drum when we were last together, but I am absolutely pro
5 more notice, better notice, clearer notice, and I also
6 know being at TRUSTe how challenging that can be because
7 the more you want to tell the consumer, the more
8 difficult that becomes to make it succinct and
9 understandable.

10 So I think -- I'm trying to remember where I was
11 going with that. But I think we have to be very careful
12 that we don't overburden the principle of notice and
13 have it come to a catchall to solve all our problems
14 such that it turns into some kind of disclaimer that
15 protects companies to the point that all they have to do
16 is sort of point at notice and say, There we told you,
17 our responsibility is taken care of and while it's being
18 sort of buried in a notice that is four pages long and
19 that no consumer is going to have the patience to sit
20 down and read through.

21 So I think we've got a very specific challenge
22 here in making sure that notice, as we continue to rely
23 on it, rely on it more to make sure that it continues to
24 be meaningful and something consumers can use.

25 MR. MEDINE: Mary?

1 MS. CULNAN: I wanted to say two things about
2 the notice issues. It's not clear -- first of all, I'm
3 not arguing that notice is the answer because there
4 needs to be a process, that needs to be appropriate. I
5 like the 4, 2 solution myself, but I still want to argue
6 you need to have something, and one reason is the
7 difference between the offline versus the online world.

8 In the offline world you physically hand your
9 credit card to a person who hands it back to you after
10 they swipe it. You watch that happening. Yes, they can
11 go into the back room and steal your credit card number,
12 and this in fact has happened to my brother, so but
13 people tend to think that's not a very risky
14 transaction.

15 And this is a sophisticated audience here, and I
16 think most of us are comfortable doing business over the
17 web, but there are people who aren't here and they
18 aren't necessarily, and I think that's one reason that
19 there needs to be some method of building consumer
20 confidence, that it is a safe place to go.

21 How we do that I don't know. The seal -- just
22 something that says, This is okay, so I would argue
23 that.

24 The other issue is when there's nothing there at
25 all. I recently two days ago applied for a mortgage

1 online, and the web site was recommended to me by a
2 realtor, said nothing about privacy or security, and we
3 had a little conversation before I gave them my
4 information. Certainly what was I to assume. They said
5 nothing, no seal, and start giving them my name and
6 social security number and all this stuff, and we worked
7 it out but I think it's potentially an issue.

8 I think we should not sweep that off the table,
9 and I wanted to go on record to say that.

10 MR. PLESSER: They did not have an FCRA notice?

11 MS. CULNAN: No.

12 MR. MEDINE: We'll discuss that offline.

13 MS. CULNAN: They basically said, We will then
14 go get your credit report, et cetera, et cetera, but it
15 was -- I don't know.

16 MR. WHAM: You can't trust that Citibank.

17 MR. MEDINE: Moving along.

18 MS. CULNAN: That was news to them.

19 MS. GAU: This is Tatiana Gau. Having just
20 myself recommended and endorsed the seal program, I
21 would like to point out one thing that has really
22 emerged as the discussion of whether or not consumers
23 actually are going and then reading the standards if
24 they see the seal or if they just want the seal there to
25 do the work for them so that they don't have to bother

1 with that.

2 One of the concerns that I have about seal
3 programs is the ease with which the seal can be spoofed,
4 and particularly as seals become more prevalent or if
5 they were to be embodied in a standard of some sort,
6 you're going to see even greater spoofing of seals,
7 which of course the number of the different seal
8 programs have taken steps to try to prevent spoofing of
9 seals so that when you click on it, if you end up at a
10 certain location, you know it's not a real seal and
11 those things.

12 But that means the consumer's clicked on it, and
13 if all the consumer's relying on is the visual of the
14 seal, I think that those -- that's a problem that needs
15 to be considered.

16 The other point I would like to make goes to the
17 discussion of the security program that a company might
18 maintain in place and minimum standards that could be
19 documented.

20 I agree with you, Deirdre, that in fact you
21 could come up with a list of steps that a minimum --
22 that a company must take at minimum, including audits on
23 a regular basis or at least some kind of penetration
24 testing and things of that sort.

25 But one thing that I would add within that

1 program would be a resource for the consumer to turn to
2 if they encounter a security problem 24 by 7, that
3 security is an issue, that they need to be able to turn
4 to somebody other than the FTC or the National Fraud
5 Organization or whatever the agency they might turn to
6 might be where they can actually get some sort of
7 response and some kind of advice on what to do.

8 I understand this might be difficult for upstart
9 companies that just don't have the resources to build in
10 that kind of infrastructure, but I think as far as
11 security goes, that the minimum expectation needs to
12 include the ability to respond to the consumer and to
13 tell the consumer where to turn, just like we require
14 privacy policies to tell the consumer who they can turn
15 to in the company to get privacy questions answered.

16 MR. MEDINE: The seal programs, I think one
17 point to respond to Tatiana's point about spoofing, and
18 then I also want to suggest possibly a controversial
19 issue which is should a web site disclose that it's
20 having security problems if consumers are assuming that
21 sites are providing good security and the site is aware
22 that it has security breaches or weaknesses. Is there
23 any duty on the site to warn consumers about the
24 problems it's facing.

25 First I'll give Steve and Paula a chance to

1 start.

2 MR. COLE: I'll be very quick. I don't want to
3 divert this discussion. Yes, seals can be spoofed.
4 Yes, there is a readily available and much used security
5 mechanism to avoid that. I don't know about PWC, but I
6 know TRUSTe and we use the same service.

7 There is really a low risk here because of the
8 high energy level put into avoiding spoofing and
9 catching it when it happens. Also if it's a well known
10 organization, in addition to those efforts which are
11 very, very extensive and workable, there's great
12 consumer feedback too, so we learn about it that way.

13 I don't think the benefits of the trust mark are
14 even close to being outweighed with the difficulties of
15 enforcing it, but resources have to go into that, and I
16 can't lose the opportunity to make my normal pitch to
17 the Federal Trade Commission, seals and trust marks are
18 kind of like the -- it's the new thing that everyone is
19 talking about.

20 And so they're coming out of the woodwork, but
21 not everybody is a quality program, even though I think
22 the ones around this table are, and so it's very
23 important to make sure that the kind of resources that
24 protect the sanctity of the seal are backed up by
25 enforcement in their views.

1 MR. MEDINE: Paula?

2 MS. BRUENING: Paula Bruening from TRUSTe. I
3 really have to echo what Steve just said. We do use
4 similar technology. It's basically out checking the
5 entire web all the time. We have constant reports. We
6 have people looking into exactly what these sites are
7 doing. We're following up on that all time.

8 It does take a lot of resources, and it takes a
9 lot visuals and a lot of monitoring, and we're
10 constantly putting more resources into that, but I think
11 it is workable, and I think it can address the spoofing
12 problem, and I agree with Steve that the spoofing
13 problem is definitely outweighed by the benefits of the
14 seal programs.

15 MR. MEDINE: Do you want to address this
16 particular issue, Larry?

17 MR. PONEMON: Yes. There may be a general
18 misunderstanding or misconception about the seal. A
19 seal is a statement. It's a disclosure of compliance,
20 and you basically underwrite that process and do some
21 review work, but it's not equivalent to a financial
22 statement audit.

23 The financial statement audit requires an
24 auditor to do a lot of stuff to test, to prove, to
25 collect evidence, and quite frankly, I think with some

1 seals, not all seal programs, but some seal programs
2 have difficulty just in terms of their own
3 infrastructure to do that kind of work.

4 So I think there's some risk that there's going
5 to be the kind of the false positive problem, and it's
6 not going to be folks around this table, but there would
7 be new emerging auditing or seal programs that will
8 provide false confidence to us.

9 We just have to be aware of that fact. It's
10 probably going to happen, and it's part of the big
11 economy that we operate in.

12 Thanks.

13 MR. MEDINE: Stewart?

14 MR. BAKER: Thanks. Stewart Baker from
15 Steptoe. I thought I would do since there's so many
16 techies around the table I would draw a grid because I
17 think it helps understand the notice issue.

18 If you wrote down one side of -- our options
19 down one side of the page like sliding scale and
20 appropriate plus plan, the 4 and 2 combination, the
21 industry standards and existing rules. Then across the
22 top you would write the enforcement options that we put
23 that could be used to make sure those actually work
24 like, government lawsuits, express cause of auction,
25 audits and just relying on existing law.

1 We generally felt that notice was not much use
2 except in certain circumstances which I marked here.
3 It's useful when you got industry standards across the
4 board because people need to know which industry
5 standard you belong to. It's useful if you have an
6 audit because people need to know that it was audited
7 and by whom, was it Larry or some fly by night.

8 And other than those circumstances, the notice
9 is not much use, and I do sense a kind of "Federal Notice
10 Commission" pressure here to say, yes, yes, yes, notice,
11 it's a great idea but it's not a good idea most of the
12 time, and you guys should curb your prejudices about
13 that.

14 MR. MEDINE: We look forward to reading your
15 views on the subject.

16 MR. BAKER: Probably in two pages only though,
17 right? On the question of whether you should notify
18 people about breaches, this isn't an issue we looked
19 at. It's another notice issue I will note, but there
20 are some real problems there.

21 You always get in compromises. You're always
22 under attack. There's always a risk that somebody got
23 into your data and you don't always know what they did.
24 There would be a serious false positive problem if you
25 tried to provide notice every time you thought it might

1 have happened, a false negative problem as soon as you
2 stop doing that, and a kind of -- an opportunity to say
3 to people, Hey, have you thought about suing me because
4 you might want to.

5 You might want to say that the last 20 things
6 you bought with your credit card weren't really
7 delivered to you but to somebody else because your card
8 was compromised.

9 I think people to do this notice when it's quite
10 clear that there's a risk, when they get evidence that
11 people's cards have been compromised because they want
12 to minimize the harm to consumers as quickly as possible
13 because they're going to end up hurt by it, but I think
14 a general requirement would be risky.

15 MR. MEDINE: Ted, and then Frank?

16 MR. WHAM: I personally have very little
17 knowledge of the security side of this, so I have a
18 question for the people who do have the expertise in
19 here, and we have a lot of them in this group. There's
20 a lot of discussion about having appropriate security or
21 not having appropriate security as if it was a very
22 binary thing, and whether there is a benefit to having
23 some type of a standard setting, and that can be through
24 a commission or it can be through a seal program or
25 something like this where there are specific tests that

1 have to be met for the good, better, best security
2 system.

3 And I think if all of us would agree that better
4 security is in general a consumer benefit, that if
5 customers could say, I could buy from consumer site A
6 that's got good security or site B that's got better
7 security then there will be a natural tendency for
8 a consumer to move towards the better security and to
9 enhance public good.

10 Is that something that makes sense?

11 MR. MEDINE: Tom, do you want to respond to
12 that?

13 MR. WADLOW: Well, yes, and I guess I want to
14 respond by echoing what Tatiana said earlier in that
15 really any kind of a technical standard on that is not
16 only useless, it's sort of worse than useless because it
17 depends to create a sense of false optimism whereas the
18 problem is changing at best.

19 A process related rating is more interesting,
20 but you still then end up having a problem of verifying
21 that the company says they're going through the process
22 is actually going through the process. An audit related
23 standard is as a fine idea, but in order to be actually
24 realistic, you need to be thinking about doing those
25 audits every month which would make Larry very happy but

1 most everybody else pretty unhappy.

2 MR. PONEMON: Why does everybody pick on me?

3 MR. SCHUTZER: I would like to respond just to
4 that point.

5 MR. MEDINE: Very quickly, yeah.

6 MR. SCHUTZER: This attention here -- I think
7 actually most of the time people would appreciate not to
8 have the security to be honest with you. What happens
9 is if you leave it up to the security officer, then he
10 would have a lock on every door and each door would have
11 a different key, and it would be difficult -- and he
12 would never let you put in new features and functions
13 because every time I put in a new feature and function
14 in a government security office, I don't want any
15 software unless it's been around for about ten years and
16 invented and I know there's no problem with it.

17 So if I'm coming in and out as the service
18 provider, I'm not the security officer, I have a
19 different hat on now, I want to put the features that
20 have new bells and whistles and the added convenience,
21 and I want to make life simple for the consumers, and
22 you know something? That's what they want unless
23 there's a problem.

24 MR. WADLOW: Exactly.

25 MR. SCHUTZER: That's the issue we have with

1 security is nobody really wants it, but they need it,
2 and they don't even realize they need it unless there's
3 a problem so you're always going to have this tension.

4 MR. MEDINE: Frank?

5 MR. TORRES: Stewart's graph was so enlightening
6 that actually, and I know he doesn't like notices, but I
7 actually came up with a very simple one. I thought it
8 might be appropriate. Maybe we might get this issue out
9 of the way. Welcome to our web site, we can't guarantee
10 your security but we appreciate your business.

11 (Laughter.)

12 MR. TORRES: One of the most frightening things
13 that has come out of this process is the fact that there
14 can be no guarantees of security, and I think it would
15 be inappropriate for a site to mislead consumers into
16 believing that a site was secure, but that puts us all
17 into a bit of a quandary.

18 I started to go down the avenue of, Is there a
19 way to provide notice to allow consumers to compare
20 sites so that sites having better security than other
21 sites might get some marketplace advantage from that and
22 that would be beneficial to consumers to know, but it
23 sounds like even getting there might be difficult.

24 I think -- this may be outside the scope of what
25 we're talking about, but I think for the consumer at the

1 of the day, I may not care about the level of security
2 that you have. What I care about is what are you going
3 to do when things go wrong?

4 With credit cards, at least liability is
5 limited, so I think it's in a way ironic until the law
6 changes, and who knows they might, but until they do,
7 right now probably the safest way to make a payment on
8 the Internet is using your credit card, and yet
9 consumers are still wary about doing that because of
10 the security problems.

11 So to me -- and I don't know how to -- I'll make
12 a push to include this as part of our discussion,
13 security is one thing, notice about security is one
14 thing, but more importantly is what are the policies of
15 the site or the company when things go wrong for a
16 consumer?

17 What steps will they take to help me figure out
18 what to do when my information is taken from a site, and
19 that I think is to me a sliding scale. It's maybe not
20 my credit card number but my debit card number where
21 some of the -- they're voluntary protections out there
22 but they're not set down in stone, so that could
23 change.

24 Actually the harm there may be great if my bank
25 account is wiped out versus you releasing information

1 about my hair color. It's a little bit different in
2 that sense.

3 MR. MEDINE: Greg?

4 MR. MILLER: Thank you. Greg Miller,
5 MedicalLogic. A couple of points, to the comments
6 between Mary and Stewart, I waited so long to say
7 something with regards to notice, its utility and
8 reasonableness and whether you need it or not, just a
9 little data point.

10 Our partner MedScape and us did some looking
11 back at our logs on our web sites. Mark Bolding, our
12 chief counsel of MedScape, did this to figure out what
13 the traffic was on our privacy notices and our security
14 notices, and you'll be interested to know for health
15 care sites, I think with all the news lately that could
16 be kind of an interest, that approximately 5 percent of
17 the entire traffic on our web sites is contributed to
18 people actually looking at either of those pages.

19 I think it would be an interesting exercise for
20 us as part of what we're trying to accomplish if each of
21 us went home and asked our web people to take a look at
22 the traffic logs and find out how many page visits are
23 attributed to the privacy notice that you may or may not
24 have or the security notices that you may or may not
25 have and then reflect on that in terms of whether notice

1 has utility.

2 Having said that, perception is 99 percent of
3 reality in the court of public opinion, and I think that
4 people are used to seeing that there is at least some
5 point or two to a notice whether or not in fact they
6 read it.

7 The other point I wanted to make was in light of
8 the remark about change being the only constant in this
9 industry, and we have to be mindful of what we're doing
10 with regard to that, to the extent of us working on
11 security options, and I was on that subcommittee, and
12 Stewart or Deirdre, correct me if I'm wrong, but I seem
13 to believe that we sort of concluded that there is a
14 distinction without significance with regards to the
15 difference between a public, semiprivate or private
16 network in terms of security options and thinking about
17 notice of access and security and whatnot.

18 Now, there may be differences with how you
19 assess risk, the kinds of security you put in place or
20 the kinds of mechanisms you use to manage access and
21 whatnot, but just bear in mind with change being the
22 only constant, I think that there's a grain, there's a
23 blurring line between private, semipublic and public
24 networks.

25 MR. MEDINE: Dan?

1 MR. JAYE: Thank you. On this topic, and I'm
2 going to rock the boat a little bit by not immediately
3 jumping on the 4 plus 2 or 2 plus 4 bandwagon here and
4 portray the fact that I have probably a natural
5 preference for sort of market forces and organic
6 solutions, and that's because on the Internet the
7 development that I think has -- one could characterize
8 the constant there is that it's grown so quickly because
9 of organic developments, and say that there may be a
10 flavor of 5 that's not maybe illustrated in this
11 write-up.

12 But it seems to me that there's a case in
13 security where -- there's an area where the company's
14 interests and the consumer's interests are aligned, in
15 which case there's already a strong incentive for the
16 company to keep the data secure. They're going to make
17 efforts, they're going to have audits, they're going to
18 hire insurance companies, and by the way I haven't gone
19 out and invested heavily in insurance companies before I
20 propose this.

21 But there's an area there that I think in fact
22 market forces and in fact the risks that the insurers
23 have to carry will drive some level of solution. The
24 issue is the gap between the consumers' interests and
25 the company's interest.

1 There are cases where the consumers' issues may
2 be dramatically larger than the company's, like the
3 credit card data. Credit card data might be an example
4 of that today. I would just wonder if there is an
5 innovative way to solve this problem by using, for
6 example, contracts with seal programs as a way of
7 bridging that gap.

8 So, for example, if I knew that TRUSTe or BBB
9 online had a right of action against me by which they
10 could effectively represent the consumers' interest or
11 heightened interest in the security of the data such
12 that that would incur -- incent me to retain auditors
13 and also take out liability insurance to cover that
14 risk, which of course would then incent them to make
15 sure I better be doing a good job at it, that that might
16 be a more innovative and market force driven solution to
17 the problem than trying to create another area in the
18 government that's going to oversee this like the medical
19 malpractice area or something equivalent to the
20 Department of Transportation that's going to try to make
21 sure that our brake safety is correct in the cars.

22 That's an example here that I go back to is that
23 consumers don't want to know that their brakes on their
24 cars are safe -- are with this specification or that
25 specification. They want to know that their brakes are

1 safe.

2 In security it's the same thing. They don't
3 care about it until it's broken. Then once it's broken
4 they want to have some sort of right of action or
5 solution.

6 MR. MEDINE: We obviously talked earlier about
7 identity theft as a situation where the interest may not
8 be coverable, but in a situation where interests are
9 aligned, how do you operationally see the difference
10 between option 5 relying on existing remedies and them
11 the 4 plus 2?

12 Do you see a difference in practice, how they
13 would -- how they would operate? In other words, if it's in
14 both consumers' and the sites' interest to protect the
15 security, how would the method of protecting it differ
16 from the appropriate end of the circumstances approach?

17 MR. JAYE: Well, I think in the case where the
18 interests are aligned, in the case of publicly traded
19 companies, there are fiduciary responsibility, and it's
20 the responsibility of the officers and directors of the
21 company to make sure that they're handling it
22 correctly.

23 I think in the cases of private corporations,
24 once again the lawyers in the room can correct me, but I
25 believe that that might be an area where you might argue

1 that there's less really obvious incentive that they
2 manage the company's liabilities to the level that
3 everyone wants.

4 MR. MEDINE: Roger?

5 MR. KIRKPATRICK: I was just going to -- two
6 things. One thing, I just couldn't resist commenting on
7 the earlier comments about rapid change and all that.
8 Wasn't it in the 60s when the Culture Shock book came
9 out? This is nothing new. I remember seeing a show
10 about the 20s about how everyone was aghast about the
11 rapid change, so, yeah, rapid change, exponential
12 change, it was the same thing a hundred years ago. It
13 will be the same thing a hundred years from now.

14 I think that just highlights the importance of
15 not creating standards that are so inflexible as to
16 prevent the benefits of change which leads to another
17 point, which is potentially against the interest of my
18 company and all the other companies here, but I'm going
19 to make it anyway, and that is we don't want to impose
20 burdens and standards either in the security area or
21 frankly in any of the other areas that raise the
22 barriers of entry to online commerce so that everybody
23 just gets locked in.

24 You can -- it's fine to talk about the kinds of
25 companies that are being represented and they're

1 advising the FTC what they're willing to do. The FTC
2 has to keep in mind the other people who are not at the
3 table because you could just lock everything in to
4 stifling.

5 MR. MEDINE: Let me propose that we go until
6 three and take a break, and so why don't we go through
7 as many comments starting with Deirdre and Rick down the
8 line until three and then take a break and then come
9 back, if that's okay.

10 MS. MULLIGAN: Deirdre Mulligan. I wanted to
11 comment on the -- Stewart made a comment earlier that
12 security is one area where clearly if people mess up
13 there are consequences, they're going to get sued, and
14 in fact we find out -- I know there's been a number of
15 studies, particularly in the financial industry, I think
16 Dan may be able to be more informative on where, I don't
17 know, it was 80 percent of companies have experienced
18 security breaches in the past six months or whatever.

19 And I'm certain that maybe 1 percent of those
20 actually resulted in a consumer even knowing that their
21 data might have been compromised, and the fact of the
22 matter is that I think security breaches are in fact the
23 most difficult for consumers to get a grip on, and
24 therefore to enforce their rights under existing
25 remedies as it is, and so the notion that the market

1 will respond to it is very, very interesting.

2 I think if there was an obligation that
3 consumers get notified when a breach has occurred and
4 their data may have been compromised, we might actually
5 get a functioning market that would lead to a race to
6 the top.

7 But in fact there's an incentive, as Stewart
8 said, dramatically in the other way, which is that there
9 is not an industry sitting around this table who wants
10 to send a notice out to all the consumers saying, We had
11 a massive security failure, everyone's data may have
12 been compromised, we don't know if it's yours, but it
13 may have been.

14 No one wants to send that notice out, and so the
15 ability to have feedback -- and we've had some pretty
16 recent examples. There's a credit card case, one of the
17 web sites three months ago I guess the security was
18 breached. Thousands of credit cards were accessible .
19 They didn't notify us.

20 MR. SCHUTZER: That was a merchant where they
21 got the credit card sites over. But it was an Internet
22 bank that recently had some losses.

23 MS. MULLIGAN: And did they notify consumers?

24 MR. SCHUTZER: Well, it hit the newspapers.

25 MS. MULLIGAN: Yeah, but all I'm suggesting is

1 that this is an area where I think there's some real
2 issues about whether or not -- I would prefer to give
3 people guidance on the front end than to rely on the
4 child wears.

5 MR. LANE: Say that a little louder, Deirdre, I
6 didn't hear you.

7 MR. MULLIGAN: Perhaps it's not such a good
8 method to say the market will work. The market doesn't
9 have full information here, and I think there's some
10 reasons to believe that full information, one, might tip
11 people off to other people's vulnerabilities. Maybe we
12 don't want them sending out this kind of notices.

13 Stewart said it might invite people coming in
14 saying, I didn't make those last 50 charges, huh, so I
15 think that I agree with you there's a place for the
16 market, but I'm not quite sure where it works here.

17 MR. MEDINE: Rick? Why don't we have Rick make
18 the last comment and take a break, and what I would
19 propose to do is then come back, have our public comment
20 period, and then keep your flags up, and you can have a
21 chance to make your points after the public comment
22 period just so we make sure we get that in and it will
23 get us out on time.

24 MR. LANE: In terms of the market forces
25 argument, and I think require all commercial web sites,

1 that's always a problem, to require what, is one of the
2 questions that we have to always ask ourselves, but what
3 will the company do.

4 I think Frank hit a really good point is that
5 from -- as he stated from a consumer standpoint, it's --
6 what is the recourse after the fact, what can -- is a
7 company willing to do, and in terms of a notice, when
8 we're talking about the security, it's hard to list
9 here's our security plan, that causes problems.

10 But you can in fact as a competitive advantage
11 if to build the consumer's confidence, here's what we do
12 if your security is compromised, and one may be
13 notification but then again we all know notification may
14 not go out immediately because they may be working with
15 the FBI or they're trying to draw folks in, so there's
16 reasons why notification does not go out immediately,
17 and it could be because of law enforcement issues.

18 But there are companies that have sent out
19 notices immediately following an attack, and one of
20 those is Real Names.com. They suffered a huge hit where
21 all their pass codes and credit card information was
22 exposed, and they immediately sent an email out to all
23 their customers notifying them because they thought that
24 was in the best interest of their consumer relationship
25 that when we are hit and instead of these charges coming

1 out and reading it in the paper, that we'll let everyone
2 know first.

3 And in fact it was the best way because they
4 continued to grow, and Microsoft has purchased 20
5 percent of them, and obviously it's been a good thing.

6 In terms of other market forces, the insurance
7 side is a great way. Insurance costs for web and
8 security is increasing. It used to be just Lloyds of
9 London was the only company out there that provided
10 network security insurance for web transactions, and now
11 there's a whole host of new products coming out.

12 With those products are coming auditing
13 procedures in order, because of the lost revenue,
14 lawsuits that could occur from private rights of action
15 and a whole other costs that can occur when a security
16 is breached, so there are market forces.

17 I mean, don't forget this is a new economy.
18 It's only three to four years old that we've really
19 started growing and getting bigger and bigger so there
20 are forces that are coming online that will take care of
21 some of the concerns and try to balance it out.

22 And the last point is from a security standpoint
23 and I didn't realize this until I heard it from Jeff
24 Bezos of Amazon, that for transactions that are done
25 online with a credit card that are not signed, the

1 responsibility of the \$50 limit, offer of the \$50 limit
2 isn't borne back by the bank to pay back Amazon, but
3 Amazon itself eats that amount, and because of that
4 there's an incredible incentive both to verify who the
5 individuals are plus to make sure you have a secure
6 transaction in place and to notify and have other types
7 of procedures in place so you don't have to bear those
8 additional costs.

9 MS. GAU: If I may, can I -- just his first
10 point about resource that you can turn to, the company
11 notifying the consumer and the consumer having the
12 ability to notify the company?

13 I again want to support that and also point out
14 that that's also an extreme value that the privacy seals
15 provide because they provide organizations that the
16 consumers can turn to to notify the organization that a
17 company is not compliant with its obligations, and we
18 completely support the privacy seals.

19 MR. LANE: Under contract don't they have five
20 days to respond to any notification under TRUSTe I
21 believe.

22 MR. SCHUTZER: We're talking about proactive and
23 resource I think at this point. You have to decide if
24 it's market forces or not. In our case we proactively
25 tell people when we think their credit card, for

1 example, has been compromised, and we give them
2 recourse. We reverse all that value. In some instances
3 when you think things are serious enough in a industry,
4 you'll actually regulate and do that.

5 But most of the time market forces do tend to
6 work that way, that those firms that are more
7 responsible providing the recourse and the proactive
8 notification get no network, but insurance, just be
9 careful who's providing the insurance and whether they
10 have the resources to back up the insurance and pay off,
11 if it's necessary.

12 MR. MEDINE: Let's take a break. Let's try to
13 reconvene at 3:15 so we can start the public comment
14 period. Thank you.

15 (A brief recess was taken.)

16 MR. MEDINE: Let me ask if there are any members
17 of the public who would like to make a comment, if we
18 could have people at the table.

19 We've set aside time at each meeting as you know
20 for public comment, and I would invite anyone, we have a
21 microphone set up, if there's anyone from the public
22 present that would like to make any comments. This is
23 your opportunity? Yes. We have a member of the public
24 who would like to speak, if you could identify yourself
25 when you arrive at the microphone.

1 MS. SOROKIN: Cherie Sorokin, and I represent
2 an upstart company. I guess she's not here to hear me
3 say that, but actually we like to think of ourselves as
4 an upstart company as a matter of fact, but the company
5 I work for is actually still in stealth mode, but I will
6 tell you a little bit about our product which is a form
7 of being able to do personalization on the web and
8 actually off the web as well in a manner that doesn't
9 compromise consumer privacy.

10 It's made possible by a whole series of advances
11 in technology and by shifting how we think about what's
12 a server and what's a client, and you can watch for
13 announcements about us in May or June.

14 But the reason that I'm here at this hearing is
15 because I do think it's important, and a number of you
16 have mentioned that today, that first of all upstart
17 companies do need to be thought of. It is difficult to
18 take on the burden as a brand new company with a new
19 idea of a lot of heavy duty regulation about both
20 disclosure and about security and a number of things
21 that you could prevent all kinds of technological
22 solutions to a very serious issue about protection of
23 consumer privacy if you overregulate.

24 And aside from the regulatory burden, there's
25 also the issue that there are many, many companies out

1 there trying to address what -- if there's a need out
2 there, there will be some company trying to figure out a
3 way to solve that need.

4 And much of the regulatory language that I worry
5 about on a daily basis is by its very nature designed to
6 address existing technology, what we know about now, and
7 it has a hard time anticipating what might be coming out
8 there and could actually block that.

9 I spent a lot of time worrying about the use of
10 verbs in legislation, share, use of data, for example,
11 if you're sharing data and you're using data but you're
12 not actually disclosing data, which is possible, how
13 does that fit within the regulatory framework which
14 prohibits sharing of data without some type of notice?

15 Well, again, if the personal identity is never
16 there and yet you're still prohibiting sharing of data,
17 it can be a real problem.

18 So my point is just do think about the start-up
19 environment and companies that are out there trying to
20 address a need that's very obvious and ways that your
21 well intended actions or well intended thoughts about
22 this could possibly prevent the very solutions that
23 you're looking for.

24 MR. MEDINE: Thank you for your comments. Are
25 there others from the public who would like to approach

1 the microphone and speak? Again if you can identify
2 yourself, please.

3 MR. LEE: Sure. My name is Dennis Lee. I'm
4 here to represent length an organization called IFSec.
5 We're an information security firm in New York.

6 It's funny because in the last few times that
7 I've been here, I seem like -- you should look at the
8 people around you, the people who are in the audience.
9 It seems like we know all of you, even though you
10 probably don't know who we are, but I want to give you
11 just something to think about as you're going into this
12 area on security, particularly notices.

13 In our experience with anything where there's a
14 need for a mass notice, mass notification to the public
15 about a security incident, our experience with things
16 like virus incidents, someone can also fake that
17 message.

18 So what I'm saying is as you're considering
19 notification to the public, there has to probably be
20 some sort of a clearinghouse within your own company or
21 your policy statement that says, how does someone in the
22 public prove whether or not that was a hoax.

23 If a credit card -- if there was some flash
24 report saying, Oh, the credit card information at this
25 company has been stolen, the public will get into a

1 panic and an uproar, so there's got to be a way of
2 dealing with that within your own company, within your
3 own policy, and I'm saying that there's probably
4 something you should consider as you think of
5 notification.

6 MR. MEDINE: Thank you very much. Others who
7 would like to speak from the audience first and then we
8 can respond to that? Yes, we have another.

9 MS. KNUDSEN: Hi, my name is Liz Knudsen. I
10 just want to make a point in listening to the
11 discussions, and it was also made, is that I think a way
12 to think about this is coming totally from the
13 consumer's perspective because if we're trying to solve
14 the problem of privacy, the consumer is the one who's
15 really going to be in the best position to monitor their
16 own situation.

17 So if you start from what would the consumer
18 need to be in the best position to monitor the
19 situation, and then build from there out to how the
20 technologies and how did the standards apply to that, it
21 might be a way to move towards a solution that may be a
22 little more viable.

23 There's always going to be problems with it, but
24 so often because there's so many industry people, that
25 that gets a little lost. If you start just from the

1 consumer it might move you in the right direction.

2 MR. MEDINE: Thank you. Others who would like
3 to take an opportunity to make a comment for the
4 committee?

5 Thank you for those who submitted public
6 comments. Why don't we take just a few more comments
7 for maybe five or ten minutes or so including people who
8 had their flags up and then turn to trying to wrap up
9 where we go from here at the next meeting.

10 Alex?

11 MR. GAVIS: Alex Gavis, a couple quick
12 comments. One thing in terms of notice that we may want
13 to think about is I think we've been thinking a lot
14 about notice of internal security measures, but also
15 notice could be important to set expectations for the
16 customer, including perhaps in the notice there could be
17 a discussion about transmission risks, the types of
18 access that might be available, what kind of encrypted
19 browsers the actual -- the web site operator will
20 accept, particularly with transactions.

21 There could be a discussion about authentication
22 and pins and how the customer should keep their pin
23 private and how that can be compromised, so I think
24 there is a room for notice and perhaps educational
25 notice. It may not have to go so far as to disclose

1 internal practices, but it might talk more about
2 transmission issues.

3 Secondly, I want to just get to something that
4 Ted said about offline and online information. One
5 thing I think that would be worthwhile just for the
6 report to actually discuss perhaps even up front as to
7 what it is that's different about the online world and
8 why it is that we're actually pursuing it or why it is
9 that this report is going to talk about the issues that
10 it is based on what we identify as the differences in
11 the online world.

12 That may be a worthwhile venture.

13 MR. MEDINE: Thanks. Jerry?

14 MR. CERASALE: Jerry Cerasale. I think the
15 first public comment actually took most of what I wanted
16 to say, but on page 3 of the security piece, there's the
17 additional policy concerns, big versus small business
18 concerns, and I would also extend that to the new
19 start-ups, the entrepreneur, this is what the Internet
20 is, and we really have to make sure that you don't
21 create a situation where you have a huge barrier to
22 entry.

23 As a matter of fact, you could look at privacy
24 and notice and security concerns as large companies
25 trying to bring huge barriers to try to lock out other

1 entrepreneurs, and I think that it is a balance, and I
2 think that we even can look at our authentication
3 discussion we talked about. You don't want to raise the
4 barrier so high that people can't jump over it or so low
5 that it's useless.

6 And I think that it's very important as we look
7 at what type of security you're looking at. I mean,
8 maybe some type of notice but to watch out for giving
9 away trade secrets is probably there, but the consumer
10 is really looking for, I want to make a purchase, do the
11 stuff, send it and know that my information's safe and I
12 don't want to read about it and know all that stuff. I
13 want it nice and easy.

14 And I think that they also want the ability to
15 -- the Internet offers of lots of new competition, and
16 we have to be careful to make sure that we don't set up
17 all sorts of audit procedures -- he's not here, damn it
18 -- audit procedures that would significantly increase
19 the cost for business or significantly increase the cost
20 if we're going to look at seal programs so that TRUSTe,
21 BBB online, et cetera, the price of the seal becomes
22 astronomically high.

23 MR. MEDINE: Thanks. Of course the FTC is very
24 interested in competition and barrier to entry issues so
25 I'm sure they'll appreciate your comments on this.

1 Richard?

2 MR. BATES: This is kind of a macro issue, and I
3 guess it involves everything we've talked about today,
4 but my understanding is we're going to issue a report,
5 and it's going to go to the FTC, and then they're going
6 to make some kind of recommendation.

7 And having said that, there's at least a dozen
8 bills pending on Capitol Hill right now dealing with
9 these issues, and there will be plenty more. They'll
10 probably be at least 200 in various state
11 legislatures around the country, and that exactly is
12 what's going to kill self regulation as far as I'm
13 concerned is 50 State Attorneys General.

14 So when we're thinking about all these things,
15 one thing I would like for us to think about, and I'll
16 certainly put it in my one-page remarks at the end of
17 the report, is that we have some uniformity of the rules
18 and regulations that we're going to try to implement.

19 We have one rule for each thing, not 50
20 different rules, 50 different regulations, and I'm
21 afraid that's where we're headed, so as far as my
22 company's concerned, that's what the scares the hell
23 out of us.

24 We'll live with what we have to live with, but
25 living with 50 different variations of that is going to

1 be very, very difficult.

2 MR. MEDINE: Dan Geer?

3 MR. GEER: Yes, Dan Geer. It's just another
4 small security point. On the issue of notice, it is by
5 and large a bad idea to say what it is you do from a
6 security point of view, whether that is prospectively we
7 do the following, or it's retrospectively, we failed to
8 do that and now we do this.

9 Regardless of that, it is by and large a bad
10 idea. It's typically well understood by people who have
11 a lot to lose, and at the same time saying or that there
12 might be some competition on the basis of whether or not
13 someone's security policy is better or worse as read on
14 a web site strikes me as a little bit like airplanes
15 saying that you should fly us, we fall out of the air
16 less often than they do, and that's not in anybody's
17 interest either.

18 I don't actually see a place for security notice
19 per se for all of those reasons.

20 MR. MEDINE: I have something to propose that we
21 call on Rob, Rick, Roger, Richard and then move into
22 Lance and a discussion of the report and the processes
23 for the next meeting, oh and Frank, just so that we have
24 time to discuss where we go from here, if that's okay.

25 Rob?

1 MR. GOLDMAN: Rob Goldman, Dash.com. This is a
2 small point but one related to the points many people
3 have raised about start-ups and the resources necessary
4 to adopt some of these policies that we've discussed.
5 It strikes me that everyone in the room probably doesn't
6 know what Dash.com does, which I think is a terrible
7 problem, so I want to outline what we do just a little
8 bit because I think it's relevant.

9 We collect clickstream of information, navigational
10 information on the users who use our tool which finds
11 opportunities for them to save money as they surf the
12 web, and we've gone to great lengths and great expense
13 and continue to in order to provide access to that very
14 detailed click stream information to the users as it
15 goes.

16 And this is a point of information for the
17 committee and stands in contrast to Greg's number on 5
18 percent, and it might be interesting to note that our
19 service is largely marketing oriented and designed
20 essentially to find new bargains online, and the health
21 information certainly is a more sensitive and
22 significant area.

23 But despite the sort of great lengths that we've
24 gone to to provide the access, very few of our customers
25 have actually used it in contrast to the 5 percent

1 number that Greg raised I actually check it every time
2 before I come to Washington, and it's at its highest
3 right now which is .014 percent of the -- it's sort of
4 apples to oranges a bit.

5 This is .014 percent of our information that's
6 actually been edited or deleted at all by users. A much
7 higher percentage has actually been accessed. But I
8 guess the good news is we believe that users haven't
9 needed or haven't felt the need to delete the
10 information largely because we provide access to it, so
11 they feel reasonable secure that the information is
12 there.

13 But we often question and scratch our heads
14 looking at the sort of vast expense that we have to go
15 to given the limited resources to provide that access if
16 it's not reasonable to expect more use of it.

17 MR. MEDINE: Thanks. Rick?

18 MR. LANE: Just a couple comments. One on the
19 fraud comment in terms of notification and someone
20 sending out -- that's one of the most common scams. I
21 remember when I got my wallet stolen. I got a call back
22 someone saying they were from my bank, we need your pin
23 number for X, Y and Z, and I was like, No, I don't think
24 so.

25 MR. WHAM: Star 69.

1 MR. LANE: I tried but because it was a trunk,
2 we couldn't trace the number. But the fact of the
3 matter is I could see that happening as well,
4 notification going out. Your credit card has been
5 compromised, here's the number we have, verify it and
6 send it back to see if -- and so that's obviously a
7 concern with notification and making sure that it is a
8 real notification.

9 Getting back to uniformity of regulations that
10 was brought out, and I think it's critical in this whole
11 world order, especially for small businesses where they
12 are trying to figure out what are the rules of the road,
13 not just in their local level, now the national level,
14 in the international level, and now with all 50 states.

15 I was testifying down in front of the statehouse
16 in Texas earlier this week, and the fact of the matter
17 is I have a digital cell phone here where I can access
18 the Internet from wherever I am. Now, if we do have 50
19 states out there with 50 security requirements and 50
20 privacy notices, which one am I supposed to try to
21 scroll through six pages of through my little cell
22 phone, and where -- is it the one, the state I'm in, was
23 I in Texas, it's a 202 area code phone, was it D.C.'s
24 privacy and security notification, is it Maryland's
25 because that's where I live, or is it where the server is

1 located or where the company is located?

2 So I think uniformity and having some type of I
3 hate to use the word preemption if we're going to go
4 down this road, and this is why from a standpoint of
5 self regulation it works because it doesn't matter, it's
6 my sensibilities instead of, Here are 50 states that are
7 dictating to me no matter where I am from.

8 And so I think if we are going to go down the
9 road of some type of regulation which I hope we don't,
10 but there has to be uniformity. The states, it could
11 cause some serious dampening of the growth of e-commerce
12 if there are differences in what we need to know in
13 terms of security, privacy and so forth.

14 MR. MEDINE: Roger?

15 MR. KIRKPATRICK: Just a quick point because
16 some of my other points were already made. I don't want
17 to sound too much like Ted but it is --

18 MR. WHAM: Thanks.

19 MR. KIRKPATRICK: For instance, in the magazine
20 industry that I'm in, people order magazines all the
21 time through tear out postcards where they write their
22 name, address on a postcard which gets mailed back.
23 Anybody can read that.

24 So you know, there are lots of commercial
25 activities that go on in this country where people are

1 not concerned about security. We need to look at
2 security I think very much on a sliding scale, what are
3 people concerned about, what are they not concerned
4 about and not just assume that they're concerned about
5 everything.

6 MR. MEDINE: Richard?

7 MR. RICHARD SMITH: Hi, Richard Smith. I just
8 want to make a quick comment about the start-up
9 situation. Clearly companies when they're getting off
10 the ground have less resources and less time to put into
11 things like privacy, security and so on, but still there
12 has to be some minimal standards there.

13 I was taking a look at a product a couple weeks
14 ago, a software product, and found lots and lots of
15 problems with it, and I was given the excuse, Well,
16 we're just getting off the ground here, but I don't
17 think that that -- that didn't make me feel good because
18 people were downloading this product. If it wasn't
19 ready to be shipped, then they shouldn't have put it up
20 on the web.

21 So there still has to be some standards, but at
22 the same time there has to be a balancing polling act,
23 and I think it's actually more with the size of the
24 company here. There might be different sets of rules on
25 a smaller organization versus a larger.

1 And then real quick on security, and it's one
2 that I made before a couple of meetings back is a lot of
3 smaller web sites are hosted by other companies, and
4 they're the ones that are really going to provide the
5 security, so I don't see security as necessarily a large
6 expense for any size web site.

7 MR. MEDINE: Thanks. Frank?

8 MR. TORRES: Just a couple points real fast.
9 It's interesting some of the analogies that were brought
10 up, the brakes in the airlines as far as safety goes.
11 You just kind of assume that they're safe, and the
12 reason you assume that some of these things are safe
13 without knowing the specific standards that go into
14 making an airline is the fact that the government is
15 involved. There's some safety. It's kind of that
16 that's fair safety, that the framework of safety that's
17 put into that.

18 To Rick's comment, there's -- states act because
19 there's a vacuum, and it's interesting that industry
20 folks are on up on Capitol Hill fighting federal law,
21 and at the same time they're complaining about states
22 acting because they'll be a patchwork of state laws.

23 With regard to self regulation, I take it
24 everybody's read the Business Week article. The vast
25 majority of people don't trust industry enough to do

1 that I think, and 57 percent of the people that they
2 surveyed said that government should be involved in some
3 way.

4 So I think we should move beyond the fact that
5 self regulation is necessarily viable in the long run,
6 and that's it.

7 MR. MEDINE: Thanks. Lance, did you want to
8 turn to some suggestions about where we go from here?

9 MR. LANCE HOFFMAN: I would. Thank you. Lance
10 Hoffman. I was concerned as was Deirdre and some other
11 folks, I talked to Stewart about this also, and so I
12 decided that at least I myself am a visual learner so
13 with the help of Deirdre put together a draft,
14 underline, draft process document, proposed process
15 document from how we get to where we are to where we may
16 wish to go.

17 MR. KIRKPATRICK: People down here, we were
18 short. We were shorted.

19 (Discussion off the record.)

20 MR. LANCE HOFFMAN: I have two.

21 MR. SCHUTZER: You can email it to us, right?

22 MR. MEDINE: We'll try to make copies right
23 away.

24 MR. LANCE HOFFMAN: Let me try to orally go
25 through it very quickly. The idea here would be to

1 have the subcommittees meet, however many subcommittees
2 there are, meet whether it's -- really electronically,
3 and then in essence I was using the model we did in the
4 security subcommittee of having a bunch of items and
5 pros and cons, and I was trying to lead people toward as
6 I said something other than mush so that if there were
7 things that everybody agreed on or almost everybody
8 agreed on, if you got above a certain threshold, maybe
9 it was two-thirds, maybe it was even more, I don't
10 really care, those winning pros and winning cons would
11 be, if you will, reported out to another level where a
12 delegate from the committee, a leader or whatever, would
13 go and somehow synthesize with the other committee or
14 committees, if you will, whatever consensus we could
15 reach, realizing as the chair has said all along that
16 we're not going to get consensus on everything by far.

17 But at least we would have some sort of floor to
18 report out. This is not to say that everything else
19 would not be recognized at all. Everything where there
20 wasn't effectively a super majority, however we define
21 that, would still be reported, and all the pros and cons
22 and everything would be written up and also produced in
23 the report.

24 However, they would be in the general discussion
25 section of the report. If you look at the document in

1 front of you on the very right-hand side, the right-hand
2 column, just to put something on the table, there's a
3 two-page executive summary, a ten-page synopsis, and
4 then the general discussion where everything would go,
5 especially the material that didn't make it into the
6 consensus material.

7 Then I think an important issue raised by Mary
8 and some others was research questions or tough problems
9 or whatever you want to call them, which there was
10 really no consensus on things on the horizon, there be a
11 section for that, and finally appendices, whether there
12 be constraint, size constraint, additional statements to
13 get into the Ron Plesser concern and those of some
14 others.

15 And I even being a professor for too long said
16 one to two pages times timely written, ball point one
17 inch margins.

18 MS. CULNAN: Could I add one thing? If this
19 matters to people that they all look the same, I suggest
20 that somebody, it could be Deirdre, make a template, put
21 it in Word, email it to everybody because again if it
22 doesn't matter, who cares, but if you want to have the
23 same title and the same format for names and addresses,
24 it's a real hassle for somebody to have to fix those
25 later, and it's not a big deal to make a template and

1 mail it out.

2 MR. LANCE HOFFMAN: The point is --

3 MR. WHAM: I nominate Mary for that.

4 MS. CULNAN: I can do that. I'll do it.

5 MR. MEDINE: You send it to the advisory
6 committee mailbox, we will distribute it.

7 MS. CULNAN: Sure.

8 MR. LANCE HOFFMAN: The point is, this process I
9 think if people go along with it, and I to put it on the
10 table and it's a draft, would allow us to get at a
11 report, which I think would put out consensus, put out
12 everything and put out future work.

13 Having said that, I suggest the Chair possibly
14 might want to recognize Stewart who had some other
15 comments to me in the hall about that.

16 MR. MEDINE: I would be happy to do so.

17 MR. BAKER: I think I have assumed that the
18 purpose of this was to lay out plausible options and
19 discarding plausible options and not to try to arrive at
20 a solution because in the end there is a wide variance
21 in views here, and therefore we're trying to produce a
22 document that is sort of a cookbook for somebody just
23 trying to decide, Well, what public policy am I going to
24 recommend or what public policy am I going to impose on
25 people when they fall into my clutches or whatever the

1 appropriate analogy is.

2 And I think we have -- we tried to do that in
3 the security area. We got a set of options that you can
4 pick one from column A and one from column B and then a
5 few issues that are sort of advice to somebody making
6 policy, think about this and we're not telling you what
7 to do, but think about these things before you decide
8 what you're going to do.

9 In the access area, we have divided up the
10 topics in ways that tended to overlap, and we haven't
11 produced as many clean option ranges, but I think that's
12 quite doable. There's probably four or five topics
13 where a range of options could be produced.

14 There are a whole bunch of options in some of
15 the papers that are sort of one shot options which I
16 think are more considerations as opposed to a set of
17 options, but if we could try to get those three working
18 groups to designate people or volunteer just enough
19 people so that we don't have to have a quorum so that
20 they could try to produce a document that has say four
21 option lists and some text around it, that would allow
22 us to produce something that is closer to a consistent
23 document.

24 I'm a little less than enthusiastic about sort of
25 super majority of voting to throw things out, although

1 that's a possibility.

2 MR. MEDINE: Can I suggest as an alternative to
3 the super majority approach which is sort of viewed as
4 the consensus approach, and that is if somebody has a
5 very strongly held view, that may be enough to get it
6 across to the threshold as well as sort of a larger
7 number of people having a view just to make sure that
8 again these -- the group was not defined to be
9 representative.

10 And so I think it would be unfortunate if
11 someone had a strong enough view, and you're all equal
12 members, if that weren't put across, and they didn't
13 feel as strongly and they were happy to put in a general
14 discussion, I think that would be fine.

15 But I propose that as an alternative.

16 MR. WHAM: If we get Stewart and Deirdre to
17 agree on it, is that a super majority?

18 MR. MEDINE: Total majority.

19 MR. PLESSER: That's a miracle.

20 MR. COLE: You just crystallized for me my
21 uneasiness, and it gets back to our conversation this
22 morning. If there's anybody who has a strongly held
23 view, it gets represented, not because they wrote a
24 separate point of view, but it gets into the body
25 because we want to get all respectable views.

1 So I hear that as saying if any option passes
2 some laugh test, there's some serious about it, it
3 should be represented, so the consequence of that is you
4 have options with pros and cons in this report that will
5 come out that it's possible that most people on the
6 committee disagree with, but it's not unreasonable.

7 There are pros and cons, and it's in the report,
8 and we create an advisory committee report that in my
9 view is highly susceptible to being misused and
10 misinterpreted.

11 MR. MEDINE: If I can respond and let others
12 respond. Again the goal here was to give the
13 Commission a range of options. If one of those options
14 may not garner a majority of the committee but may
15 ultimately garner a majority of the Commission, then
16 that's at least from our point of view what's most
17 important.

18 So I think there's a structure that's been
19 suggested in the appendices that would allow people to
20 express their views and that there may be an option
21 proposed that --

22 MR. COLE: I think you're completely misreading
23 the reality of how the media, the public and the
24 Congress and the FTC will use this. This will be a
25 report. This will be a very prestigious committee that

1 will have delivered the committee. It's called an
2 advisory committee so they're giving advice on things.

3 As a consequence of all that, there will be a
4 strong opportunity for misinterpreting that these long
5 ranges of options are actually considered by the
6 committee to all be viable options.

7 Now, they may be viable in the sense that the
8 Commission might like one or more of them, but they may
9 not be viable in terms of the opinions of the 40 people
10 on the committee who 35 of them may think that six 6 of
11 the options really ought to be off the table, and the
12 Commission would be making a mistake thinking about one
13 or more of them.

14 And I don't know how this format allows that to
15 get considered.

16 MR. MEDINE: Ron?

17 MR. PLESSER: I think that some of the documents
18 have gone very close to resolving that issue, and I
19 agree with Stewart a hundred percent, except to the very
20 end because I really think the idea of the super
21 majority really should be out.

22 I don't think -- I think that we should take a
23 really true issues and options with pros and cons
24 approach, identify the issues, identify the options, and
25 then under the options throw in the pros and cons which

1 then this would be impossible to do or whatever. You
2 could throw in pros and cons, Steve, and get in your
3 thing.

4 I would resist and even in the security area
5 where we probably could come to a super majority, I
6 think we did substantively come to a sense of kind of
7 where we are, but I still think that even in the
8 security area it should be issues and options, pros and
9 cons, because I think there's too many issues that
10 aren't going to fit into that pattern.

11 And if we use that pattern for some and not for
12 the others, I think we're making statements beyond what
13 we want to make, so if we can do this issues, options
14 and then each serious option has the pros and cons under
15 it, I think that's as close as we're going to get as a
16 format that's going to really be helpful to the
17 committee.

18 MR. COLE: Indulge me just for 30 seconds
19 because I don't think we're communicating well right
20 now.

21 Our subgroup has a list of pros -- a list of
22 options and pros and cons, a pretty long list. I think
23 it's a great paper that the drafters did, and I take no
24 credit for it, but there's one item -- I'll just pick
25 one out at random, actual cost fees, and the option is

1 companies should charge fees reflective of actual cost,
2 and there are pros and cons.

3 So let's say everybody in our group thinks those
4 are intelligent description of the pros and cons, and
5 there is a viable option that people think, but what if
6 the committee by some vote, majority, super majority,
7 unanimity, thinks that's a real big mistake, but it's
8 submitted to the Commission as a report, as a viable
9 option and the Commission never finds out that the
10 committee actually thinks it's a bone head idea?

11 Now, maybe this isn't -- I'm not necessarily
12 taking a position on this particular one, although I
13 have one.

14 MR. MEDINE: I appreciate that.

15 MR. COLE: And I took the example for a reason,
16 but the point I'm trying to make is if our conversation
17 is all about making sure the pros and cons are right,
18 we're missing the point why we got together I thought
19 which was try to find what is the viable direction the
20 business community and/or the --

21 MR. MEDINE: Let me just suggest that I don't
22 think it's a total dichotomy in the sense of the cons to
23 this particular -- articulate in your con description
24 that the Commission on reading it would use that was a
25 --

1 MR. COLE: It's a big burden on a 50-page
2 document.

3 MS. MULLIGAN: I want to second what Steve is
4 saying. I don't view my responsibility here as writing
5 a bench brief. I view my responsibility as writing an
6 opinion, and I think that for this particular meeting we
7 did an excellent job of writing a bench brief, Here are
8 all the options, here are pros and cons.

9 But if I hand over a document that doesn't give
10 the FTC any notion as to which ones of those I think are
11 better and worse, you'll see that we went to great
12 lengths to make sure that the pros and the cons were
13 equally weighted.

14 They each have six lines, seven sentences, and I
15 think you could see from the discussion around the table
16 that many of us have a strong opinion about which of
17 these are the best options, and I wouldn't want to
18 deprive the FTC of that advice.

19 So I think that there is a hybrid model where we
20 say here's the thing that really -- the majority of the
21 committee members felt were good, here's the two things
22 there was a breakdown on, maybe it's -- people who are
23 involved in the database industry feels like this,
24 people that are marketers feel like this -- who knows.
25 It's the privacy community. There may be two options in

1 many of them to garner the most interest.

2 However, we would like you to know we considered
3 these other eight options and here are the pros and cons
4 so you understand we did do our due diligence here but
5 we discarded these because we don't think the FTC really
6 -- we didn't know what we were doing. You asked our
7 advice. That wasn't really useful.

8 That happens sometimes, but I think there's a
9 hybrid and like Steve, I would feel very remiss in the
10 taxpayer dollars that have gone to support this lovely
11 event if I didn't provide advice.

12 MR. MEDINE: Lance?

13 MR. LANCE HOFFMAN: I'll make this brief because
14 I presented this the first time around, but I'm going to
15 give a technical interpretation. Deirdre did a very
16 good job of expressing what is my opinion here, I think
17 lawyers and technologists do the same thing.

18 This comes down to an issue between what I
19 gather is a bench brief, which I would consider mush
20 versus --

21 MS. MULLIGAN: Good explanation of all of the
22 issues.

23 MR. LANCE HOFFMAN: Thank you, but in the true
24 technical world, there's mush versus non mush and bench
25 brief versus opinions, and if we want to give the FTC

1 our expert opinion, as much as we can, I say we have to
2 vote for some process that delivers that and makes some
3 decision for full opportunity for people that disagree
4 to get into it and how will we do that?

5 MR. SCHUTZER: Some opposing briefs, minority
6 opinions in the appendix, but we're going to try to come
7 up with interpretations and judgments.

8 MR. MEDINE: Does that --

9 MS. CULNAN: As a committee, right.

10 MS. GAU: Within the sub committee.

11 MR. SCHUTZER: You don't want to have 40
12 different judgments.

13 MR. TORRES: It's up to us to explain to the
14 Commission and to the world, the media or whoever else,
15 the range of our opinions, and if we do our job and do
16 that, we'll prevent any misinterpretations from
17 happening. If the bulk of the committee thinks one
18 thing, then we say that up front, and kind of explain
19 that, so I concur with Deirdre's suggestion.

20 MR. MEDINE: Dan and then Ted?

21 MR. GEER: If I may, coming to a vote or however
22 you want to say it amongst these committees implies that
23 we are going to do a good job of convincing each other
24 that who they represent are wrong headed amyous, and I
25 still think the way to do this is to in fact lay out,

1 pardon me, the mush and have each of us then make
2 whatever crystalline condensate out of that we can.

3 The opinion is the best that I can do with the
4 data that I have in front of me. I think that the FTC
5 would gain more of what we are capable of doing if it
6 were to get that unalloyed by the process of us, each in
7 terms of other representation, coming to some compromise
8 which by its very nature throws away data.

9 MR. MEDINE: Stewart?

10 MR. BAKER: I have an unease about some ways in
11 which this process has been described, but it could be
12 that we're all struggling towards the same process.

13 I think that as soon as you start to say we're
14 going to arrive at recommendations, you are going to
15 create situations in which you're going -- well, it's
16 60/40 for this and the other people think the other one
17 is pretty good, how do you write that?

18 It's very hard to write that in a way that's
19 fair to all concerned. It's much easier to say, Here
20 are a range of options that represent the range of views
21 that were in the group, and to the extent that what
22 we're saying is no options survives unless it has a
23 defender who feels strongly about it, then that's easy.

24 We can say here's a range of defended options,
25 and then you can state the defenses and the oppositions

1 to them fairly clearly.

2 We did that in the security group. We threw out
3 a couple options and then said, Well, we're not going to
4 throw them out completely, but they don't belong as
5 separate options when you're thinking about doing that,
6 and we kind of stuck two options, mused options
7 together in this discussion here.

8 But I wouldn't want to throw out what we have
9 now as a range of options based on a vote, even if it
10 was 90/10 on one particular one, and so we shouldn't be
11 pushing people to do more than produce a range of
12 reasonable options but we certainly should encourage
13 people to throw out options.

14 MR. MEDINE: Richard?

15 MR. PURCELL: I disagree entirely. I think
16 it's time to advise the Commission what our beliefs
17 are. We have a strong commitment to protecting
18 privacy. We've gone through all of the options. When
19 you go to somebody and ask their advice, it's worthwhile
20 to go through all of the options and say, Well, on the
21 one hand there's this, on the other hand there's that.

22 But when it comes down to, Well, what's your
23 advice, you have to make some choices. If I were you,
24 this is the deal, this is the way we go. And I would
25 encourage, and I hope to encourage, the committee in

1 general that's the point we're at now.

2 We have the options in front of us, and now
3 we've been asked for our advice. How do you provide
4 that? You have to make some hard decisions. You have
5 to make some compromises. You have to incorporate all
6 of the options and evaluate them, and frankly despite
7 our -- despite people around this table we have to be
8 wise, and it's just going to have to happen. But it's
9 time for us to advise.

10 MR. MEDINE: Ron?

11 MR. PLESSER: I would modify I think my response
12 somewhat. I still think it needs to be not mush, but a
13 very clear, defined issues and options. I think
14 Stewart's idea that only defended options in is an
15 excellent one, and I think that Deirdre's suggestion is
16 probably a good one too.

17 At the end of each section you could put a kind
18 of summary of use paragraph which says -- almost like
19 what the FCC does when they look at comments which was
20 to say, Well, there's really -- we put this option 1 up
21 there but no one really much thinks that's a good idea.

22 Option 2 is favored by the consumer groups.
23 Option 3 tends to be favored by the industry groups and
24 then the merger, and then 4 has supports, some support
25 from a mix of people.

1 I think if we can try to be creative and work
2 with something like that, we can do it, but to go to
3 where I think my dear friend Professor Hoffman wants to
4 go is too far. I don't think it's doable. I don't
5 think you're going to wind up with anything but
6 generalities.

7 If you do that I think it's going to force
8 everything into just the highest plane principles
9 because I think that's the only way you're going to
10 really get agreement, and I think the value of the
11 Commission is to come up with a range of thought through
12 options.

13 And I think Deirdre's suggestion that there is
14 some of an editorial comment that there is some sense of
15 political support or for each of them is an appropriate
16 addition, but I would not want to take it to the next
17 step of forcing it to a real consensus. This is our
18 recommendation.

19 Richard, if we had a year we could do that.
20 We're not going to that in a month, and if we do it,
21 it's going to come up at such a high level that it's
22 going to be useless.

23 MR. MEDINE: I'm sorry, actually James had his
24 first and then Ted.

25 MR. WHAM: He's not as fast.

1 MR. ALLEN: James Allen. It strikes me -- I
2 think Ron's right, if we had a year we might arrive at
3 one set of recommendations but we don't have a year. We
4 have six weeks.

5 It strikes me that we could include all the
6 options that had any support, and we could rank them by
7 the order -- in order by the amount of support they had
8 and just count how many people supported an option, and
9 all of us would know that or assume that the FTC was
10 going to give more weight to the options that had more
11 supports so we would seek to arrive at options that had
12 more support and not be supporting an option that you
13 were the only supporter of.

14 MR. MEDINE: Ted.

15 MR. WHAM: Kicking off of Richard's comments,
16 there was a line from Henry -- Harry Truman, excuse me,
17 where he said what I really need is a one armed
18 economist, because they're always coming through and
19 saying on the one hand inflation could go up and on the
20 other hand inflation could go down.

21 Similarly, we need one arm advice here. We have
22 one set of advice, and I think it's unreasonable to
23 expect that we're going to have one set of advice.

24 But if I can take kind of reductio adocertum
25 (phonetic) here, if you look at the security options

1 that we talked about, the security team did just a
2 dynamite job of laying out seven opportunities. They
3 looked at two of them and they said, These are really
4 bad ideas, we're going to toss those out.

5 And then of the five that were remaining, we
6 talked about them here today, and I heard a lot of
7 consensus around the -- what I think named 2 Plesser,
8 right, it was the combination.

9 MS. GAU: 4 plus 2.

10 MR. PLESSER: I didn't work on that stuff.

11 MR. LANCE HOFFMAN: That's Washington for you.

12 MS. MULLIGAN: Stewart doesn't want
13 responsibility for it, Ron.

14 MR. WHAM: And Dan Jaye has left, but he did
15 weigh in with some comments about number 5, thinking it
16 was number 5, so in practice how I see a report on this
17 could happen is is that I don't want to take the options
18 say number 1 and number 3, which nobody really liked.

19 They're all reasonable none of us said they're
20 entirely bad ideas, but I don't even want those in the
21 main body of the document because once this document is
22 produced and we put our little signatures on it, we
23 submit it to the FTC, any sense of control that we have
24 is long gone and it becomes sound bites and it becomes
25 little fodder for people's specific agendas.

1 And it's just -- I want all of those things that
2 none of us agreed on, I don't want to go to the FTC and
3 say, Here's a reasonable option if none of us thought it
4 was a good idea. I want that sitting down in an
5 appendix some place and say, It's technically possible
6 but none of us thought it was a good idea.

7 Within the body you then say, The committee
8 identified two plausible alternatives for ensuring
9 security. The first one was number 4 plus 2 and it
10 looks like this. 35 of 40 committee members approved on
11 it. It was dominated by industry database
12 representatives and marketers.

13 On the alternative, a second less popular view
14 point was number 5, and five committee members approved
15 those, and it was dominated by consumer representatives
16 or whoever it was.

17 I think that does all of our responsibilities
18 of, A, not trying to strive for a consensus opinion,
19 which I think is foolish in this circumstance, B, coming
20 up with the meaningful recommendations that we think are
21 workable within the whole process and laying them out
22 and not creating the document that's mush.

23 Is that a readable document?

24 MR. MEDINE: Tom?

25 MR. WADLOW: Actually I was going to say

1 something else but something Ted said sparked a
2 thought. In fact, coming into this I was thinking that
3 in fact sort of a consensus opinion would be
4 interesting, but the more I think about it the more I'm
5 coming to agree with Dan but also with some flavor of
6 what Ted said, in that maybe the right answer here is to
7 come to a consensus on which of the options are crap and
8 which we should throw out but leave the general ones in
9 there, and then in fact go through and have each
10 committee member say, I would support this, this, this
11 and this of those options.

12 So what we have is the FTC has the options we
13 think are reasonable in general, the options that each
14 of us think are the best and the raw data. Somebody
15 talked about breaking down in terms of the database,
16 people like this and other. Well, give them the raw
17 data, here's the ones I supported, here's the ones you
18 supported, and then they can draw their own conclusions
19 from this.

20 MR. MEDINE: This seems to be somewhat of a
21 synthesis of what's going on. Do you have a quick
22 comment?

23 MR. PLESSER: Well, I just think if you look at
24 the security document, 1 and 3 are very helpful to have,
25 and it helps define the debate if you have 1, 2, 3 and

1 4, but if you don't have 1 and 3, then the question
2 Well, do they look at the statutes, do they look at
3 industry standards, and I think then the choice of going
4 to the combined 2 and 4 becomes much more meaningful and
5 at the end paragraph that we were talking about as
6 saying, The committee on the whole thinks that really
7 the way to solve this is 2 and 4, but 1 and 3 are
8 important steps.

9 You throw out the stuff that doesn't work or
10 that's not defended, but that's a good example. I think
11 if you just do 2 and 4 you really shunt the whole
12 process.

13 MR. WHAM: I'm not talking about not doing it.
14 I'm just saying throw it out of the main part of the
15 document that's going to get all the attention.

16 MR. PLESSER: I wouldn't agree with it. I don't
17 agree with that.

18 MR. LANCE HOFFMAN: I never proposed that. I
19 think Ron's on to something here. I never proposed
20 throwing out 1 and 3. I think Ron said it better than I
21 did in terms of get the good stuff up above the line,
22 define a fixed area, ten pages, I don't care what it is,
23 and the good stuff goes there, and you can say, In
24 arriving at this where most of the people thought these
25 were good ideas, we also looked at this and this and

1 this.

2 They're described more fully in the next
3 section, in the general discussion section, so nobody's
4 throwing it out. It's just not above the first ten
5 pages.

6 MR. MEDINE: Yes?

7 MR. ISAY: As someone who has just listened for
8 this entire day, I think the one thing that even Deirdre
9 and I can agree on is we don't want mush, and it seems
10 to me it would be so difficult for us to have any kind
11 of consensus that wouldn't be mush, as Ron said, that we
12 should move towards what I think is a very good goal of
13 this Commission -- committee which is to give choices
14 and give reasonable, logical pros and cons to those
15 choices.

16 I don't consider that at all a waste of taxpayer
17 money, and in fact I think it's one way to give very
18 good advice to the Commission, and I think that would be
19 a successful, and I think you can whittle down the
20 choices, but you give the choices that make sense, the
21 options that make sense and you do pros and cons.

22 That won't be mush. That will be good advice.

23 MR. MEDINE: I think we can spend the evening
24 discussing this, and I guess I think we need to come to
25 some closure on a process going forward.

1 I guess I'm still hearing, if I can try to
2 synthesize if possible -- I'm not sure we're going to
3 get unanimous agreement on this, but synthesize is that
4 it would be useful to the committee to identify certain
5 credible options and separate out options that are
6 either totally frivolous or are so deficient as to not
7 be credible to sort of stratify so that people -- but
8 avoid a situation where you necessarily have come to one
9 conclusion but you may come to two or three as was done
10 in the security area that people think are viable
11 credible options or may apply in some situations and not
12 others.

13 That would be sort of the main discussion, and
14 then you would discuss either options that you discarded
15 or options that are more problematic elsewhere in the
16 report and then come up with what I think would be a
17 very useful document to the Commission, which is to
18 identify a couple of viable options and support them.

19 So I guess I would propose if that is manageable
20 to try to do that. The security group I think can
21 essentially try to translate what they've got pretty
22 closely into that.

23 There are three access groups, and the question
24 is can they try to avoid some of the overlap and sort of
25 go to the core of each of their groups' discussion, and

1 then maybe identify one or two people from each of them
2 to kind of work as a drafting committee on the access
3 side to come up with an access report.

4 Again we have to be cautious. Legally we can't
5 constitute an access committee that's equal to a quorum
6 of this group because then it would have to meet in
7 public session, but the access committees can designate
8 one or -- one or two people into a drafting group to try
9 to accomplish those goals maybe after the committee --
10 subcommittees have met and reached the conclusions about
11 the options.

12 Is that --

13 MS. MULLIGAN: Can I add on that? The reason I
14 circulated the other document, the reason I was late was
15 I was trying to put together what Lance had asked for,
16 was just the access discussions -- each one of those
17 documents was really useful, but it was totally unclear
18 to me how we integrate them.

19 And so I tried to at least put one notion of how
20 could we just do an analytic approach. I'm not
21 suggesting that this is the right one, but I'm
22 suggesting people take this and maybe bang around
23 with it, and maybe each one of the access groups looks
24 at this and says, No, we think we should structure it
25 this way.

1 And then a designated person from each one of
2 those kind of sits down and looks and sees if there's a
3 way to actually get some consensus of approach because
4 right now I think we all found in the access groups
5 there was an enormous amount of duplication of work
6 among the different groups, and they're just -- they're
7 kind of circular because you're going and then all of a
8 sudden you hit someone else's issue and so you kind of
9 circle back.

10 And if we can figure out how to tie those
11 threads together I think that will help the report.

12 MR. BAKER: David, I have a procedural
13 question. It seems to me, although I shouldn't say
14 this, this system rewards the people who talk and
15 disrewards people.

16 MR. MEDINE: This is not a particularly
17 bashfully group.

18 MR. BAKER: Yeah, but if we're going to start
19 taking options and saying, This a defended option but it
20 doesn't have support from a large group, we can't do
21 that on the basis of non quorum meetings. We can't do
22 that on the basis of something other than a vote.

23 So at this stage at least we ought to try to get
24 the defended options from the groups that are sub
25 quoromed groups, and then we need a discussion or a vote

1 to say Okay, are there options on each of these that we
2 would elevate, and it's only then that we can say, Well,
3 here are the people that support it or don't support it
4 because other than that, you don't know. It's just the
5 luck of the draw who happens to be in that group.

6 MS. MULLIGAN: I second that. I think that's
7 reflected in Lance's process document too.

8 MR. MEDINE: Jonathan or Richard too?

9 MR. JONATHAN SMITH: I would like to make a
10 slight modification, just as a suggestion to the
11 structure that you've made here, Lance. I've seen a
12 format I think is very useful that's occasionally been
13 admitted by the National Research Council which is kind
14 of nice, which is a fairly extensive executive summary.

15 So in the executive summary, one could have a
16 set of recommendations, and it tends to be in my
17 experience most people who are really looking for sound
18 bites stop there, and that could be a set of
19 recommendations, and those might be things like we chose
20 the following suggestions for security.

21 And then in the body of the document, we do the
22 breakdown of the various access and security provisions,
23 and then anything that's really kind of detailed or a
24 major source of disagreement you could stuff off an
25 appendices, but the highlight of the document is the

1 executive summary.

2 MR. MEDINE: That seems consistent with what I
3 guess Lance has described as the synopsis.

4 MR. JONATHAN SMITH: What does the executive
5 summary in this document do that the synopsis doesn't?

6 MR. LANCE HOFFMAN: I was worried that the
7 executive summary which I insisted be no more than two
8 pages because that's all some people will read, it
9 couldn't do justice to the issues that got above the
10 line in the synopsis.

11 That's why I broke it out between an executive
12 summary, a synopsis and all these other things. I
13 understand your point. I was just a little -- I could
14 go either way, but I think it's better to have the
15 separate executive summary and then the synopsis and
16 then the general discussion. I thought otherwise you
17 could lose too much.

18 MR. MEDINE: Ron.

19 MR. PLESSER: Well, I don't like the approach.
20 I think it should be issues and options paper. When we
21 see what we got we can write an executive summary or
22 synopsis, but I think to put the synopsis first rather
23 than force through the kind of process that Stewart and
24 I and other are talking about I think is not helpful,
25 just leave that to the end.

1 When we get a document that has the issues and
2 options and the pros and cons, then I think it will be
3 fairly easy to put a synopsis and executive summary, but
4 I think that really has to be the emphasis. Otherwise
5 we're going to lose all the options as I think we
6 discussed, so I think we have a disagreement.

7 MR. MEDINE: Well, again I think we've exhausted
8 this subject, and I'm not sure we can come up with -- I
9 think we've come up with a sense you how the approach
10 ought to take place.

11 I don't think we can dictate a specific approach
other

12 than I think it's useful to have options that are
13 strongly held and well supported come through not
14 necessarily by super majority vote, and that ultimately
15 they are summarized in a summary or synopsis of some
16 sort, but have subcommittees at least as the initial cut
17 try to flesh out the options that are solid options that
18 the committee is comfortable recommending.

19 And I guess we'll be in touch with the
20 subcommittees if you need feedback on the process, but I
21 don't think we can really set forward more strict ground
22 rules at this point.

23 I would again -- we have recirculated a
24 calendar, and again I'm not sure we need a vote on this,
25 but I would again like at least the sense of the

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 committee that we will aim for drafts at the close of
2 business on the 19th.

3 And that's really again the product of these
4 subcommittees meeting and drafts of the committees and
5 so forth, drafting comments by the larger group, again
6 the importance of having wide input, by the close of
7 business on the 24th with a revised report to be
8 circulated on the 26th.

9 We will meet on the 28th again, and I think
10 given -- I would propose to make a motion at that time
11 on the 28th unless people want to make a motion now
12 authorizing email vote to finalize the report, but I
13 suppose we can also see how things develop on the 28th
14 and perhaps we'll have a clear consensus or even a
15 decision at that point.

16 And then if we need some additional time we
17 propose a period of discussion with a deadline of May 3
18 afterwards and final reports and so on, but I don't
19 think we necessarily need to address that until we get
20 to the 28th and see what the reports looks like.

21 So I realize it's not for certainty, but I would
22 propose that we proceed on roughly the discussion we
23 just had and adjourn unless anyone has any propelling
24 comments. Deirdre?

25 MS. MULLIGAN: It's a very short process

1 comment. I would propose that the access groups each
2 pick a person or I guess they could have two, right, six
3 people would be fine?

4 MR. MEDINE: Right.

5 MS. MULLIGAN: And plan to meet on Friday the
6 14th to see if we can work on having some kind of common
7 format or maybe Monday the 17th would be better actually
8 so if we could aim for Monday the 17th afternoon
9 meeting, two o'clock?

10 MR. KIRKPATRICK: General suggestion?

11 MS. MULLIGAN: At CDT?

12 MR. KIRKPATRICK: In Seattle?

13 MR. MEDINE: And also Ron I think and Richard
14 and Deirdre have agreed to be helpful to try to
15 coordination committee on some production issues as
16 well. And Mary's going to do a model, a separate
17 statement so that we can all share format.

18 Any other final comments? Again, thank you all
19 for again your hard work and commitment and diligence to
20 this process.

21 I think we'll have a fair amount of work to do
22 on the 28th so I propose we met again at eight a.m. to
23 four to accommodate our West Coast travelers. Thank
24 you.

25 (Time noted: 4:19 p.m.)

1 C E R T I F I C A T I O N O F R E P O R T E R

2

3 DOCKET/FILE NUMBER: P004807

4 CASE TITLE: ONLINE ACCESS AND SECURITY

5 HEARING DATE: MARCH 31, 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 SALLY J. BOWLING

16

17 DEBRA L. MAHEUX

18

19 C E R T I F I C A T I O N O F P R O O F R E A D E R

20

21 I HEREBY CERTIFY that I proofread the transcript
22 for accuracy in spelling, hyphenation, punctuation and
23 format.

24

25 SARA J. VANCE