

FEDERAL TRADE COMMISSION

BEHAVIORAL ADVERTISING
TRACKING, TARGETING & TECHNOLOGY

Friday, November 2, 2007

9:00 a.m. to 5:11 p.m.

United States Federal Trade Commission

Conference Center

601 New Jersey Avenue, N.W.

Washington, D.C.

Reported by: Linda D. Metcalf

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

TABLE OF CONTENTS

1

2 Page

3 Welcome and Introductory Remarks

4 Joel Winston, Associate Director, BCP.....3

5

6 Disclosure to Consumers.....9

7

8 YouTube Contest Presentation.....95

9

10 The Regulatory and Self-Regulatory Landscape.....133

11

12 Roundtable on the Future of Behavioral Advertising....203

13

14

15

16

17

18

19

20

21

22

23

24

25

P R O C E E D I N G S

- - - - -

WELCOME AND INTRODUCTORY REMARKS

MS. BRANDENBURG: Good morning. If you all could take your seats, we'll go ahead and get started. I would like to welcome you back to day two of the Behavioral Advertising Town Hall. Just a few reminders before we begin. When it's time for audience questions, we have two microphones set up in the aisles, and the moderators will indicate that it's the time for audience questions and you can come up, and, again, please be mindful of time so that everybody has an opportunity to ask their questions. If you would like to submit comments for the record, you may do so up until November 16th on the FTC website, www.ftc.gov.

We have a number of important housekeeping reminders. Security, if you leave the building at any time for lunch or to take a break, you'll need to be rescreened when you come back into the building. Please wear your name tags at all times, and if you should see anything suspicious, please, of course, report it to the guards.

Please turn off or set to vibrate your cell phones. You may use your cell phones outside of the conference center, but please refrain from using them

1 even in the foyer behind us. Fire exits are located
2 through the main doors at the front of the building on
3 New Jersey Avenue and through the pantry area to the G
4 Street corridor and out to G Street, which is directly
5 behind us. In the event of an emergency or drill,
6 proceed diagonally -- to the building diagonally across
7 Massachusetts Avenue.

8 Finally, I would like to thank Microsoft for
9 providing the coffee and bagels this morning. And now
10 without further delay, let me introduce Joel Winston, the
11 Associate Director for the Division of Privacy and
12 Identity Protection.

13 **(Applause)**

14 MR. WINSTON: Thank you, good morning to
15 everybody. I guess if the measure of a success of an
16 event like this is how many people show up the second
17 day, so this is great, nice crowd. And the real test
18 will be how many of you stay until the end, so we may be
19 locking the doors at some point just to make sure we have
20 a good crowd.

21 What I would like to do just in a few minutes
22 is kind of lay the groundwork for today's session, and I
23 think we got off to a great start yesterday. And it
24 really laid the ground work for what we're going to talk
25 about today. What we learned yesterday was what

1 behavioral marketing is, and of course we're going to
2 have our YouTube presentation later that will further
3 explore that.

4 We learned about who is using behavioral
5 marketing, how it works, what information companies
6 collect, how they use that information. So I think we
7 all have a better idea now what we're talking about.

8 We also heard about the benefits of behavioral
9 marketing, the fact that it enables consumers to get
10 content on the Internet for free. And the fact that it
11 delivers ads that are more relevant to people, less ad
12 clutter, and of course there's certain business
13 efficiencies that come from this practice.

14 At the same time we also heard about some of
15 the concerns that have been raised, the privacy concerns.
16 We heard about the lack of control that some consumers
17 may feel over their information. We heard about concerns
18 about the collection of sensitive information, medical
19 information and other sensitive information, how that
20 might be used.

21 We heard about anonymity, the issue of
22 anonymity. And there was a good discussion of what
23 anonymous means in this space, for example, is an IP
24 address anonymous or not, the debate on that. We heard
25 about some concerns about possible discrimination, that

1 targeted information could be used in some way to
2 discriminate against a vulnerable group such as children
3 and others, and also the overreaching of these vulnerable
4 groups. And, in particular, we heard about the social
5 networking sites and concerns about how information
6 collected through those sites could be used to target
7 teens.

8 We also heard about the possibility of data
9 breaches, that these compilations of information exist
10 and if they're not adequately secured there could be
11 significant harm to consumers. Interestingly, at least
12 what I heard yesterday was that consumers seem to be less
13 concerned about the advertising they're getting as a
14 result of behavioral targeting and more about the fact
15 that the information is being collected and stored.

16 So that may give us some ideas for how to
17 approach this problem in the future. So as is so often
18 the case in the law and in policy, the challenge is to
19 find the right balance. How do we preserve the benefits
20 that behavioral targeting brings to consumers and to
21 industry while protecting consumers from some of the
22 possible privacy concerns or abuses that might arise.

23 And if you don't mind me giving a shameless
24 plug for an upcoming workshop that we will be having in
25 December on the use of Social Security numbers in the

1 private sector, it presents really the same kind of
2 balancing test. Social Security numbers that are
3 collected have a lot of beneficial purposes for industry,
4 for government, for consumers. They allow the matching
5 of information and fraud prevention and lots of other
6 good uses.

7 At the same time, there's a potential for
8 abuse, there's a potential for identity theft. So,
9 again, the trick is finding the right balance. And
10 that's what we're going to focus on today. Today we're
11 going to talk about solutions in the future. We're going
12 to talk first about disclosures. Can they be made more
13 effective? Can consumers be empowered to control their
14 own information or do disclosures simply not work in this
15 space? Is this information that consumers simply can't
16 absorb, don't have the time or the will to really look at
17 and understand. And then of course the YouTube
18 presentation will be a good example of how to communicate
19 information, so I think that will be a lot of fun. We're
20 also going to talk about the regulatory environment and
21 what exists now, what self-regulation might be
22 appropriate here, what sort of government actions might
23 be appropriate.

24 And then finally we're going to close with a
25 roundtable on the future, where is this going and what

1 can we do to shape the future? And hopefully we won't be
2 hearing anything more about Larry Ponemon's mother.
3 That's sort of my goal for today.

4 Anyway, I think it will be a terrific session.
5 And hope you all stay and participate. Remember, this is
6 a town hall, we want everybody to get involved. Thanks.

7 **(Applause)**

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 **SESSION 6: DISCLOSURES TO CONSUMERS**

2 MS. ENGLE: Good morning, I'm Mary Engle, the
3 Associate Director for Advertising Practices at the FTC.
4 At this morning's session, we're first going to hear
5 three presentations, and then we'll have a roundtable
6 along the lines of the last panel yesterday. First this
7 morning we're going to hear from Lorrie Cranor, who is an
8 Associate Research Professor at Carnegie Mellon, then
9 we'll hear from Declan McCullagh with CNET, and finally
10 Scott Shipman from eBay. Lorrie?

11 MS. CRANOR: Good morning. I'm going to talk
12 with you really quickly about some of the research we're
13 doing at Carnegie Mellon that's related to disclosures to
14 consumers. We've all seen the studies that show that
15 people say they care a whole lot about privacy but they
16 don't always take steps to actually protect their
17 privacy. And there are all sorts of possible
18 explanations for this that have been tossed around.

19 The two that I want to focus on today are that,
20 A, they don't understand the privacy implications of
21 their behavior, so they don't realize that what they're
22 doing might have a privacy implication; and, B, the cost
23 of privacy protection is too high. And this includes the
24 cost of figuring out how to protect your privacy.

25 One of the problems is the privacy policies

1 themselves. They typically require college-level reading
2 skills to understand, and they also contain a lot of
3 language that includes legalese and obfuscated language.
4 There was a study that counted the number of hedging
5 claims in typical privacy policies. And these include
6 things like "except as", "on a limited basis", "we
7 reserve the right to". And a typical policy includes at
8 least 20 of these claims.

9 The students in my lab did a study this summer
10 to test a variety of privacy policy formats and find out
11 how effective they are with consumers. We started with
12 one real-life privacy policy from a real company, but we
13 removed the name of the company. And then we came up
14 with several variations on that format. We formulated a
15 highlights notice with the standard six boxes in it. We
16 also used the P3P computer-readable version of that
17 privacy policy to derive some other formats. These were
18 experimental formats we tested where basically you're
19 given some summary of the privacy policy and then you can
20 click on links to drill down and get more information.
21 We had 864 participants that came to us on the Internet.
22 Each were assigned to read just one of these policies.
23 We then asked them eight questions about how well they
24 thought they understood and trusted the policy. And then
25 we asked them to find six specific pieces of information

1 in the policy.

2 We found that when people read the original
3 natural language version of policy, there was some
4 information they could find very easily. This was the
5 information where they could just look for a keyword and
6 find the information. So, for example, we said "Does
7 Acme use cookies?" They could look for the word cookie,
8 and 98 percent of them correctly answered the question."

9 But when we asked a question that required more
10 comprehension, they had a lot more trouble. So, only 71
11 percent of people correctly answered the question, "Does
12 this policy allow Acme to put you on an email marketing
13 list?" And then an even more complicated question, only
14 half the people got right: "Does this policy allow Acme
15 to share your email with a marketing company that might
16 put you on their email marketing list?"

17 So our preliminary findings, and we're still
18 actually going through all the data that we have, our
19 preliminary findings are that even well written policies
20 are not well liked and they're difficult for consumers to
21 use. We also found that the layered notice variant in
22 the current format doesn't appear to help very much,
23 although we think some changes might be able to be made
24 to make that a lot better.

25 We also found that people perceived the long

1 policies as slightly more trustworthy but find
2 information faster in short policies, so we have a bit of
3 a contradiction there. The experimental formats that we
4 tested were not immediately intuitive to consumers. They
5 had trouble figuring out where exactly to find the
6 information in those policies. But based on these
7 findings, we plan further refinements and experiments,
8 and we think we can come up with something a lot better.

9 Another approach to privacy communication is to
10 provide privacy information in search results. We
11 developed a search engine called Privacy Finder which is
12 available to the public at privacyfinder.org. We
13 conducted a study this summer to determine whether people
14 actually could use the privacy information provided by
15 Privacy Finder and whether it influenced their purchases.

16 We did a lab study. We had 72 Pittsburgh
17 residents come to our lab, and we paid them to make
18 online purchases using their own credit cards and
19 exposing their own personal information. We paid them
20 all a fixed amount and allowed them to keep the change,
21 thus they had an incentive to try to save money.

22 So, this is what the Privacy Finder search
23 results looked like. You can see on the left column
24 there's a privacy meter, those little green boxes, and if
25 you click on the link underneath, that's a privacy

1 report, which provides a summary of the privacy policy.
2 On the right you can see the cost of each of the
3 products. And you can see that the one at the bottom,
4 which is at the site with the best privacy policy, you
5 would have to pay 69 cents more to buy that product.

6 We also tested a condition with irrelevant
7 information. It was exactly the same, except the privacy
8 meter was labeled "handicapped accessibility." And we
9 did this to test whether people were attracted to the
10 pretty green boxes or whether they were attracted to the
11 fact that it was related to privacy.

12 The third condition had no information down
13 that column. Our results were that when provided with no
14 information or irrelevant information most people just
15 made their purchase at the least expensive site, not a
16 surprise. The very interesting finding was that when we
17 provided privacy information a lot of people actually
18 paid more to make their purchase at the privacy-protected
19 website. And we think this is really an interesting
20 result, and it shows that accessible privacy information
21 can affect consumer behavior. Consumers may be willing
22 to pay for better privacy and Privacy Finder can help
23 users make privacy-informed decisions.

24 So, we have a lot of follow-up work planned to
25 drill down a bit more on this. But the high level bid

1 here is that if you can communicate clearly with
2 consumers about privacy, it does make a difference.
3 Thank you.

4 **(Applause)**

5 MS. ENGLE: Next we'll hear from Declan
6 McCullagh of CNET.

7 MR. MCCULLAGH: Hi, there. Good morning.
8 Thank you. So, news.com has done a series of privacy
9 surveys, including of search engines and
10 telecommunications providers and so on. And two of them
11 are relevant here, and that's what I wanted to mention.

12 The first we did in February 2006, and my
13 colleague, Eleanor Mills, helped with both. She's out in
14 San Francisco and covers the search industry. News
15 organizations tend to be more event-driven, and so the
16 first survey responded to privacy questions raised by the
17 Department of Justice's subpoena of Google. And you can
18 see the URL at the end of the presentation, if you want
19 to look at it yourself, but here are some highlights.

20 We asked all of the major search engines,
21 again, February 2006, this question. And Microsoft's
22 answer is representative of the rest. It's a little bit
23 more detailed, but basically all of them came back with a
24 very similar response and justification for storing of
25 this. Probably a more interesting question is this one:

1 If you have a list of search terms, can you then -- let's
2 say if the Department of Justice asked you, and let's
3 assume that a lawful procedure is followed here, produce
4 a list of people who search for that term. Al-Qaeda
5 might be an interesting one or something more detailed.
6 And, so here is -- the answers were all yes except AOL,
7 which was the outlier here, saying, no, we can't do it.

8 Here is another question, sort of the opposite
9 or the inverse of the previous one, which is given
10 someone's IP address or cookie value, let's say that you
11 already had that in a similar criminal context, can you
12 say what this person did?

13 The answers in this case were actually uniform.
14 All of them -- and of the four companies we surveyed said
15 that, yes, they could with no exceptions. Now, this is
16 one we did in August of this year. This came -- the
17 second survey was a result of some of the recent news
18 regarding improved privacy protections by search engines,
19 and so Eleanor and I wanted to sort of put this in a
20 clearer form to our readers and say, so, what exactly
21 does this mean. Some of the companies were using
22 different terms, and we wanted to explain to our readers
23 what was going on by asking them the same questions and
24 reproducing their answers verbatim.

25 What do you retain, how long do you retain it

1 for, do you completely delete it, or do you anonymize it?
2 We can call it sort of pseudo-anonymization. Some
3 companies don't fully anonymize; they instead just strip
4 off the last few bits of the IP address, and so the IP
5 address is narrowed to one in 256 or so addresses. How
6 do you anonymize? And then the last four dealt more with
7 behavioral targeting. Do you do it? Is there a way to
8 opt out? Do you use personally identifiable information?
9 And do you link other services that you provide like
10 instant messaging or email when trying to display a
11 search ads on the main search engine?

12 And, so here are the results. If you're
13 looking for -- I mean, what some folks, our readers,
14 wanted is how -- what's the most privacy-protective
15 search engine? And the answer is it depends. Ask.com
16 has its product which is not available yet, so let's skip
17 over that. So then if you look at the other ones, there
18 is -- do you care more about how long data is kept? Do
19 you care more anonymization? Do you care more about
20 behavioral targeting or not?

21 The only company besides Ask that did not
22 engage in behavioral targeting is Google. Some of them
23 had fine print in terms of whether or not you can opt out
24 of it or not. Microsoft said you can on third party
25 sites but not Microsoft's own site. But on the other

1 hand, Google was not as privacy protective as AOL and
2 Microsoft in terms of deleting versus anonymizing data.

3 So, the survey results of the August survey are
4 here at the tinyurl.com link. We're also doing a
5 follow-up one, but it was not quite ready in time for
6 this, and so expect it later this month.

7 One last thought, companies were far more
8 forthcoming this time around, the second survey in
9 August, compared to the first survey we did in early
10 2006. Also, if you look at some of the quotes, Google
11 said, "We keep data for as long as it is useful" in
12 February 2006, and they've changed their policy
13 substantially since then.

14 Microsoft gave us a very similar remark early
15 on, and so they both changed their policies and also it
16 just is easier to get information out of them. They seem
17 to know -- they seem to be more willing to talk about
18 privacy data retention than they were a year and a half
19 ago. Thank you.

20 **(Applause)**

21 MS. ENGLE: Finally we'll hear from Scott
22 Shipman with eBay.

23 MR. SHIPMAN: Thank you. Good morning. So I'm
24 struck a little bit by the first two presentations. The
25 first was I thought very informative on what consumers

1 are looking for and what they're finding, and certainly
2 the second on the search industry. What I'm going to
3 talk about is a little nuance from that in the sense that
4 on the first presentation we, as eBay, as a online
5 community, really try to aspire to those notice
6 principles and keeping it easy to read for customers, so
7 that component is certainly relevant for us as a company.

8 And on the second part with search and privacy
9 related to the retention of information, within the
10 search space, naturally eBay is a community and online
11 e-commerce platform, so our retention periods are
12 slightly different for a number of different reasons,
13 obviously fraud protection and others. But nonetheless
14 that does mean that we keep a large amount of data on our
15 customers related to the transactions and certainly have
16 a responsibility to make sure that we use that
17 information as the customer would expect.

18 And, so, disclosures to consumers for eBay is
19 not a new theory or even a new realm of work for us here
20 or my team. And as I think the environment can be
21 summarized, it's evolution, right? We've seen even back
22 in '97 and '98, privacy policies that were these long,
23 wordy, legal drafted statements. We've then moved to or
24 at least many communities, many online platforms have
25 moved to summaries, principles, charts, appendices. We

1 have seen P3P. eBay has rolled out detailed preferences,
2 and now when you look at the preferences, even at my own
3 admission, it's a very long page, so it's almost too many
4 choices. And, so, finding that balance has always been a
5 challenge. And what I'm here to talk about today is
6 another choice, another preference that we've worked hard
7 on and certainly the team has put countless hours into.
8 And that is a preference where we'll be linking, we are
9 linking with the team working through the weekend
10 actually to make sure it was up for the presentation
11 today.

12 We are linking to a choice from our
13 advertisements. And here's an example. Now, as it turns
14 out, what we're doing is we're testing placement and
15 we're testing labels because what we want to find out is
16 we want to find out from the customer what graphic, what
17 word, what option resonates best for them. And, so, over
18 the next few months and even as early as you can log onto
19 your computer today, you can go to the eBay website, and
20 as you travel throughout the Internet as well I'll
21 describe the differences in some of the ads.

22 You will see ads on eBay that will look similar
23 to this and they will have an advertisement label. Those
24 advertisement labels will also be accompanied by either a
25 parens that says "about." It may say "what's this?" And

1 if you're off eBay, you'll see a different type of banner
2 ad, an eBay ad, and that ad will say AdChoice, as an
3 example here. When you click on that link, our idea, our
4 notion, the concept is we want to provide you more
5 information about the ads and about the information
6 that's being used to serve you that ad.

7 Now, you may be an absolute guest, an unknown
8 to us. You may be in an identified state but not in an
9 authenticated state. If you're on eBay platform and
10 signed in, you're in an authenticated state. And so as
11 you move through those different identities as you relate
12 to us, we can use different pieces of information and/or
13 share information with advertisers anonymously so that
14 they can target an appropriate ad to you.

15 If you feel that that appropriateness, that
16 targeting, that customization isn't something for you,
17 you'd prefer to see a generic ad or you have the
18 creep-out factor, a la Minority Report, you have the
19 opportunity to learn more and an opportunity to express
20 your opinion and opt out. And, so, this is clearly a
21 notice and an opt-out procedure. And as you see here
22 from this example, this is a rough mock-up of a few weeks
23 ago of a popup, so when you click on that link it
24 immediately takes you to this popup that describes a
25 program and allows you to opt out.

1 If you were to go to your eBay preferences in
2 My eBay, so you're in an authenticated state, there is a
3 long list, but once you scroll down to general
4 preferences, advertising preferences, again you can see
5 that we provide a clear area for you to learn more and to
6 express your preferences. As you move into AdChoice,
7 again, you can see that there's two components. One is
8 whether or not we use the information on eBay to serve
9 ads to you; and the other is whether or not we share it
10 in an anonymized form so that ads off of the site can be
11 targeted to you.

12 So an example of an ad off the site would be an
13 eBay ad as I showed with the AdChoice slug. An example
14 of on eBay would be the large graphical with the
15 advertisement or the about slug. And I think one of the
16 great things about this, as even in this conference we've
17 seen, AOL has announced another technology solution for
18 this type of opting out and notice with behavioral
19 targeting. And I think that that's the crux of it right
20 there, right, we've got different technology solutions
21 for different types of communities, different types of
22 providers, search, e-commerce, and I'm excited to see
23 what the next technology innovation is going to bring.
24 Thank you.

25 **(Applause)**

1 MS. ENGLE: Thank you, Scott.

2 Okay. I'm just going to briefly go down and
3 introduce everybody who's sitting at the table, starting
4 at that end. Hopefully this is right, from the notes I
5 have, because I can't see down there. We should have
6 Jane Horvath, Google Senior Privacy Counsel; and George
7 Pappachen, Director of Privacy SafeCount, which is an
8 online survey company; then Zulfikar Ramzan, who is
9 Senior Security Researcher at Symantec; Ken McGraw, who
10 is Executive Vice President at Zango, an adware company;
11 Professor Carlos Jensen from Oregon State University. I
12 guess that's the Badgers, we learned yesterday.

13 PROF. JENSEN: No, the Beavers.

14 MS. ENGLE: Oh, Beaver, sorry. Not much of a
15 sports fan here. And Scott Shipman from eBay; and Esther
16 Dyson from EDventure; of course Joel Winston; myself; and
17 Marty Abrams for the Center for Information Policy
18 Leadership at Hunton & Williams; Lorrie Cranor, again
19 from Carnegie Mellon; Declan McCullagh from CNET; Peter
20 Cullen, who is a General Manager at Microsoft; Srinija
21 Srinivasan, Editor-in-Chief at Yahoo!; and George Milne,
22 who is a Professor of Marketing at University of Mass.-
23 Amherst; then Colin O'Malley, who is Director of
24 Strategic Business at TRUSTe; and, finally, Michael
25 Cassidy, who is President of Undertone Networks, an

1 online ad network.

2 MR. WINSTON: Well, I'll get the ball rolling
3 and I'll ask some questions and Mary will ask questions,
4 and some of them will be directed at particular
5 individuals, others we can just open up the floor, too,
6 but anybody who wants to chime in should feel free to
7 chime in.

8 First I want to reassure everyone there will be
9 no homework, no final exams.

10 MS. ENGLE: No grades.

11 MR. WINSTON: No grades. We will have
12 pass/fail, so you do at least have to pass, but otherwise
13 we'll make this easy for you. I think the ultimate goal
14 is for us to try to get a handle on whether disclosures
15 work when it comes to behavioral targeting. We heard a
16 lot yesterday about how consumers don't read privacy
17 policies, they don't understand them when they do read
18 them, they're bombarded with a lot of information, maybe
19 more information than they want. You've got sort of a
20 wear-out factor that you have to be concerned about.

21 So the question is, how do you make disclosures
22 effective, can you make disclosures effective and what
23 works and what doesn't work? And I think we want to hear
24 from everyone about what their businesses use and what
25 they think works and doesn't work.

1 But I was wondering if we could start back with
2 Scott. Could you put your slides back up? Would you
3 mind?

4 MR. SHIPMAN: Sure.

5 MR. WINSTON: Ok, if you'll go to the slide
6 with the ad for the CRV.

7 MR. SHIPMAN: Yep.

8 MR. WINSTON: Do I understand this right that
9 in order to get that message "Why did I get this ad?" you
10 have to either click on or put your cursor over the
11 question mark; is that right?

12 MR. SHIPMAN: Yeah, that's correct, so in some
13 implementations as I explained, we have got some
14 different tests. Some include a mouse-over. In this
15 particular instance with the question mark we've actually
16 decided not to go with the question mark logo. It didn't
17 have enough to it, so the embodiments that we're using
18 right now are either an advertisement with a paren,
19 (about), or advertisement with a paren, (what's this), or
20 advertisement with a paren, (AdChoice). And, naturally,
21 AdChoice being unique doesn't necessarily have a lot of
22 meaning, yet we hope events such as this and discussions
23 with our community members will increase that as an
24 opportunity.

25 MR. WINSTON: Yeah, and I guess that does

1 address what I was wondering, and that is how do you
2 motivate people to search further? How much information
3 do you have to give consumers about what it is they
4 should inquire about before they'll inquire? Is a
5 question mark good enough? Is the word advertisement
6 good enough? You know, some of these may or may not
7 motivate consumers to actually take the next step. What
8 do you think about that?

9 MR. SHIPMAN: Yeah, and I think one of our --
10 one of our key objectives is to make the program known
11 and to make the option known. So that's why we're using
12 different embodiments, because you just don't know yet
13 what they want.

14 MR. WINSTON: Right. I'm wondering whether
15 some of the other businesses alert consumers to the
16 availability of information on their sites about how
17 advertising may be targeted to them other than through
18 the link at the bottom of the page to privacy policy.

19 Peter Cullen, do you want to start with that?
20 How does Microsoft do that?

21 MR. CULLEN: We've explored different ways of
22 providing advice, providing notice to our customers. And
23 it really -- it's a balance between how do you provide
24 relevant advice in situations that might be very
25 contextual versus, to be really blunt about it,

1 overburdening the consumers.

2 So, let me think about an example of
3 overburdening the consumer. So, in some parts of the
4 world, as we heard yesterday, an IP address is considered
5 personal information, so think about a scenario where you
6 went to get a weather forecast off of MSN.com and there
7 was a popup notice that said that here's how we collect,
8 use your IP address. And I think most consumers would
9 say, hey, look, all I want is the weather.

10 So that may be an example of kind of
11 overnotice. The way that we've approached it is in
12 certain situations, for example, the phishing filter
13 where there's a sensitivity between providing Microsoft
14 perhaps with URLs as well as providing the protection we
15 do, kind of a very just-in-time consent notice. For
16 other less invasive types of things, for example, use of
17 behavioral information to provide ads or even contextual
18 information, that's an example where we would have very
19 detailed information in a privacy notice and provide the
20 consumer with the ability to opt out of that tracking,
21 despite Declan's information, that's not quite accurate,
22 you can actually opt out of off-network and on network.

23 MR. MCCULLAGH: That's what you told us at the
24 time.

25 MR. CULLEN: Sure the other -- so there's

1 different notices for different scenarios. And it's a
2 balance between providing access to the information,
3 providing relevant information in the context that from
4 our understanding of our customers that they expect.

5 MR. WINSTON: Yeah, I think that's a good
6 point, that there has to be a balance between too much
7 information and not enough. But if you think about
8 effective communication, the first step is getting the
9 consumers' attention, letting them know there is
10 information there that they might be interested in. And
11 then you move to, all right, once the consumer is
12 interested how do you explain it in a way that they can
13 understand and what choices do you give them at that
14 point.

15 MR. CULLEN: Yeah, so, you know, another
16 interesting balance point is that for a user that first
17 comes to Windows Live, applies for a Windows Live ID,
18 they actually have to affirmatively attest they have read
19 or received the privacy notice. Now, do we make sure
20 that they have to scroll through even the short form
21 notice? No, because in all honesty that's -- our
22 customers have said that's just kind of an overdoing it.

23 Do we make it accessible on every page?
24 Absolutely. Do they have the ability to express some
25 choice around that? Absolutely. So it's a balance

1 between making the information available, doing it in a
2 way that makes it easily accessible, in fact, invites
3 accessibility but doesn't make the consumer have to click
4 through 18 screens just simply to sign up for an ID.

5 MR. WINSTON: Esther, you wanted to say
6 something?

7 MS. DYSON: Yeah, thanks. I wanted first to
8 talk about the disclosure of my own information in the
9 bio here. It's kind of ironic. If you look at my bio,
10 it's kind of vague. I do emerging stuff. The fact is
11 I'm very involved with a bunch of companies that do
12 online advertising. Somebody -- some I'm sure junior
13 person at the FTC wanted to make my bio sound more
14 prestigious or something, and they took out all these
15 dinky little companies, but just for the record, I'm
16 involved with Boxbe, which lets you manage your own email
17 inbox and sell access to it to marketers, so it tries to
18 empower the user.

19 I'm involved with Dotomi, which originally
20 started with a similar user empowerment kind of business
21 model where you get personal messages in a banner space
22 on your website. We found that too confusing to sell to
23 consumers. So I understand exactly what the issues are
24 around trying to tell people stuff they don't really want
25 to take the time to understand.

1 I'm on the board of WPP Group, which owns three
2 of the world's largest advertising agencies. I'm an
3 investor of Link Storm and a few more. But just -- I
4 wanted to get that out there to make the context clear
5 and also just to illustrate how disclosure itself is
6 difficult even if you're well meaning.

7 The point I wanted to make here is to try and
8 move the discussion from what we're doing now towards
9 what I would call Disclosure 2.0. And you see a little
10 bit of it with eBay. It's so why are you showing me this
11 ad? What is it that you know that makes you want to send
12 me this ad?

13 I think over the next few years, the most
14 effective disclosures are really going to be tell the
15 consumer what you know about the consumer. If you know
16 their IP address, show them their IP address. If you
17 know their name and email address, show them their name
18 and email address. Of course it's not as simple as it
19 sounds, because you may combine all this information to
20 do segmentation. You may have very clever names like
21 Baby and Bath, or, you know, who knows. You may have
22 third party information. But if you're a marketer and
23 you can figure out how to sell this stuff to advertisers,
24 you should be able to figure out how to present it to
25 consumers in a way that they can understand, because most

1 consumers are probably as smart as most advertisers,
2 generically.

3 So I think you're going to see more and more of
4 this happening. I don't think the FTC needs to set
5 standards. Unlike, for example, you can see your credit
6 report now. It's a very defined process, exactly what is
7 shown and so forth, and it's free, and part of the issue
8 is around funding this, but I think the market is
9 beginning to work. I think you're going to hear more and
10 more today about examples of this kind of thing.

11 The second thing that gives me hope, and I'm
12 going to be very brief, is Facebook. People are now
13 becoming accustomed to developing, designing, looking at,
14 maintaining, refining, if you like, curating their own
15 profiles. It's no longer such a weird notion. If I
16 curate my profile to show to my friends, and if I decide
17 which of my friends can see which part of my profile, why
18 can't I simply have a list of marketers for whom I'd do
19 the same curating? This is what these guys can see; this
20 is what those guys can see; this is what's visible to
21 everybody. If you had tried to do this 10 years ago,
22 people would have said I don't understand, it's too
23 confusing. But I think the courtesy of Facebook and
24 other companies, this notion is now going to be
25 completely comprehensible to consumers so that Lorrie's

1 problem of they don't understand is going to be solved
2 not by a single standard but by consumers' greater
3 familiarity with all these tools.

4 MR. WINSTON: Thank you, Esther.

5 Just to pursue a little bit more how companies
6 are getting over this barrier of getting consumers'
7 attention and alerting them to this -- the availability
8 of this information, Srinija, am I pronouncing that
9 right?

10 MS. SRINIVASAN: Yeah, that was perfect.

11 MR. WINSTON: Wow! How do you do that at
12 Yahoo!? How do you tell consumers that you're gathering
13 this information for advertising purposes, and explain
14 how that works.

15 MS. SRINIVASAN: Sure. So, I'm Srinija, I'm
16 Editor-in-Chief at Yahoo!, and I've been with Yahoo!
17 since we were five people, and I can tell you since our
18 inception that we got into this because we were so and
19 remain so passionate about the transformative power of
20 this medium that we can't wait to unleash that positive
21 power for others and empower others to find out and
22 discover what can be done, what's possible.

23 And we recognize that in order for that to
24 happen there has to be a fundamental trust by all
25 members, all participants in the ecosystem that drives

1 this medium in order to drive participation. So we were
2 one of the first companies to have a privacy policy, and
3 I don't want to for a second discount the power of that
4 level of disclosure.

5 The policy itself, the final document, is an
6 important outcome. And in it I think you'll find on the
7 very top page where we try to succinctly boil down the
8 essence of our information practices, you'll see that we
9 very clearly say, we use the information we observe in
10 order to customize the content and ads you see.

11 We further break down -- you know, we have been
12 talking a lot about layered policies in the last day or
13 two. Our version of layering has been in place for many
14 years. And that is that many different Yahoo! customers,
15 consumers, think of us in different ways because we offer
16 so many different sorts of products and services. So we
17 actually detail for each of our products and services
18 what are the privacy practices that apply to this
19 particular product? That way you don't have to read
20 about the tons or more of specific instances that may or
21 may not pertain to you, but you can see in a central
22 policy what are the principles that apply. And then the
23 practice is broken out by product.

24 So that's one way just in our policy statement
25 that we make sure we have ubiquitous links to this on the

1 footer of every page, not just the home page, and that we
2 want people to know this is -- we take this seriously.
3 This is something that we think about.

4 The other thing is that has been quickly
5 alluded to here, I think, but bears further discussion is
6 that the policy itself, while it's very important, is the
7 outcome of the thoughtful process that led to it that
8 says we're a company that spends time thinking about the
9 implications and the outcomes. And these are our
10 guardrails.

11 We want to make that clear in as many ways as
12 we can. So, if you're traversing across Yahoo!, we have,
13 for example, a universal header. When you are known to
14 us, it will say, "Hi, Srinija." If you are not known to
15 us, because you've never registered with us or you aren't
16 logged in, then there won't be that identifiable
17 greeting. And that's just one small example of letting
18 you know implicitly in the experience something that
19 pertains to what we know about you.

20 MR. WINSTON: Let me just follow up for a
21 second. The way consumers get to the privacy -- this is
22 all in the privacy policy, right?

23 MS. SRINIVASAN: Of course the elements of the
24 policy are all in the privacy policy.

25 MR. WINSTON: Right.

1 MS. SRINIVASAN: Something like a universal
2 header is just one example of where we want to give you
3 cues implicitly in your experience that tell you in that
4 particular example are you logged in, have you
5 registered, and are you logged in, are you known to us?

6 MR. WINSTON: Right, but if I'm a consumer and
7 I'm traversing the site, the way I would find out that
8 you collect this tracking information and target ads to
9 me is by clicking on the privacy policy?

10 MS. SRINIVASAN: That's right.

11 MR. WINSTON: Okay.

12 MS. SRINIVASAN: And we think that customers
13 are aware of this value exchange. You know, we make it
14 very clear that you know when you're dealing with Yahoo!,
15 you see the Yahoo! brand, or you're on our brand and
16 network of sites. And we think people understand this is
17 the value exchange, and then we spell that out very
18 clearly to say we use this information to customize the
19 content in ads that you see.

20 MR. WINSTON: Okay, and do you have any data,
21 and if anyone else has any data, on how many of your
22 visitors, you know, what percentage of your visitors
23 actually click on the privacy policy? Do you have any --

24 MS. SRINIVASAN: I don't know the specifics of
25 the usage. It's read, but, again, I want to underscore

1 just because I think there's been a lot of varying
2 opinions expressed about the value, the relative value of
3 privacy policies. I strongly believe that the presence
4 of a privacy policy and the pervasiveness of these
5 policies in the industry is a really powerful
6 demonstration.

7 You know, the fact that we've got the leading
8 companies in the industry here in this dialogue and that
9 we're demonstrating good practices, I think, underscores
10 that the fabric of this medium, the fabric of this
11 marketplace, gives us all an incentive to ensure that we
12 have that kind of trusted relationship with our
13 consumers. So, the extent to which people are reading
14 every word is one indicator, but also I think the
15 presence of the policy can't be underestimated.

16 MR. WINSTON: Okay. Carlos, do you want to
17 comment?

18 MR. JENSEN: So, we in academia have been
19 trying to get figures on how many people actually read
20 privacy policies for a long time in a real world setting.
21 And it's one of these very closely guarded secrets. And
22 the best that we've been able to get is kind of off-the-
23 record statistics showing that when you prompt people for
24 a credit card, less than 1 percent will read your privacy
25 policy. And you can only imagine what the acceptance

1 rates are going to be for regular transactions like
2 search. I mean, Google doesn't even have a link to the
3 privacy policy off of the main search page. You have to
4 drill down.

5 The problem with the traditional privacy policy
6 in this space especially is that I'm not dealing with a
7 single transaction. I'm dealing with a prolonged
8 transaction over days, weeks, months, and the information
9 accumulates. So whether users are really aware of the
10 implications of their transactions with this company
11 after reading the policy one time at the beginning of the
12 relationship is unclear to me.

13 I really liked what we saw here from eBay,
14 which is a kind of constant reminder that we are aware of
15 who you are, we are aware of oh, you should be aware that
16 we're doing something with information that we're
17 gathering about you. And I think that's a much more
18 powerful direction to go in.

19 MR. WINSTON: Jane Horvath from Google, do you
20 collect any statistics on how many people click on the
21 privacy policy?

22 MS. HORVATH: I don't have those available
23 right now. But I did want to talk about what we've done
24 because we do agree that the privacy policy tends to be
25 very legal oriented and difficult to read and difficult

1 to follow, so we're exploring different means of making
2 our privacy practices clear. In particular, we first
3 started with blogs. And we were blogging about different
4 issues with respect to privacy, and these blogs are
5 interactive blogs, so users have the ability to write
6 back and ask questions.

7 And in response to a number of the questions we
8 realized that there were some issues with respect to
9 search and what information we were collecting. So we
10 decided that we would use another vehicle, which is
11 video, because our YouTube product is very popular and
12 people like to see things, like to watch TV. So we have
13 recently launched two videos that explain some of our
14 privacy practices. And we plan to launch more videos as
15 well.

16 And just the other day we launched a new
17 channel on YouTube, which is our privacy channel, where
18 we're hoping to aggregate as much information about our
19 privacy practices as possible.

20 We also believe that we have increased notice
21 where there's more actionable PII, in particular with
22 respect to the tool bar, the Google tool bar where you
23 can turn on a feature that we believe is collecting more
24 personal information. We will actually query you with an
25 opt-in in plain English that says this is what's

1 happening to you, do you want to proceed? And you can
2 opt-in from there.

3 And then finally, similar to eBay, we are
4 actually testing an advertisement with an ad policy link
5 on it in connection with our third party ad serving
6 product for display ads.

7 MR. WINSTON: And just to clarify, right now
8 we're talking about how do you get consumers to pay
9 attention to the fact that there's information here that
10 they might want and what are the best techniques for
11 drawing consumers' attention to this issue? I think
12 later we'll want to talk more about the content of the
13 disclosure, how do you actually effectively communicate
14 that information when the consumer reads it. Mary?

15 MS. ENGLE: Well, I was wondering if anybody
16 wanted to comment. I mean, we heard yesterday that
17 consumers don't really read privacy policies very much
18 and perhaps also that the mere presence of a privacy
19 policy suggests that the privacy is being protected more
20 than it actually is. If you actually read the privacy
21 policy you would see that they're going to be sharing
22 with affiliates or so forth.

23 So I don't know if Srinija or somebody else
24 wants to talk about it, is there some other way or
25 particularly with respect to the ads that you could

1 present this information to let -- you know, other than
2 having to rely on consumers to just -- well, they see
3 privacy policy, so I guess, you know, I'm safe here or
4 I'm covered.

5 MS. SRINIVASAN: So, as it relates to the ads,
6 we -- so for Yahoo!, we're very new to the space of
7 delivering ads off of our branded network. In fact,
8 while we have announced some acquisitions in this area
9 and, you know, we'll certainly want to deepen those
10 relationships over time, the one instance where we employ
11 behavioral targeting in advertising off of our own
12 branded network is with eBay. And you've heard from
13 Scott about the AdChoice model.

14 So in our first instance, this is a model that
15 we're really happy to participate together with eBay on
16 because it provides immediate contextual notice within
17 the context of that activity to say that near that ad
18 unit or perhaps in the ad unit a user can see there's
19 something here, there's something I might be interested
20 in regarding how this ad is delivered.

21 And from there, you can get directly to not
22 just their opt-out but also our opt-out, even though the
23 behavioral targeting off our network is anonymous, you
24 can opt out of that as well. So associated with ads,
25 that is our first foray, and that's the model that we've

1 chosen to adopt.

2 We, like eBay, are looking forward to
3 continuing to experiment and explore any models. I mean,
4 it's absolutely in our interest to promote the greatest
5 transparency and control for users because, again, it
6 comes back to just our original purpose. We want to
7 unleash the amazing power of this medium. That requires
8 participation; participation requires trust.

9 MS. ENGLE: Marty?

10 MR. ABRAMS: Thank you. I think there's some
11 assumptions that are inherent in the discussion so far,
12 and I think we need to at least acknowledge those
13 assumptions and explore them. The question is, what can
14 I do -- you know, your framing question is what can I do
15 to force consumers to read privacy notices? And the
16 honest answer is that individuals are incredibly busy,
17 individuals have lots of things in their lives that are
18 very important to them. Individuals want a market that
19 they can trust. Individuals go to brands because they
20 recognize the brands and they recognize that those brands
21 have reputational risk which makes those organizations
22 more willing to be innovative and try things.

23 If we're saying that we can come up -- we've
24 tried many devices on the Internet to force people to
25 read things. We darken the screen, we put popups, we

1 make people click through things, and the fact is that
2 we're never going to get rid of the fact that individuals
3 are incredibly busy, that individuals have lots of things
4 to do in their lives, that individuals want a great
5 experience when they go on the Internet, and there are
6 lots of things that are bundled into that.

7 So when we think about privacy notices, I think
8 we have to think in terms of the roles of privacy
9 notices, and it's not -- so it's not just consumers are
10 aware of what's going on so they can make choices.
11 Privacy notices establish a sense of what is fair and
12 what's unfair by the comparison of notices, the
13 comparison of behavior.

14 Privacy notices create a sense of
15 accountability that they define how an organization is
16 going to behave and then organizations can be measured
17 against that behavior. And that's a very different thing
18 than just saying we're going to try to force individuals
19 to read notices so that the consumer can then be in a
20 position to police the market.

21 And then when we think about this whole concept
22 of the role of notices, I think we need to think about
23 the concept of privacy as it relates to the role of the
24 Federal Trade Commission, because we're at the Federal
25 Trade Commission. And over time the Federal Trade

1 Commission is really in many ways because of the adoption
2 of the concepts of harm and protection against harm which
3 is appropriate for a consumer protection agency, it's
4 really come down to a discussion of what is the
5 appropriate uses of information.

6 And the appropriate uses of information,
7 actually when we talk about communication, goes beyond
8 just the role of notices as a privacy notice but also the
9 concepts of the uses of information that are in terms and
10 conditions, especially as you get away from branded
11 organizations. So I'm just suggesting that while privacy
12 notices are incredibly important, my God, I have spent 20
13 years working on privacy notices, I led the process of
14 coming up with the multi-layered notice approach, we
15 don't -- we shouldn't have an expectation that notices
16 alone are the issue and that we shouldn't spend all of
17 our time trying to figure out how we force consumers to
18 read notices. We have to think about the accountability
19 process that goes into a notice.

20 MR. WINSTON: I think that's right, Marty,
21 although I think this panel really we want to drill down
22 on how do we get consumers to look at this information
23 and understand it and make good choices for them,
24 recognizing that privacy policies serve a lot of other
25 purposes.

1 Peter?

2 MR. CULLEN: With respect to that, I do think
3 we do need to pick a little bit on Marty's points a
4 little bit. So, for example, the state yesterday, which
5 I was incredibly surprised about, you had 15 percent of
6 the whatever it was that Fortune 500 companies don't even
7 have a privacy statement, so I think it's wonderful that
8 we're up here discussing about how we can improve privacy
9 notices. Perhaps the goal is to get people to read them.

10 But Marty's point about that an organization's
11 privacy statement is also a promise to consumer advocates
12 who frequently look at those statements to make sure that
13 they're not deceptive, it's a promise to the FTC, after
14 all, we have a 20-year love affair with you on that.

15 **(Laughter)**

16 MR. CULLEN: So, I think they serve a very
17 valuable purpose, but I think we also need to be thinking
18 about, well, why is it that 15 percent of those top
19 companies do not even have a privacy statement? What
20 does it mean for the perhaps less respectful companies in
21 terms of what their promise is. So, you know, it's a
22 fascinating debate that we have some very, very large
23 brands up here and we're talking about whether our
24 notices are effective when we have a bunch of perhaps
25 questionable actors out there that aren't perhaps even

1 have the confidence to put a statement up.

2 MR. ABRAMS: When Bonnie Guiton was head of the
3 Office of Consumer Affairs when we had still had an
4 Office of Consumer Affairs in the United States, Bonnie
5 Guiton used to talk about the concept of the teachable
6 moment. In many ways the reason the privacy notices have
7 to be approachable is that when you're at that teachable
8 moment, when there's a motivation for the consumer to
9 read it or the consumer or the privacy advocate to read
10 it, that there's the ability to come to grips with that
11 notice and to drill down in a meaningful way in the parts
12 of notice that are important.

13 So, this concept of -- we shouldn't lose sight
14 of the fact that why did she come up with this concept of
15 the teachable moment? Because she realized that you
16 can't force someone to do something that they don't have
17 time to do today, and that notices are incredibly
18 important and they need to be incredibly useful, but it's
19 not the fault of consumers if they don't read them and
20 it's not necessarily the fault of organizations if they
21 can't get them to read it. That's the point, Joel.

22 MR. WINSTON: Let me just ask this question and
23 throw it open to anybody. At the risk of being
24 completely over-simplistic, why is it that a site that is
25 engaged in behavioral marketing, why can't they put a

1 notice on the home page, wherever, that says we collect
2 information about your activity on this site and use it
3 to direct ads to you that may be most relevant to you.
4 To learn more about this and to understand what your
5 choices are, click here. And then you go to a statement
6 that explains all this. Is that -- is anybody doing
7 that? Is that feasible? Would that be effective?

8 MS. DYSON: I mean, frankly, that's what the
9 question marks and learn more and all those other things
10 are for. If you're a guy designing a website or a web
11 page, every single square inch of this real estate is
12 very valuable. You want to know how it's used, how it's
13 monetized, what it's for, and spending a lot of space on
14 this kind of thing is very hard to do if you're a
15 marketer, so they use these little things. If you want
16 to learn more, you can click on the learn more.

17 And I think -- you know, I don't think you can
18 force consumers to look at this stuff. I don't think
19 it's somebody's fault. It's just something, if they want
20 to know you want to be able to help them learn more. I
21 wanted to point out that Google has something called web
22 history, which is not positioned as a privacy statement,
23 but is exactly this kind of thing. Learn more about what
24 Google has been tracking of your activities online.

25 And, again, I think the level of ambient

1 knowledge is getting to the point where people know what
2 the question marks and the "learn more" or "find out
3 more" links mean. And if they're interested, they do
4 click. The problem is indeed with what they find when
5 they click, which is mostly incomprehensible.

6 MR. WINSTON: Just one quick response to that.
7 Several years ago the FTC undertook sort of a review of
8 how disclosures online work, what works and what doesn't.
9 Basically what we concluded is that putting in a link
10 without any explanatory information, whether it's a
11 question mark or it says privacy policy or whatever it
12 says, generally is ineffective.

13 Consumers don't know -- consumers are busy,
14 they're not going to click on every link and they need to
15 be drawn to it. They need to be told why it's important
16 for them to click on that link. And as a result what we
17 suggested is that the links have some basic explanation,
18 like to learn more about how we collect your information
19 and use it to send ads to you, click here. And that
20 otherwise consumers are not going to click. That's what
21 we basically concluded several years ago. Now, maybe
22 that's changing over time, but, Mary, do you want to ask
23 something?

24 MS. ENGLE: Yeah, I wanted to ask Ken McGraw at
25 Zango, because, you know, you have, I think, a model of

1 labeling your ads. Do you want to discuss that at all?

2 MR. MCGRAW: Sure. For those that don't know
3 Zango, we're an ad-supported online media company. We
4 use a software download to the desktop to deliver
5 contextually targeted, not behaviorally targeted,
6 advertisements.

7 It was a couple of years ago when Esther Dyson
8 was at an anti-spyware conference and she challenged the
9 industry to continue to give consumers notices to what's
10 on their machine. And it's something that Zango accepted
11 the challenge and has done ever since.

12 Since we're a download, as opposed to just a
13 web page, we do have additional notice and consent. We
14 have a fully easily understandable notice that appears
15 before any download or installation occurs. And we also
16 provide the after-the-fact reminders within 72 hours
17 after the installation, as well as every 90 days
18 thereafter that the software is on the machine.

19 The software delivers advertisements, and we
20 identify those advertisements with a bar at the bottom
21 that states that the advertisement is brought to you by
22 Zango, together with a hyperlink for the consumer to
23 learn more about both where they're getting the ad, what
24 information that's being collected, with a link to the
25 privacy policy as well as how to uninstall the software.

1 So while we're a slightly different space than
2 most of the behavioral targeting folks on the panel, we
3 do look at consumers' privacy as a very important thing,
4 and we are out there to disclose what we think is
5 appropriate for the type of activities that we do.

6 MR. WINSTON: Professor Milne, you have studied
7 consumer behavior, consumer attitudes about these privacy
8 policies. What do you think about the idea of -- how do
9 you get consumers to pay attention to this? Or can you?

10 PROF. MILNE: Well, it's very difficult to get
11 them to pay attention because most don't. But there are
12 differences between different types of consumers. One of
13 our goals, I guess, is to try to sell consumers more
14 goods as marketers. And I have done a study that looked
15 at the amount of consumption that people buy online
16 versus the amount of skill that they say they have in
17 terms of being able to navigate through the web.

18 And those people who are more self-efficacious
19 in terms of their abilities are the ones who will read
20 the notices. And it's not the big companies that we're
21 talking about today, it's when they're going to the new
22 sites, they have a higher propensity to read notices
23 there.

24 So I think notices are really important in
25 terms of a signal. I like the comments about the

1 accountability. I think that's very important. But I
2 think one of the problems we have here with all these
3 technical solutions, which I think are very creative, and
4 I like the eBay one in particular, as well, is the lack
5 of standardization, because consumers are cognitive
6 misers. They don't want to go through and learn one
7 person's system and then another person's system.

8 Along with this study that I have been looking
9 at in terms of seeing what people do when they buy online
10 is they also do a lot of risky behaviors online as well.
11 And those people who are not as skilled tend to do a lot
12 of risky behaviors, and there's really two segments that
13 buy online, the people who are not very well educated and
14 the people who are really educated.

15 What we're missing out on is the middle
16 segment, the people who really want to buy, you know, who
17 are our market to expand e-commerce. And, so
18 standardization would probably bring those people in,
19 because they right now don't feel they have the skill
20 level to navigate some of these difficult areas.

21 MR. WINSTON: Question?

22 MR. WHITEHEAD: So, I just had a question for
23 the panel, and I would actually like to follow up on your
24 comment and go back to what Joel and Esther were talking
25 about earlier.

1 MS. ENGLE: Could you identify yourself,
2 please?

3 MR. WHITEHEAD: Steve Whitehead from Verizon.
4 I'm wondering if, going back to Joel, your comment about
5 putting some sort of a notification on the web page, and
6 obviously the preciousness of that space, but what about
7 creating, say, a set of standard symbols that could be
8 placed on web pages that could provide an indication of
9 the level of privacy or the level of tracking that's
10 going on associated with that page at that point in time,
11 so you can envision, you know, one simple model would be
12 sort of a green, yellow, red type of thing. Or I'm sure
13 we could come up with a relatively small set of symbols
14 that could provide an indication of what the publisher is
15 doing and what information is being gathered associated
16 with that page. I'd just like to get folks' comments on
17 that concept.

18 MR. WINSTON: Does anyone want to comment on
19 that? Scott?

20 MR. SHIPMAN: Having been volunteered for a
21 comment on this . . .

22 MR. WINSTON: I thought I saw you raise your
23 hand.

24 MR. SHIPMAN: No, that's fine. That's fine.

25 MR. WINSTON: You're scratching your head?

1 MR. SHIPMAN: That will teach me. I think one
2 of the challenges certainly with labels is I think even
3 in the context of the eBay and Yahoo! relationship with
4 respect to AdChoice that there are many, many different
5 permutations. So, for example, in our relationship it's
6 anonymous aggregate sharing of information between eBay
7 and an ad network partner. Yet in other instances,
8 people, it may not be anonymous.

9 So what is the implications of that type of
10 sharing? So there's two colors. You know, is the
11 information sold, or is it just being shared for a one-
12 time purpose? There's three colors. And you can go on
13 and on and on. So, I think the challenges you end up,
14 you know, with some sort of rainbow on the page, and you
15 may lose all of the meaning that you were trying to get
16 at.

17 The other comment that I had with respect to,
18 you know, can we put a sentence on the page that
19 describes, you know, we're doing advertisoral or
20 behavioral targeting, the challenge there and certainly I
21 know at least one member of my team will probably hear
22 the chalkboard with nails on it in a minute when I say
23 that our UI team always says every pixel fights for its
24 life.

25 **(Laughter)**

1 MR. SHIPMAN: And, you know, ultimately,
2 they're trying to make sure that there is the best
3 customer experience possible, and what that means is
4 sometimes white space is what makes the best customer
5 experience possible because it's clear and clutter-free.

6 On other occasions it means question marks or
7 links or mouse-overs as other types of functionality, so
8 I think while in theory it's a great concept, I know a
9 number of teams have tried to explore how do we get
10 labels. I know there have been chirping parrots on
11 browsers and other types of things I've seen in the past.
12 I don't see any of them working today in a fashion that
13 really is getting the consumer on top of the notice.

14 MR. WINSTON: I guess the downside of the color
15 scheme would be that people might confuse it with a
16 terrorist threat level or something.

17 MR. CULLEN: Yeah, Joel, don't forget, we've
18 had some experience with standardized privacy notice. I
19 think it was called GLBA, but . . .

20 MS. DYSON: We also tried this at TRUSTe. And
21 the challenge is, as Scott said, it's complicated, it's
22 not really a question of levels. There's also orthogonal
23 things like what kind of information is it, what kind of
24 marketing partners is it that you give it to and so
25 forth.

1 So, again, I think the clearest thing is to put
2 up the question mark. There are companies that sell
3 browsers that have these kinds of warnings on them.
4 There hasn't been huge take-up. Putting a question mark
5 or something like that and letting people see the
6 examples of what's going on, I think, is the most
7 effective way.

8 MR. ABRAMS: I think that there's a -- if you
9 think about -- I think a lot of time thinking about what
10 the regulatory structure is going to be three, four, five
11 years down the road, and I think that you're going to be
12 seeing the concept of trustworthiness related to a set of
13 standards within industries. And, so, rather than a
14 color code or multiple codes related to differing levels
15 of data use, it's the trustworthiness around the data
16 use.

17 In some ways the pickup on seals within the
18 seal programs are an indication of that future, but I
19 think the future is going to have multiple standards
20 based on types of industries with greater regulatory
21 oversight, so I think that something like that is coming,
22 but it's not in the near term.

23 MR. WINSTON: Well, why don't we do this?
24 Carlos has been wanting to say something.

25 MR. JENSEN: Let Lorrie answer first.

1 MR. WINSTON: Lorrie, Carlos and then Peter.
2 And then we have some questions for some of the other
3 panelists, too.

4 MS. CRANOR: So, I think the notion of symbols
5 is appealing, but as my colleagues have said, there are
6 so many different permutations. If we could find out a
7 small number of permutations that customers actually care
8 about, then that sort of thing might make sense. And
9 that's a big if, I don't know if we could do that. I
10 think it would be worth exploring whether, you know,
11 there are lots of subtle distinctions that the industry
12 cares about but maybe consumers don't, and so that's
13 something that would be worth getting some actual data
14 on.

15 I also think we should go back to finding ways
16 that we don't have to bother the consumer about all this.
17 The notion behind P3P, to bring up now an old technology
18 here, is that your browser can read the policy and make
19 decisions for you. And, so, if websites can convey all
20 their nuances in their P3P policy and the consumer can
21 once set up their browser and say, well, this is my
22 threshold and only bother me if they cross the line, that
23 might be something that could actually work in the space
24 and we should be thinking about.

25 MR. JENSEN: I mean, Lorrie brings up a very

1 good point here. Putting links to policies and context
2 is a great first step. The problem is that many of the
3 policies that are embedded in these privacy policies are
4 putting an undue burden on users.

5 So last time I looked at a privacy policy
6 seriously two years ago, 50 percent of policy -- 50
7 percent of the sites that we visited had a policy that
8 effectively said if we decide to change our mind about a
9 privacy policy, we'll let you know here in the privacy
10 policy. So that means that as a consumer I have to go
11 and check the policy every time I visit the site or I
12 have automatically agreed to new terms.

13 MR. WINSTON: Yeah, I think that's something we
14 definitely need to talk about, and maybe we should move
15 to that now, but for now we were focusing on the first
16 step, how do you get the consumer's attention. Then the
17 problem comes, all right, you got his attention, he
18 clicks on it, he goes to privacy policy, how does he make
19 heads or tails out of it.

20 MR. JENSEN: But I think this undue burden is
21 exactly what's driving users away from reading the
22 privacy policy. So, if -- I mean, reading a privacy
23 policy that could change five seconds after you read it
24 means that I'm not going to bother.

25 MR. WINSTON: Peter?

1 MR. SWIRE: Yeah, my name is Peter Swire, I'm a
2 law professor at Ohio State, a fellow at the Center for
3 American Progress. So, I want to pick up on this link to
4 context and especially what -- how manageable it is for
5 the people running the systems, and we have a lot of
6 people who run systems here, to have a policy that can be
7 detailed enough that it actually makes sense to readers.

8 There's a great temptation to be vague in the
9 policy, namely we collect lots of different things about
10 you and it changes over time. And part of that is for
11 really good reasons, which is you won't get sued. That's
12 a good reason. And another good reason is you do about
13 500 different things that are coming in from different
14 perspectives and it changes over time and you have 43
15 contracts you're managing.

16 And, so the question is if you had Esther's
17 idea or Joel's question of a link to in context to what
18 the sorts of things are we gather about the consumer, is
19 that manageable, can you actually say things, given your
20 systems that any person can use? Can you have that data
21 and have meaningful things, or is it so complicated, so
22 changeable over time and so scary because you might say
23 it wrong that you just basically inside your
24 organizations can't say what it is you're collecting.

25 MS. ENGLE: I have a question for Colin

1 O'Malley at TRUSTe. Is there a role for --

2 **(Laughter)**

3 MS. ENGLE: I'm sorry.

4 MR. WINSTON: Have we dissed you in some way,
5 Peter?

6 MR. SWIRE: No, I think the FTC has some
7 questions, that's all. If he can't answer it now . . .

8 MR. WINSTON: Okay.

9 MS. ENGLE: Okay, well, just turning to the
10 possible role of a seal program and trying to deal with
11 some of these issues.

12 MR. O'MALLEY: Sure. And I do think Peter
13 Cullen from Microsoft made an interesting point before
14 that there's a bottom-line accountability that has to
15 exist in looking at these issues, right? Because they
16 evolve constantly over time. And when we look at the
17 TRUSTe program and we're going on ten years now, we just
18 had our 10-year anniversary party, the issues that we've
19 looked at in the last ten years have evolved constantly.
20 When we first launched the program we weren't really
21 studying the impact of cookie use. We weren't looking at
22 web beacons, we certainly weren't looking at behavioral
23 targeting.

24 So, any sort of high level alert system that is
25 color-coded or that really tries to simplify the

1 trustworthiness of a site has to take into account those
2 sorts of evolving issues. And I think that's what we've
3 tried to do in the TRUSTe seal program is create a
4 standards document that evolves over time and continued
5 to fold in new issues as they begin to emerge.

6 There could potentially be a role for issue
7 specific seals, and we have seen a certain amount of that
8 within the TRUSTe program. If you look at the evolution
9 of our organization from a web seal privacy certification
10 only organization to an organization that also looks at
11 email privacy practices. And our most recent program,
12 the trusted download program, where we're looking at the
13 quality of notice prior to install of downloadable
14 applications, the extent to which any advertising or
15 tracking behavior is robustly noticed prior to install
16 and the completeness of uninstall we're seeing that as
17 well.

18 And you can see a potential corollary in
19 behavioral targeting if we're able to come up with a good
20 set of industry best practices and a moniker that would
21 be meaningful to consumers.

22 MR. WINSTON: And before we go on, just to
23 respond to Peter Sire and some of the comments about --
24 which get to the issue of the value of disclosures and
25 whether there's a better way of addressing this issue,

1 you know, I think there's a serious question here about
2 whether it's simply not feasible for businesses or for
3 consumers to go -- use this sort of notice and choice
4 model. Is it more information than consumers can handle?
5 Is it too difficult for businesses to explain in a way
6 that gives consumers sort of both sides of the equation?
7 Is it too much to expect of consumers?

8 And, you know, a lot of people have been
9 talking over the last months or years about the
10 weaknesses of the notice and choice model, and it's
11 something we're going to address, I think, in later
12 sessions as well. But for now what we're trying to focus
13 on is if we do go the notice route how do we make it
14 better or can we make it better?

15 George, there you are, I understand that
16 SafeCount has a cookie transparency strategy. Can you
17 talk about what that is and how it works?

18 MR. PAPPACHEN: Sure, sure, I'd be happy to.
19 SafeCount.net is a company that works with advertisers
20 and publishers using survey research to get consumer
21 opinion on marketing programs. And, you know, I do
22 believe that, you know, publishers value every inch of
23 their space and they want the consumer experience to be
24 as optimal as possible. And as somebody said yesterday,
25 that consumers have choices. And if they're not able to

1 deliver on promises consumers will go elsewhere.

2 So, the first thing we did insofar as we reach
3 out to consumers when they're on web pages and ask them
4 and invite them to take a survey, we worked with
5 publishers to work out rules that we want the consumer
6 experience to be not overloaded by invitations, so we set
7 site rules and said, you know, we won't contact the
8 consumer every -- but once every so often; whatever the
9 site rules indicate.

10 Then we decided, you know, we want to have a
11 process where the consumer will be able to see everything
12 we have about them that we would deliver to a partner of
13 ours. So we built out SafeCount.net. And, you know,
14 there might be a question, well, why -- how would a
15 consumer ever get there? Our presence on the web is such
16 that over time we believe that with our survey
17 invitations, an interested consumer would want to click
18 through to our privacy policy, or at some point there are
19 times when consumers are busy but there are other times
20 when they might be surfing a site and a SafeCount
21 invitation may come and they would choose to find out
22 more.

23 And if they do land at SafeCount.net, our web
24 page, our SafeCount.net web page, we turned it into sort
25 of a consumer education program as much as anything else.

1 I mean, we're not in the business of educating consumers,
2 but we felt that it was so important to sort of help
3 consumers understand what we do, that it helps out the
4 good actors and it helps our partners.

5 On SafeCount.net, we developed a cookie tool, a
6 cookie viewer tool, as I said, which enables consumers to
7 see every SafeCount cookie that is on their browser.
8 Further, we said we want to let the consumer dictate,
9 have control over the rules of engagement, so they can
10 set -- a consumer can come to SafeCount.net and set how
11 frequently they would want interaction with SafeCount, if
12 at all. They can say, well, I want to deliver my opinion
13 maybe only once every six months, once a year, never.
14 And we observe that rule.

15 Of course we worked with NAI and the IAB and
16 other such organizations and individuals within those
17 organizations to go further to make sure that, you know,
18 our brand is identified with safety and trust and the
19 partners that we work with, all of our contracts, you
20 know, we talked about how sometimes 15 percent of
21 publishers don't have privacy policies. Our contracts
22 require that any partner that we work with has a privacy
23 policy consistent with our own.

24 And, so, we see it as a space that we're in
25 together. It's a difficult space to understand, but I

1 believe that every brand here, and we work with most of
2 the large publishers here, I would say all of the large
3 publishers and most of the websites that are frequented
4 by consumers, and I would say that every one values the
5 consumer and the consumer experience. And we're just but
6 one company that's identified a way by working within
7 this space to grow our brand as a trusted brand, and as
8 consumers use this space more we want SafeCount to be
9 known as a -- we want SafeCount to be a symbol of trust
10 and consumers willing to engage with us.

11 MR. WINSTON: What do others think of that?
12 Does that sound like a sensible thing to do? Anybody
13 want to comment on that? I guess not.

14 MS. ENGLE: I'm not going to comment on that,
15 but I'll ask another question of Michael Cassidy. As an
16 ad network, what approach do you use for disclosing to
17 consumer what your behavioral targeting policies are?

18 MR. CASSIDY: Sure. I think we have a unique
19 responsibility in that we don't directly deal with
20 consumers. Our constituents are the advertisers and the
21 publishers, and we sit between both those parties, but
22 obviously we make it our responsibility to try to be as
23 forthcoming as we can. And our site receives very little
24 traffic, as you would imagine, consumers have little
25 interest in going to an ad network's website, but we do

1 have privacy policies and we do have opt-out
2 opportunities for consumers interested.

3 I think the approach that we've tried to take
4 is to really advertise the people that control the
5 budgets, and those are the advertisers and agencies.
6 There's a lot of marketers interested in behavioral
7 targeting and these types of programs, and I think a lot
8 of those organizations have actually done a good job of
9 being very thorough in their questioning of these types
10 of programs and how they can be used, how it regards to
11 privacy.

12 So ultimately the interest in behavioral like
13 programs are certainly growing, but especially as we're
14 talking to the Fortune 500 companies, many of them are
15 asking those tough questions, because I think they have
16 been kind of a silent partner in this and that they're
17 very much interested in maintaining a good dialogue with
18 their consumers because ultimately the consumers if
19 they're upset at some sort of ad or some sort of
20 behavioral program, that feeling that they get is
21 probably going to be taken out either at the publisher
22 where they're seeing the ad or the ad that they're seeing
23 themselves.

24 So, we have again some communication with
25 consumers, where it's appropriate, but, again, most of

1 our efforts have been on the education side with the
2 advertisers and publishers to a lesser extent.

3 MS. ENGLE: Well, when you say you are making
4 educational efforts, I mean, do you review their
5 policies, understand what the policies are, or try to
6 affect those at all?

7 MR. CASSIDY: With the advertisers?

8 MS. ENGLE: Yes.

9 MR. CASSIDY: Yeah, I mean, I think with the
10 advertisers, since our business is about working with
11 advertisers and helping them communicate their ads to
12 consumers across the web, our responsibility lies more in
13 how they're communicating that and making sure that if
14 there are any behavioral tactics used that they're used
15 in an appropriate way and that we are safeguarding any
16 sort of information that might be acquired, which at this
17 point is no PII at all.

18 So, we will certainly work with advertisers and
19 make sure that they're comfortable with what they're
20 doing and obviously not do anything that would jeopardize
21 any sort of consumer. We don't acquire any sort of
22 information that could jeopardize a consumer. Right now,
23 most of the behavioral targeting that we engage with and
24 a lot of the other firms is very much just more on the
25 surf-based side of things, so there isn't any sort of

1 confidential information that's being acquired.

2 But, again, with where we stand most of our
3 efforts go more towards the advertisers.

4 MR. WINSTON: Zulfikar Ramzan, from Symantec's
5 standpoint, how do you think advertisers or websites
6 should give consumers the information they need to make
7 good choices? What works, what doesn't work?

8 MR. RAMZAN: So, I think we have seen so far
9 that what doesn't work is trying to provide consumers
10 with more information because they barely read the
11 information that they're given now and it's a big
12 challenge we're seeing. So part of our goal really has
13 been to make the task easier for the end customer.

14 One way we do that right now is through a new
15 set of technologies that are designed around helping
16 users to manage their identities in a much easier way.
17 Right now I have identities -- multiple online
18 identities. For example, I have an identity with eBay,
19 one with Amazon. I've got one with a social networking
20 forum I'm part of. I've got one at work and so on and so
21 forth. Each of these identities right now for most
22 people tend to have a common set of criteria. Like I
23 might give the same email address to all different
24 people. In fact, one email gets disclosed in some way,
25 basically I am -- I'm more or less hosed, and everybody

1 is going to spam me and so on and so forth.

2 So, one thing we're trying to do right now is
3 allow people to be able to provide different identities
4 or different online entities that are consistent with how
5 they use the entities. For example, the ability to have
6 different email addresses for different online
7 identities. If I were to do that now it would be
8 complicated, but with some of the technology we're trying
9 to build and that we have been building, we've simplified
10 that process considerably so that when I do log in to a
11 particular website I can associate an identity with that
12 website automatically and then I don't have to worry as
13 much about what I'm doing.

14 I think part of our goal is really ultimately
15 to make the process much simpler for people rather than
16 trying to present them with too much information, let
17 them manage the information that they have with them in a
18 much easier fashion.

19 MR. WINSTON: It sounds like most of you feel
20 that improving notices is like rearranging the deck
21 chairs on the Titanic, that there may be better ways of
22 giving consumers the tools they need to protect
23 themselves. Is that --

24 MR. ABRAMS: Notices have value that does not
25 relate -- that goes beyond the consumer just

1 understanding. I don't think we can lose sight of the
2 fact that notices create a framework for accountability,
3 a framework for defining fairness in the marketplace.
4 So, we should care about notices being addressable,
5 notices being accurate, notices being able to drill down
6 through as many layers as it takes, that there's an
7 importance to notices that goes beyond just guiding
8 individual choice. And I think that that's an important
9 point.

10 I mean, the notices have to be accurate, they
11 have to be addressable, they need to be actionable, they
12 need to give guidance, they need to drive competition,
13 they need to do lots of things. But if we just say it's
14 a matter of give notice, have choice, it's -- it goes
15 beyond that.

16 MR. WINSTON: Colin.

17 MR. O'MALLEY: Yes. I don't think it's about
18 rearranging the chairs on the Titanic at all. I think
19 notice is incredibly important, and I think that we need
20 -- as an industry need to work on ways to deliver
21 proactive notice, to come outside of the privacy
22 statement and to delivery proactive notice in a fashion
23 to consumers that's meaningful.

24 The problem is that when we get -- in our
25 programs, for example, we're really running self-

1 regulatory programs. We're trying to provide guidance on
2 industry best practices for emerging technologies. And
3 when we get really prescriptive with the types of notice
4 that we expect in a proactive fashion, across our network
5 of websites, we tend to always get behind the curve.

6 Once we come up with standards for how a
7 proactive notice needs to be delivered, the context
8 changes across the properties that might be within our
9 network. And ultimately contextual notice is probably
10 the most meaningful notice. So, when we're looking at --
11 I was describing some of the ways in which our program
12 has evolved, all those different stepping stones within
13 the privacy landscape, the cookies, the web beacons, the
14 behavioral tracking and go into further detail on what
15 software might be available on that website and whether
16 or not this site engages in email marketing and under
17 what circumstances and what kind of sharing with third
18 parties might be done, really anything that might be in
19 that privacy statement. If we head along the road, come
20 up with very prescriptive proactive notice standards for
21 each of those, then we'd probably end up with a home page
22 at this point that looks like a terrible food warning
23 label that includes, you know, dozens and dozens of
24 bullets.

25 So I think from our perspective, yes, proactive

1 notice is incredibly important. And in particular for
2 the issues that are currently highlighted at this point
3 in time as being critical to the user, and I think that
4 one of the functions of a workshop like this is to say,
5 listen, behavioral targeting is becoming one of those
6 issues and we need to think about creative ways for
7 delivering proactive notice, because this issue is
8 becoming really topical.

9 But we don't want to become really prescriptive
10 and put a deep stick in the mud on this particular issue
11 in isolation of all the other issues that are really
12 important, and we need to recognize that we may very well
13 have another town hall meeting 12 months from now on an
14 issue that we didn't contemplate today.

15 MR. WINSTON: Lorrie?

16 MS. CRANOR: Yeah, I agree. We do need to
17 improve the existing notices, and it is worth putting
18 effort into that so that when people want to read them
19 they're there and they can read them and they can be
20 effective. And the fact that people don't read them
21 shouldn't be a reason to abandon them. I don't think we
22 should -- I don't think our metric should be do people
23 read them. I think our metric should be when people want
24 to find information, do they find them useful at that
25 point in time.

1 And I think we should continue to find creative
2 ways of getting to the meat of what people want without
3 them having to go read the full notice. So any of these
4 things that get just what you need, just the facts when
5 you need them and making them available and especially
6 some of the technological approaches that let people do
7 this without having to go read long things I think are
8 steps in the right direction.

9 MR. WINSTON: Carlos?

10 MR. JENSEN: My previous statements kind of
11 make me sound like I'm very much against privacy notices,
12 but that's not true. The privacy notice provides a
13 framework within which, you know, companies can think
14 about their commitment to the user and kind of provide
15 some framework for accountability.

16 There are, however, some very significant
17 usability problems with the privacy notice in that it
18 puts too much burden on the user. And, you know, taking
19 advantage of context, things like -- let's go back to the
20 issue of when a policy is being updated. Most of the
21 companies here know when the user was at their site last.
22 Why not have a policy of providing like a popup or a
23 prominent notice when something has changed? So, I think
24 there are a lot of mechanisms like that that can be
25 exploited to make privacy policies a lot more usable.

1 MR. GIVOTOVSKY: Yes, just a quick comment and
2 perhaps a question out of it.

3 MR. WINSTON: Would you identify yourself?

4 MR. GIVOTOVSKY: Yes, My name is Nick
5 Givotovsky. I'm a consultant. My company is called
6 Datasphere Interactive, and I study rights and policy in
7 the digital realm, among other things. And I'm very
8 curious. I mean, what we're hearing is a diversity of
9 different privacy policies and statements of those
10 policies across respective environments.

11 And I think if you drill down you can find out
12 what the effect of those environments are and one's
13 rights within those environments and the flexibility
14 offered by those respective environments. And clearly
15 there are some innovative developments here that suggest
16 a greater degree of accountability on the part of
17 presenters of advertising to consumers. And I think
18 that's very productive.

19 As a consumer, as a user of the web, there's no
20 way to combine across all of those different environments
21 an aggregate profile of one's web exposure. There's no
22 comprehensive location to go and say, well, to what
23 extent am I exposed across all of my activities on the
24 web? What's my active profile? And to what extent is it
25 distributed and redistributed across these environments?

1 And so the gentleman from Symantec just brought
2 up a topic that I mentioned yesterday, which was digital
3 identity. And digital identity is enabling people to
4 move their credentials and their profiles across multiple
5 environments. So to what extent will those tools enable
6 or not enable a unified notion of one's exposure, with
7 respect to even across diverse digital delivery
8 environments?

9 MR. WINSTON: Anybody want to comment on that?

10 MR. RAMZAN: I heard Symantec mentioned, maybe
11 I should comment. So first of all, actually, I think
12 that certainly the idea of having a unified digital
13 identity that's more of a virtual concept can from a
14 security position pose a real danger because that one
15 identity can now be exposed. So, I'm used to thinking
16 about all the bad things, so excuse me if I'm a bit
17 pessimistic sometimes.

18 But in reality I think that we often have
19 multiple digital identities, it's not just one. In fact,
20 even in the real world we have multiple identities. We
21 have an identity at work, we have identity among our
22 friends, we have identities at different places we do
23 business with and so on and so forth. So I think that
24 part of the solution will be to allow people to simplify
25 how they deal with those different identities. And I

1 think that at least breaks it apart so there's no one
2 single point of failure, so to speak. That's basically
3 what I want to say.

4 MR. GIVOTOVSKY: Point taken. And I think the
5 tools that are out there now for digital identity offer
6 that promise. But I'm very curious as to whether those
7 tools will be leveragable or be applicable to the problem
8 that I mentioned, which is, okay, an association with my
9 -- be it my work, my play, my private persona, to what
10 extent have I disclosed and to what extent am I exposed
11 in the application of that individual sub-persona,
12 because I think we ultimately do have singular
13 identities, even if we manifest personas separately
14 within environments.

15 And, you know, many of the targeting activities
16 that are undertaken right now are considered are all
17 about combining the activities within different domains
18 to one another, so that we can get marketing offers in
19 one environment, perhaps acting in a private context,
20 when behaviors were tracked in another environment acting
21 perhaps in a professional context. I mean, that's the
22 goal of surrounding people with marketing messages that
23 are personalized is to create context in which meaningful
24 communications can be presented.

25 So the purposes that we're describing are

1 actually at cross purposes and there will be an
2 intersection that I think is a collision coming down the
3 road between integrated digital identities and targeted
4 marketing.

5 MR. WINSTON: Jeff?

6 MR. CHESTER: Jeff Chester, and I have a
7 question about disclosure, and by no means do I endorse
8 this, but I have been thinking about there has to be a
9 simple unified way to tell the individual exactly what is
10 going on. One of my critiques about behavioral targeting
11 is we need to make the process conscious so that the
12 user, the individual, the citizen, the consumer
13 understands what the purpose of the system really is and
14 then can make meaningful choices.

15 So, I want to ask a question about disclosure.
16 Why can't you say you're collecting and targeting and
17 profiling all this information? Why can't you say what
18 you tell your clients? You know, which we look at and
19 read with interest, that you're collecting this data to
20 move people through the, quote, unquote, conversion
21 funnel, that you'll be mixing information across
22 platforms, that your system is designed to deepen brand
23 identity, that your systems are designed to, as many of
24 you put it, not necessarily you but behavioral targeters
25 say to up-sell, to retarget. Why can't you say to the

1 consumer what the marketing purposes and designs are of
2 the system that's been put in place? Thank you.

3 MR. SHIPMAN: I think that's a great question.
4 In some of my prep material for the panel today I
5 actually printed out an announcement that we put on our
6 announcement board. We put it out on October 5th. It
7 actually has a picture of me when I joined the company in
8 like 1998.

9 **(Laughter)**

10 MR. WINSTON: Want to pass that around so we
11 can all see it?

12 MR. SHIPMAN: Feeling quite youthful. It
13 begins with hello, you've seen a lot of news lately
14 spotlighting privacy issues for Internet companies like
15 Google's purchase of Double Click, Facebook's new ad
16 programs or the improvement of practices among search
17 engines like Microsoft, Yahoo!, Ask.com, all the things
18 we've been talking about, right?

19 But to your point, why can't we just tell our
20 customers what we're doing with the information, this
21 general announcement, which is still available on the
22 eBay announcement boards, talked about AdChoice and
23 talked about what these links around the ads were going
24 to be so that they could understand exactly how we're
25 serving ads and why.

1 And I heard from Jane earlier about the
2 blogging and the videos that they're doing. And, so, I
3 think that we're seeing some attempts to get to the
4 customer and say here is why we're collecting information
5 and here is what we're doing with it. I think that the
6 challenge is the customer might not be used to it and
7 we've got to get them up to speed with what to look for,
8 which is why we're testing different types of links and
9 different types of UI.

10 But you're absolutely right. It's a challenge,
11 which is, is it a paragraph on the bottom of every page?
12 Is it on the top of the page, is it on the left or the
13 right? Those types of messaging for a bidder when
14 there's five seconds left are going to be completely
15 ignored and all they're going to do is try to find the
16 bid now button to get that item that they must have.

17 And, so, in that context, it's completely
18 inappropriate. So finding the right context which is
19 also what I've heard today on the panel is also equally
20 relevant.

21 MR. WINSTON: Peter?

22 MR. CULLEN: Jeff, can I pick up on that?
23 Because I think you raised such a great point. Last June
24 you may recall we made some commitments to attempt to do
25 a better job of describing many of the things that you

1 just did. And, so, for example, those went live this
2 week, so many of the things that you actually talked
3 about in terms of what information is collected, how it's
4 used, how it's aggregated, have now been added to our
5 particular privacy notice, in addition to being very
6 explicit that we do not use personal information. So
7 there's a pretty profound statement.

8 And I want to kind of go a little bit sideways
9 on that, because it's not just the disclosure but it's
10 also then the practices that an organization has to put
11 into play. I suspect you've had a chance to look at the
12 paper that's available here in terms of how we actually
13 do that decoupling between that. So I'd love your
14 feedback on that.

15 But I kind of want to then go a little high
16 level, because, you know, we're having a discussion about
17 how we perhaps provide some uniform symbol or whatever
18 that might be more relevant to a consumer, yet we're
19 still, I think, kind of ignoring one of the fundamental
20 challenges that today there is no regulatory requirement
21 in this country for companies to even post a privacy
22 statement.

23 And, again, not to flog this horse yet once
24 more, but we're, you know, pretty active in terms of
25 saying that it is time for some form of uniform privacy

1 legislation. We think that's the right thing for
2 consumers of which obviously providing notice would be a
3 core part.

4 MR. WINSTON: Carlos

5 MR. JENSEN: No.

6 MR. WINSTON: No? Okay.

7 MS. ENGLE: Well, just setting aside the issue
8 of legislation for a moment, absent that, what about -- I
9 wanted to go back to an issue that Joel raised earlier,
10 the notion of, you know, is it an oversimplification to
11 have some sort of statement that would be more than just
12 the question mark or something like that, that will give
13 consumers a little bit more of a clue as to why they need
14 to click here to find out more information.

15 And people talked about the preciousness of the
16 real estate. Well, perhaps some sort of uniform label or
17 logo could be developed along those lines and that people
18 would come to understand in a way you understand what a
19 shopping cart means and things like that.

20 MR. CULLEN: Here's the challenge.

21 MS. ENGLE: And that wouldn't -- I'm not
22 talking about, you know, a red, green system for the
23 privacy practices themselves, but just something that
24 consumers would understand here is where I need to go to
25 find out this information about how this ad or how I'm

1 being tracked.

2 MR. CULLEN: So, let's take just a step, high
3 level here. So, today, we're talking about behavioral
4 targeting, we're positing may be perhaps instead of a
5 link at the bottom of the page that says privacy, we
6 might have something that hovers over it, learn more
7 about behavioral targeting.

8 One might speculate that two weeks from now
9 when you have a town hall on Social Security numbers the
10 subject will be well, maybe we should have a hover to
11 learn about how Social Security numbers or, well, perhaps
12 we should have a hover to learn how we respond to court
13 orders.

14 So you start to think about pretty soon we're
15 back to, wow, I guess that link called privacy is still
16 not a bad place to at least create a start.

17 MS. ENGLE: But then tying back to the notion
18 of just in time, I mean, that's -- people have -- a lot
19 of people have mentioned that that seems to be important,
20 that consumers need to have some sort of trigger to know
21 to check the privacy policy. I mean, for example, I
22 recently bought something online and before I bought it I
23 had read some consumer reviews.

24 And afterwards -- and I purchased the product
25 and had used it, I thought maybe I'll post a review of my

1 own, because I found the reviews helpful. Well, when I
2 went to do that and they asked for my email address and
3 so forth there was a little button right there, it said,
4 you know, privacy policy. And I thought, okay, well, I
5 better go check that.

6 And it turned out if I had given my email
7 address, which I had to in order to enter a comment, they
8 were going to share that with all sorts of people and I
9 could be marketed to. And, so, obviously I chose not to
10 post a comment, but that was an example where I wouldn't
11 even have thought that posting a comment would have
12 resulted in, you know, the sharing of my email address.
13 So I think that kind of just in time, the idea that
14 people need to know at the point where their information
15 is being shared, they need to have some reason to click.

16 MR. WINSTON: I have a note here that Jane
17 Horvath would like to speak. I can't actually see her
18 from here.

19 **(Laughter)**

20 MS. HORVATH: That was a ways back but . . .

21 **(Laughter)**

22 MR. WINSTON: I just got the note this second,
23 so it's not my fault.

24 MS. HORVATH: I was just basically going to say
25 what Peter said. I mean, if we come up with another form

1 of notation that something other than privacy policy in a
2 month or two it's going to become generic as well and
3 people will not click on that for the same reason. And
4 that's why we've chosen to use things like blogs to go
5 much more into detail about important issues and then
6 videos as another way to illustrate and to use more space
7 and to bring the -- to illustrate the privacy policy in a
8 much more user-friendly way than having just a link down
9 at the bottom that becomes genericized after a while.

10 MR. ABRAMS: You asked a question about just-
11 in-time notices, because a number of us in the industry
12 have been talking about this whole concept of just-in-
13 time notices for about a year. And I think that there is
14 an attractiveness when something is going to be
15 surprising to give a sense of warning to the consumers
16 that something is surprising.

17 But there's a lot of norming that has to go
18 behind that to define what is going to be surprising
19 because today we're talking about surprising in the sense
20 of something that had nothing -- well, I guess did have
21 to do with marketing -- but it had to do with what is
22 surprising when you were going to give a rating or a
23 review.

24 And I think that you can't say "let's create a
25 new standard" without saying that there's a lot of

1 norming that goes around that standard and that you have
2 to think about that standard as it relates to other
3 standards. So, the point is, all of these are great
4 ideas, but you can't say, I'm going to do one simple
5 solution that's going to fix an amorphous problem so I
6 think there is some attractiveness that is being
7 discussed in industry around this concept of just-in-time
8 notices, but there's a lot of background work that needs
9 to be done before you can get to the place of saying
10 where should that be.

11 MR. WINSTON: Srinija.

12 MS. SRINIVASAN: I was just going to make the
13 simple point to Mary's point that it is normal course of
14 business for us at Yahoo! to put that just-in-time notice
15 at the point of information collection, so any time
16 you're traversing our site if there's a survey or a, you
17 know, sweepstakes or a place where we're specifically
18 collecting that information, I mean, the initial place
19 where we would receive personally identifiable
20 information would be if you choose to register with us.
21 And at that place there is an abundant opportunity to
22 read our privacy policy. We ensure that you have an
23 opportunity to see our privacy policy, where I really do
24 feel, I'm really proud of the clarity of the language in
25 that policy that says this is what we collect and we use

1 it to customize the content and advertising that you see.

2 So what you just described is absolutely
3 routine, normal course of business for us. And I think
4 that you're seeing continual evolution and innovation in
5 terms of "where are the -- as Marty, I think, said,
6 teachable moments?" So in the case of employing
7 behavioral targeting in anonymous fashion off our
8 network, you know, you've seen the model that eBay and
9 Yahoo! have chosen to go out with.

10 In other words, I just -- I think that this
11 notion of contextual notice is absolutely important.
12 Every opportunity that we have to let people know we have
13 a privacy policy, you can consult it, if you have
14 concerns and questions in that regard we use it. And I
15 think you're seeing lots of experimentation and
16 innovation in that area.

17 MR. WINSTON: Colin, is that you down there?

18 MR. O'MALLEY: Yes.

19 MR. WINSTON: Yeah, that's you.

20 MR. O'MALLEY: So, I want to separate two
21 questions that I think are imbedded in that question of
22 whether or not there ought to be a standardized
23 communication vehicle. The first question within that
24 really is do we need some kind of communication vehicle
25 to proactively deliver notice to consumers about

1 behavioral targeting. And I think the answer to that is
2 yes. We need more proactive communication and noticing
3 to consumers on this issue, absolutely.

4 The second sort of follow-up larger question
5 there is do we lead with the prescription, right? Do we
6 lead by saying not only do we need the notice in a
7 proactive fashion, but do we have a way to universally
8 across the industry communicate this in a standardized
9 way?

10 The fact is, with TRUSTe, for example, as a
11 small organization, we don't feel like we know yet what
12 that right standardized method is. And the best way for
13 us to figure out what that method is is to actually allow
14 people to experiment for a little while. Yahoo! -- I'm
15 sorry, AOL had an interesting announcement yesterday with
16 their communication and education campaign through the
17 Dakota network, the eBay presentation today had a really
18 interesting set of explorations on this topic.

19 We need to let those explorations go out there
20 for the experimentation to happen, for us to be able to
21 have a data set and enough examples to view and assess to
22 even consider going with the prescription. So, yes,
23 proactive notice, but we don't want to lead with the
24 prescription.

25 MR. WINSTON: Is there anyone on the panel who

1 thinks the government should step in right now and
2 prescribe a notice? Don't all raise your hands at once
3 here. Question or comment?

4 MS. DYSON: I want to just continue on this
5 topic. I think in addition to just in time we should
6 have just for you. It's sort of ironic, marketers are
7 now figuring out how to tailor advertising and offers and
8 all this kind of stuff to individuals. They will use
9 different copy for different kinds of people. Yet why
10 can't we do the same thing with privacy statements?

11 So when you say the privacy statement may
12 change a week later, perhaps there's a way to ask the
13 person if you're relying on this privacy statement and
14 you'd like to know if we update it, click here. So that
15 you end up having not just -- not only just in time but
16 also consumer-specific information about privacy
17 policies. I do care about medical information, I don't
18 care about financial or whatever. But apply these same
19 techniques and the same brilliance of communication you
20 use advertising chocolate chip cookies to advertise
21 online cookies.

22 MR. WHITEHEAD: Steve Whitehead. So, I wanted
23 to comment on the just-in-time thing and the need for
24 notification. I think that's a great idea. It actually
25 goes back to that previous comment about having the set

1 of standardized symbols, for example. I think that would
2 be a great example of a place where you can have
3 potentially standardized symbols that said what is this
4 information that you're entering into this field being
5 used for.

6 It seems to me that you could have a relatively
7 small set of standard symbols that could potentially be
8 used to provide course-grain indications to users about
9 whether this is being used for third party marketing or
10 whatever.

11 But my comment, and maybe I'm a bit of a
12 pessimist, but I don't see that ever happening. I think
13 it would be someone like TRUSTe that would drive such a
14 thing, but I don't see it happening because I don't
15 really see that the publishers have any incentive to do
16 that. I don't think it's there. And, so, it won't
17 happen without strong incentives. And I don't see how
18 the publishers have any incentives to do that.

19 Any comment?

20 MS. DYSON: Consumers may ask for it. They're
21 getting used to it on Facebook. I really think the
22 consumer expectations are changing. And that's what's
23 going to change the marketers' behavior.

24 MR. McCULLAGH: Oh, and one other thought. I
25 mean, this doesn't have to be done by the companies

1 represented up here. If you've got a great idea for a
2 startup that would be a third party rating service, go
3 for it. If you're right and people actually want this,
4 there's lots of money kicking around for startups right
5 now.

6 MR. WINSTON: Question over here.

7 MR. CULLEN: Esther, you going to invest in
8 that one?

9 MS. DYSON: I already have.

10 **(Laughter)**

11 MS. DYSON: But it wasn't in my disclosure
12 statement because they took it out.

13 MR. ZITELMAN: Hi, my name is Jeff Zitelman,
14 I'm a citizen and stakeholder here. I would urge -- I
15 think there is a role for the Commission to take to
16 create something that's very simple. I mean, there have
17 been some relatively complex problems in other industries
18 that have been solved by simple solutions.

19 A good example is TV rating. I happen to have
20 a teenager, there's certain shows I don't wish for them
21 to watch, okay? As soon as a TV show starts, I see that
22 TV-MA, TV-14, whatever it is, in the corner. That could
23 be done in this, with the symbols such as the gentleman
24 before me had mentioned.

25 I think that requiring people to look through

1 privacy policies is frankly absurd because more often
2 than not, orders of magnitude more often than not, people
3 will simply click yes, I have read something, when indeed
4 they haven't. So I would suggest that the Commission
5 does have a role but play to create something very simple
6 and put it in place.

7 MR. WINSTON: Thank you.

8 Lorrie, did you want to . . .

9 MS. CRANOR: So you asked a question as to
10 whether there should be a regulation with mandated
11 standardized notices. And while I'm not ready to say
12 yes, we should definitely do that, I think the answer is
13 maybe. And, so, I'll go out on a limb here further than
14 my fellow panelists.

15 But I think, though, that we shouldn't just be
16 talking about mandated notices for behavioral
17 advertising. I think that we should be looking at the
18 privacy issues online more holistically and we shouldn't
19 look this week at behavioral advertising and next week at
20 Social Security numbers. We should be looking at the
21 whole picture and think about do we need a nutrition
22 label for privacy, privacy in general and, if so, which
23 are the things that we need to pull out?

24 I mean, there was a whole lengthy process in
25 designing the nutrition label. There was a lot of

1 research that went into it. A lot of research figuring
2 out that, you know, calories and fat are really important
3 or whatever. And I think we need to start doing that
4 kind of research now to see what are the things that are
5 really important? Once we know what's important, then
6 what's the best way to communicate about that. And, so,
7 I would support the FTC starting that process of research
8 at this point.

9 MR. WINSTON: As many of you probably know, the
10 FTC and the bank regulatory agencies have undertaken
11 exactly that process in an effort to make the financial
12 privacy notices that we all get and throw away
13 comprehensible. And it's literally been three years of
14 consumer testing and learning a lot, trial and error.
15 So, there is some precedent for that, but an interesting
16 idea.

17 MR. ABRAMS: You started that process in 2001,
18 so while you have three years of testing, you have a six-
19 year process. And I don't think this is the forum for
20 discussing that, but part of the process issues was the
21 marketplace changed significantly from 2001 to 2007. And
22 I think that, you know -- and that's part of the
23 difficulty government has in the norming process is, this
24 is a marketplace that changes incredibly rapidly, and it
25 is very difficult for you to come up with a norming

1 process that takes six years to then have it applied to
2 the issues that exist when it's done.

3 MR. WINSTON: Just to clarify the record, two
4 people have now said that next week we're going to
5 require disclosures about Social Security numbers. And
6 our workshop is not for another five weeks.

7 **(Laughter)**

8 MR. WINSTON: You've got at least five weeks to
9 worry about this.

10 Carlos?

11 MR. JENSEN: To follow up Lorrie's point, I
12 agree that there's very strong need for standardization
13 of policies, and not just within the financial domain but
14 across all domains. Right now, policies are confusing
15 because users don't know what they're going to find in
16 them and whether they're going to address their
17 questions.

18 And on the issue of iconic representation, I
19 think we're approaching this maybe the wrong way.
20 Representing a complete privacy policy in iconic form is
21 incredibly complex, and you'd probably end up with a set
22 of 800 icons, which no one is going to memorize, but if
23 you look at what users care about when they visit a web
24 page, that's a very limited amount of information, and
25 coming up with a small set of iconic representations or a

1 short list of, you know, this is the food content label,
2 would be feasible.

3 So, let's take an example of what kind of
4 information that could be. When you go to a web page,
5 for instance, having a short list of who else is getting
6 information about my visit here, and is my information
7 that's being tracked combined with any other source.
8 That's a very small amount of real estate that's required
9 and something that is incredibly powerful to users.
10 Getting notices that say this information may be shared
11 with trusted third parties, does that mean that I have to
12 stop talking?

13 **(Laughter)**

14 MR. JENSEN: I mean, big notices such as, you
15 know, this information may be shared with trusted third
16 parties is completely meaningless to users. Who are
17 these third parties? Who trusts them? I certainly
18 don't.

19 MS. ENGLE: Well, actually, we do just have
20 about one minute left. If there are -- question?

21 MR. CAPEK: Just a very quick comment. My name
22 is Peter Capek. There seemed to be very little
23 information available, at least that people are willing
24 to share, about how many people read privacy policies.
25 And what little information there is seems to indicate

1 that almost no one does.

2 I'm curious, I'm curious whether anyone has
3 looked at whether -- and maybe somebody could, if the
4 information is available, whether there's more
5 examination of privacy policies in situations proximate
6 to things that you might expect people to worry about.
7 For example, if I go search for cancer at Google, did I
8 just go look at the privacy policy before that or right
9 after it? Probably before it is more indicative. Or if
10 I look at medical sites, is there more use of privacy
11 policy? I don't really care about eBay's privacy policy,
12 because there's nothing I do there. I assume they will
13 take appropriate care of my credit card number, but
14 beyond that, I don't really care who knows what I buy.

15 MR. WINSTON: Any other last comments?
16 Anybody?

17 MS. DYSON: Yeah, the way to get people to read
18 these statements is to say follow this link and earn a
19 chance to win \$5.

20 **(Laughter)**

21 MS. CRANOR: I just wanted to comment that I
22 would love to have that sort of data. I'm not in a
23 position to collect that data, but with our Privacy
24 Finder search engine, some of the data that we do plan to
25 collect is when do people click on the privacy report

1 link and is there a correlation between, say, healthcare
2 searches and clicking on the privacy report link.

3 MR. CULLEN: You know, this -- we seem to be
4 inferring that this information about few people collect
5 is some proprietary type thing, It's just, you know, I
6 think many of us probably look at it. I don't have
7 current data, but I can tell you when we first launched
8 service pack 1 -- 2, sorry, for Windows XP, it was the
9 first operating system that actually had a privacy
10 statement.

11 In the first three months over 1.5 million
12 people clicked on it. Now, do I know whether they
13 actually read it, do I know what page -- but it gives you
14 some order of magnitude that people actually do look at
15 these sorts of things.

16 MS. ENGLE: One last comment from Carlos.

17 MR. JENSEN: To answer your question more
18 directly, I mean, we do have experiments that show that
19 when you ask people for information -- directly ask
20 people for information that they consider to be sensitive
21 such as Social Security numbers or credit cards, they do
22 check privacy policies a lot more frequently than when
23 you're at a random search engine, which may or may not be
24 the right thing to do.

25 I like to joke that no one knows you as well as

1 Google does, because -- simply because of the
2 accumulation of information over time. So hopefully that
3 answers your question.

4 MS. ENGLE: Well, I'd like to thank all of the
5 panelists this morning, and we will reconvene at 11:15.

6 **(Applause)**

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 **SESSION 7: YOUTUBE CONTEST PRESENTATION**

2 MR. MAGEE: Hi, everyone. We're going to start
3 Session 7. My name is Peder Magee, I'm in the FTC's
4 Division on Privacy and Identity Protection.

5 For this session, we're going to do something a
6 little bit different. So far we have heard a lot about
7 cookies and their use in online behavioral advertising,
8 but whenever we see the cookies in the presentations they
9 show up as a long line of abstract letters and numbers
10 and I think it's hard to get a real feel for them.

11 So, to get a somewhat different perspective on
12 what cookies are and how they operate, we're going to
13 watch five short videos that were submitted to YouTube in
14 connection with the Berkman Center's Cookie Crumbles
15 Contest. A lot of alliteration.

16 Our group of judges will discuss the videos and
17 address some of the issues they raise, and then we're
18 going to take questions from the audience. I hope we'll
19 have participation there and we're going to have a vote.

20 So, let me introduce the judges and then I'm
21 going to turn over the Max Weinstein from the Berkman
22 Center. Our judges are -- they're sitting in the front
23 so they can watch the videos. If they could stand up as
24 I say your name.

25 Esther Dyson of EDventure and several other

1 companies that we didn't disclose in her bio.

2 **(Laughter)**

3 MR. MAGEE: Jeff Chester of CDD. Alissa Cooper
4 of Center for Democracy and Technology. Michael Zaneis
5 of the Interactive Advertising Bureau. Professor Lorrie
6 Cranor from Carnegie Mellon. Rob Pegoraro from the
7 Washington Post and Tikva Morowati who is a designer
8 researcher, artist and community builder.

9 So, Max, if you want to introduce the contest.

10 MR. WEINSTEIN: Sure, thanks, Peder, and good
11 morning, everyone. When Esther Dyson came to us at the
12 Berkman Center a couple months ago and said she had an
13 idea to do something really interesting and fun and
14 interactive at an FTC event --

15 **(Laughter)**

16 MR. WEINSTEIN: -- we were a little mystified,
17 but then she explained and it really was a great idea,
18 which was to have this YouTube contest and ask people to
19 submit short videos explaining the purpose and use of
20 Internet cookies and to use it as basis for discussion
21 about the larger issues around privacy, marketing and
22 behavioral advertising.

23 So, we're really excited that during the course
24 of the couple of weeks that the contest was open we
25 received 24 really interesting entries, some really great

1 stuff, a wide range of creative ideas. And from those,
2 they were paired down to five by our friends at Consumer
3 Reports Web Watch. They picked the five that they
4 thought best represented both a really creative and fun
5 look at the subject and also the most informative and
6 interesting and something that would be able to connect
7 with consumers and convey really useful information.

8 So, those are the ones you're going to see here
9 today. What I'm going to do is introduce each video,
10 we'll show the video, and then four of the five finalists
11 are actually here today. So, we're really excited to
12 have them here with us. The fifth, before you feel too
13 bad for her for not getting a trip to D.C., she's
14 actually in Paris right now. That's why she couldn't
15 come. So, she has a representative of hers here to stand
16 in her place. So, I'll have each of them stand up and be
17 recognized at the end of their respective video clip.

18 I do want to quickly thank the sponsors without
19 whom we wouldn't have been able to make this thing
20 happen. Esther's company, EDventure, is one of our
21 sponsors, Medium, and our sort of jumbo cookie sponsor,
22 if you will, was Google. So, we certainly thank them for
23 their support of this program.

24 We also want to express our appreciation for
25 the FTC for opening up an event like this to a slightly

1 different type of panel discussion.

2 So, on that note, we're going to start with our
3 first video.

4 MR. MAGEE: Apparently, we may have to run the
5 videos straight through. If that's the case, then we'll
6 have the creators get up at the conclusion of the fifth
7 and we'll do it that way. Sorry.

8 MR. WEINSTEIN: All right, sounds good. So,
9 let's see the first video and possibly all five.

10 **(Laughter)**

11 **(Videos played)**

12 **(Applause)**

13 MR. WEINSTEIN: So, while someone tries to
14 figure out how to get the lights back on, we'll introduce
15 each of the creators and ask them to stand. The first
16 video, which is the one with the clever graphics, was
17 called "Cookies" and that was by Clayton Miller from the
18 Chicago area.

19 **(Applause)**

20 MR. WEINSTEIN: The second one with the young
21 girl, that actually was a girl, by the way, doing the
22 Cockney accent was called "What's a Cookie with Mari,"
23 and that was submitted by Leslie Weiner of Florida and
24 her daughter Mari.

25 **(Applause)**

1 MR. WEINSTEIN: They're being represented by
2 Frank Paynter today.

3 **(Applause)**

4 MR. WEINSTEIN: The third one with the real
5 live Internet server was called "Got Cookies," and that
6 was by Justin and Kristin Schaack of Minneapolis.

7 **(Applause)**

8 MR. WEINSTEIN: The fourth and sixth video was
9 "What Is A Cookie," and that was by Aaron Suring who came
10 down from Juneau, Alaska.

11 **(Applause)**

12 MR. WEINSTEIN: And the fifth one with the
13 creator starring as the in-your-face guy is "Cookies 101"
14 by Tim Welsh of Orlando, Florida.

15 **(Applause)**

16 MR. WEINSTEIN: So, we'll ask now the panelists
17 to come up and join us for some discussion.

18 **(Brief pause)**

19 MR. WEINSTEIN: All right, I would like to just
20 start very briefly, there was a great line in Aaron's
21 video, cookies aren't the scariest thing on the Internet,
22 but I wish they were. So, with that in mind, I'm going
23 to ask Esther who came up with the idea of this contest,
24 why the focus on cookies?

25 MS. DYSON: I'll tell the story of how this all

1 started. I was thinking about these issues as, amazingly
2 enough, I often do, and it seems to me, again, the real
3 problem is not with the disclosure statements or
4 typically with the behavior of companies who actually
5 deliver on their promises, but on consumers'
6 understanding of what's going on. And I thought, well,
7 why not do a YouTube video contest? That's the way
8 everything else happens.

9 The purpose is not really to pick a winner and,
10 in fact, I have recused myself from voting. So, I'm
11 going to be part of the discussion, but sort of to prove
12 the point that voting isn't the real purpose. It's the
13 discussion that these videos will generate. I thought it
14 would be really cool to do this. And the product, number
15 one, could be used as education; number two, it would
16 inform the discussion here; and number three, with luck,
17 there will be another contest like this that will be even
18 better, that will have a longer time for the videos to be
19 submitted, that will get more visibility, that will cover
20 other issues, specifically what companies do with the
21 data collected by cookies.

22 But if people don't understand how cookies
23 work, it's sort of like that's the first step, it's
24 certainly not the last step.

25 I took this idea to a board meeting of WPP

1 Group and said, "Wouldn't you like to sponsor this?" And
2 they said, horrors, no. So, then, I decided, well, I'm
3 just going to make it happen anyway. We got a little bit
4 of pushback from Jeff Chester, who's up here, and I
5 decided it would make a lot of sense to ask the Berkman
6 Center to take over and that way it was a clever ruse. I
7 avoided doing any work, and thank you very much, Berkman
8 Center.

9 MR. WEINSTEIN: Thanks, Esther. And I'd like
10 to turn it over to Jeff because, Jeff, you did express
11 some concerns about this contest, particularly in the
12 scope of the contest in terms of focusing so narrowly on
13 what I believe you considered a broader issue.

14 MR. CHESTER: Yeah, thank you very much. In
15 the first place, I want to congratulate all of the media
16 makers. They're terrific pieces of work. I'm so glad
17 that you are recognized. I hope that you are and will
18 continue to do this very important creative work. So,
19 congratulations and thank you.

20 **(Applause)**

21 MR. CHESTER: So, my criticism is not aimed at
22 you. I also want to thank Peder and the FTC and I want
23 to thank Esther and certainly Max. I had concerns about
24 this from the beginning when it was framed around
25 cookies. The problem isn't cookies and the industry

1 knows this, and in many ways, this contest fits how the
2 industry wants to frame the problem, in a very narrow,
3 technical way.

4 The industry understands in its own words the,
5 quote, "marketing and media ecosystem" that it has
6 created. It has fully implemented the one-to-one
7 marketing paradigm where a vast apparatus is now in place
8 across applications, across platforms to collect, profile
9 target and engage. That's the issue, and it's not about
10 just cookies. And I urge you, if you haven't read our
11 report, the Digital Food Report that came out in May -- I
12 cite it because, in many ways, it's the best I think
13 that's been written -- and I co-wrote it, yes.

14 **(Laughter)**

15 MR. CHESTER: But this is an area that I work
16 on and care about. It's the best that's been written --
17 I do this with my wife, Kathryn Montgomery -- that
18 describes the whole picture. It's blogs. It's the data
19 collection and the relationship that's been created on
20 blogs, on broadband, videos, through instant messaging,
21 through social networks, it's an all-encompassing system
22 that we have to address because the default is data
23 collection and targeted marketing without the consent,
24 awareness of the user to get them to engage in
25 behaviors. Maybe it's shopping, voting for a candidate

1 now and others without their awareness and consent.

2 So, I have a problem with the narrow framing.
3 None of the videos really addressed the behavioral
4 targeting issue. I don't want to take up too much time,
5 I have other comments, and I'm happy to say that I'm sure
6 I will as we get on with this.

7 But, first place, if you really want to know
8 what the industry is doing, look at the research they
9 fund which we talk about in our report. The industry
10 can't hide and say we don't know because they have spent
11 tens of millions of dollars, in particular, looking at
12 children and teens to know exactly how to target and
13 collect that data. It's fully conscious, it's there. So
14 let's be honest about it.

15 And I just also want to conclude by saying one
16 thing, the industry has set up a kind of false dichotomy
17 here. It's sort of suggesting we're anti-advertising,
18 which I'm not, but what it really is saying is, well,
19 without advertising there can't be editorial content.
20 But what we're saying is there has to be rules here,
21 safeguards for everyone to make sure that that content is
22 given to the public in a way that ensures integrity.

23 And then one final thing, which I hope I can
24 get to in the next panel, the industry also knows that it
25 is purposefully creating content, it is purposefully

1 creating landing pages, it is changing the editorial
2 content for each user in order to give them a different
3 relationship with the advertising and to facilitate the
4 data collection. It's the industry, broadly speaking,
5 that, in fact, is using editorial content to create and
6 capture all this data, and we need to make these issues
7 more visible. Thank you.

8 MR. MAGEE: Jeff, I think you made some good
9 points. Online behavioral advertising is not just about
10 cookies, but they are a part of it. And I think one of
11 the messages that came out of the videos, at least for
12 me, was that consumers have a lot of empowerment in terms
13 of being able to go on to their computer and delete
14 cookies and things if they're concerned about them. But
15 in some ways that puts a big burden on the consumers.

16 I'm not sure that -- whenever I think about
17 this, I think of my mother who is not the most computer
18 savvy as opposed to my mother-in-law who really is. But
19 my mom really just views the computer as a way to send
20 email back and forth and pictures of her granddaughter,
21 and I think the idea that she should be expected to
22 understand cookies and be able to manipulate them is a
23 little farfetched. I'm wondering if the panelists have
24 any ideas on how to make the process more transparent or
25 easier for people that aren't necessarily the most

1 technologically savvy.

2 MS. DYSON: Does your mother file taxes?

3 MR. MAGEE: I hope so.

4 **(Laughter)**

5 MR. MAGEE: I don't think I'm a dependent any
6 more either.

7 **(Laughter)**

8 MS. DYSON: It's amazing what people can learn.
9 So, I think part of consumer empowerment is giving people
10 a little credit for some intelligence. And, again, they
11 either have to have an incentive, which is if they don't
12 pay taxes they'll be put in jail, or if they watch a
13 video about cookies they'll actually be amused and
14 entertained as well as informed. Maybe this is a
15 challenge to the advertising industry to get better at
16 explaining itself or else Jeff Chester will explain them
17 for them, and they might want to do it for themselves.

18 MR. ZANEIS: I might just jump in there. I
19 think from a technical standpoint it is pretty easy. I
20 think every consumer's three clicks away from blocking
21 all cookies on their browser. So, technically it
22 couldn't be much simpler. So, I think the issue is a big
23 one of education. I can't think of anything better than
24 the FTC asking consumers to help educate other consumers,
25 which is what we're doing with this contest and future

1 contests. So, I think everybody should be applauded for
2 their participation and having that viewpoint and knowing
3 that it's really about -- consumers are empowered, they
4 just may not quite know it yet. So, what can we do to
5 get the word out there I think is key.

6 MS. COOPER: I would respectfully disagree with
7 Mike. I think that despite how simple it may seem for
8 all of us sitting in this room, I watched the five
9 finalists several times, and almost all of the
10 submissions, and it was not clear to me that any of them
11 really fully explained all the controls accurately. And
12 you saw, for example in the last video, Cookies 101, he
13 holds up his computer and he says, well, how do you
14 protect your privacy, you delete all your cookies.

15 And with the self-regulatory regime that we
16 have right now, if a consumer had opted out using the NAI
17 opt-out, that opt-out cookie that gets set, based on the
18 mechanism that we have today, would also get deleted.
19 So, not only would all your third party cookies, all your
20 first party cookies, that all of these finalists did a
21 great job of explaining, disappear, but your one choice
22 to opt out of behavioral targeting that you have right
23 now would also disappear.

24 So, I think there's certainly room to make the
25 controls easier for consumers, to make it more

1 straightforward and to not necessarily use the same
2 mechanism to track consumers to also opt them out or to
3 also give them choice. So, I think there's definitely
4 space to grow in how easy we can make the choices for
5 consumers.

6 MR. ZANEIS: If I might just clarify, I wasn't
7 talking about NAI's self-regulatory. That's a whole
8 different issue. I'm talking about a tool that's built
9 into every single browser, so every single consumer has.

10 MS. COOPER: It may be a separate issue, but I
11 think it's a big part of why we're all here to discuss
12 today.

13 MR. ZANEIS: It just shows the options that are
14 available to consumers.

15 MR. MAGEE: I think Alissa's got a good point,
16 though, the cookie paradox of going in and deleting your
17 cookies and then deleting your opt-out cookie which could
18 be very frustrating, I think, to consumers. What are the
19 options on that?

20 MS. DYSON: Well, also, it doesn't guarantee
21 you privacy to delete your cookies if you have entered
22 your email address. It will guarantee your privacy from
23 certain kinds of tracking, but it's -- just deleting your
24 cookies is a false promise if anybody says it will
25 guarantee you privacy. That was a problem with one or

1 two of the videos, which fortunately I'm not voting on
2 because I can't remember which one it was.

3 MS. COOPER: Well, I think only given two
4 minutes, it's probably impossible to -- we didn't only
5 ask you to talk about how you can delete, how you can
6 manage your cookies, the questions were, what is a cookie
7 and -- you know, far too much information to provide in
8 two minutes. So, it's a challenge.

9 MR. PEGORARO: Yeah, one of the things I often
10 hear from readers, there's a lot of folks out there who
11 have this sort of single-mined focus on cookies. On the
12 one hand they forget that there are many other things
13 they should be worrying about in the Internet in terms of
14 their security of their computer, which in turn means
15 their privacy. If you get hit by spyware, who cares how
16 many cookies you've accepted, you have far more problems
17 to worry about.

18 On the other hand, there's this thing called
19 the rest of your life where you might use a credit card
20 or use a loyalty card at a supermarket and that will put
21 out far more data exhaust than any amount of cookies you
22 could possibly pick up browsing the web for years on end.

23 MR. MAGEE: Lorrie, it looks like you have a
24 comment on that.

25 MS. CRANOR: Yes, a few comments on a few

1 things. I agree that cookies are actually a relatively
2 minor part of the problem. They are part of it, but
3 there's a lot more out there. Also, as far as how do we
4 get the message out to the public or what do we need to
5 do, I think these educational videos are good, but I
6 think we really also need to look to the tools that users
7 have built into their web browsers. I think those tools
8 have really come a very, very long way from Version 2 of
9 the web browsers. However, they're still not completely
10 where they need to be.

11 I think if you actually look at, for example,
12 it was shown -- I believe the IE 6 or IE 7 cookie
13 controls and if you actually read the text next to that
14 slider bar for high, medium, low, it's nearly impossible
15 for most people to understand what it means. Now, that
16 said, the default setting in Internet Explorer arguably
17 is actually a reasonable choice for a lot of people
18 because, by default, it's actually blocking a lot of
19 third party cookies when there's no opt out available to
20 data sharing. And by making that a default setting
21 Microsoft actually kind of set a bar.

22 Now, we could argue as to whether they set the
23 bar in the right place, but there's a lot of power in how
24 we set the default settings in our browsers.

25 MR. MAGEE: Jeff, do you have a comment? I see

1 your hand up.

2 MR. CHESTER: Yes. I don't think it's fair to
3 place it on the user. We want to work with industry here
4 in the United States and we started to work in the EC as
5 well to try to address these concerns. But it is the
6 entire system. All you have to do is read the report
7 that I referred to yesterday, which is just one of dozens
8 of these things. The first IAB AAAA report, HD
9 Marketing 2010, most of you probably are members so
10 you've gotten it already, Sharpening the Conversation, it
11 just lays out the entire scope of it and how it all
12 interacts and how marketers -- and I think it's so
13 interesting, Esther, I want to blog this -- that WPP,
14 which now owns 24/7, didn't want to fund this.

15 They know what they're doing in terms of the
16 design. We need to approach this in a holistic way and I
17 just want to underscore, in particular, that we are
18 talking about a system that is especially attuned to you
19 here in the United States and elsewhere. And as trite as
20 it might sound, these are the emerging citizens. We have
21 to make sure that this space supports and nurtures them,
22 provides for the autonomy, helps them grow as active
23 members of our society. And to have a interactive media
24 environment designed wherever they go to collect and
25 target and direct them is incredibly unfair.

1 MR. MAGEE: Let's maybe talk about some of what
2 we liked about the various videos. I mean, I thought
3 they were all fantastic. One of them, I think it might
4 have been Aaron's video, seemed to say that there's a way
5 that your cookies could get intercepted and maybe I'm
6 misreading that, but is that possible? When someone is
7 online, can their cookies be hijacked?

8 MS. DYSON: They can, but so can your password
9 and your financial information which is much more
10 dangerous than your cookie being hijacked. It all goes
11 down to, especially if you're using a WiFi connection,
12 your stuff may be in the clear. So, I think your cookies
13 are probably the least problem you have, but they
14 certainly can be hijacked.

15 He was also a bit glib when he said, it's a bad
16 implementation to put a Social Security number in a
17 cookie. It's a disaster.

18 **(Laughter)**

19 MR. ZANEIS: I think that's really the key is
20 what kind of information is in the cookie. By and large,
21 they're just anonymous random numbers and letters and
22 such. The scary guy in the corner, the shady guy in the
23 corner, I think, was what he talked about. But to your
24 credit, you also talked about they're not really a data
25 security problem in and of themselves and they don't

1 deliver viruses, which I think was key to that video. I
2 thought it was well-balanced there.

3 MR. WEINSTEIN: Let's stay on that theme for a
4 minute and talk more about why cookies are there in the
5 first place, a little bit about what are the good things
6 that are coming out of cookies that make users actually
7 want to have that particular technology and tool
8 available to them. Certainly, the videos illustrated
9 several of these.

10 MR. PEGORARO: I really liked the analogy. I
11 think the first and the fifth used virtual postcards,
12 Post-It notes, which sort of get across the fact that
13 cookies -- a lot of websites need them to function. I
14 remember reading somebody's blog a while back which said,
15 if the inventor of the cookie format had just called it
16 website preference or something innocuous, no one would
17 be wiggled out about it. Instead, you have this cutsie
18 name and people have gotten to think that cookies are a
19 form of spyware, which they're not a form of any sort of
20 ware. They're just an inert file on your hard drive.

21 MR. CHESTER: Look, I mean, it's not too long
22 ago, even though it goes back to '93, '94 in the history
23 of it, they were created purposefully to advance the role
24 that advertising could play -- I mean, Netscape did it --
25 in the online environment. So, personalization is one

1 thing, but it has, from the very beginning, been a part
2 of implementing what they call the one-to-one paradigm,
3 the fact that they can -- the goal of interactive
4 marketing is to know so much about each and every one of
5 us that it can then engage us in very deep ways. I don't
6 have to tell you guys because you're doing it. I don't
7 know how many non-industry people are here.

8 So, that's really the primary role of cookies
9 and the associated data collection applications like
10 pixels and web-bugs that have evolved.

11 MS. CRANOR: Well, that's how cookies are
12 being used now, but I don't think that's how they were
13 originally invented. They were originally invented as a
14 state management mechanism is the computer science term.
15 And there's actually a really nice paper by the people
16 who invented them in the IETF that talks about the
17 history and how basically the first year that they were
18 out there, they were using them so they could actually
19 make the web work, and then somebody discovered, this is
20 great for advertising and they felt like, oh, my gosh,
21 this thing is out of our control and there's nothing we
22 can do about it now.

23 MS. DYSON: Yeah, the advertisers had no idea
24 what cookies were when cookies were being made first.

25 MR. CHESTER: By the way, that's not the total

1 history here. And if you go back to Netscape and the
2 role of Netscape in helping create the cookie, it was
3 clearly the advertising was in mind, and I refer people,
4 I'll plug my book, I'll refer people to my book, Digital
5 Destiny, which came out earlier this year. I have a
6 whole chapter on the history of the interactive marketing
7 system, including the origination of the cookies for
8 commercial purposes.

9 MR. MAGEE: Tikva.

10 MS. MOROWATI: Hi, guys. I first want to tell
11 you all who I am. I used to be a film maker and this
12 whole space is not even two years old to me. I went
13 through an international telecommunications program at
14 NYU, which many of you might know about. Anyways, I'm
15 telling you that because I see myself somewhere between
16 you and the customers. And we've already gotten to the
17 discussion about different age groups and places that
18 people are at, a customer, there's lots of different
19 kinds of customers.

20 Anyway, because you had asked a question,
21 Peder, one of your first questions was about your mom,
22 what can we do about your mom and these kinds of things.
23 What I see valuable in having this conversation and in
24 this competition really is about -- especially in the
25 scope of this conference is that we're really in touch

1 with where the users are coming from. It's really
2 interesting. Like every single one of the videos,
3 there's an inaccuracy about the way that cookies work,
4 and that's interesting, I think.

5 And I think the key is not -- in this panel,
6 we're not talking about really the regulatory aspects
7 like we are in the rest of the conference. Rather, we're
8 just taking a look at the reality of where people are at
9 and educating people about how they can empower
10 themselves. I think it's true there's potential, the
11 potential is there for empowerment, but I just don't
12 think it is there. I think people are pretty head in the
13 sand, butt in the air about their privacy.

14 MR. MAGEE: Well, I think the idea of using
15 videos like this just from consumers and having them sort
16 of self-educate is a really interesting one. Maybe we
17 can talk about other contexts in which this could work.
18 But, also, Max, what sort of response did YouTube get?
19 Like how many people looked at these and what were the
20 comments that were posted? Did the public find them
21 interesting?

22 MR. WEINSTEIN: It's a good question. I'm not
23 sure we have a great answer for you right now. When we
24 publicized this contest, it was on fairly short notice.
25 Esther gave us a little bit of a short time frame and we

1 actually were really pleased with the results in spite of
2 that.

3 MS. DYSON: And your lawyer spent a little
4 while --

5 MR. WEINSTEIN: And our lawyer spent a long
6 time coming up with all the terms and conditions and all
7 the fun stuff that goes along with having a contest as
8 well, for sure.

9 But the result of that is I think the word may
10 have gone out a bit more to the people who were
11 interested in creating the videos than the people who are
12 the audience for seeing the videos. What we're hoping is
13 that now that we have some finalists, after today we'll
14 have a grand prize winner; YouTube is actually, I
15 believe, going to be adding these finalist videos to that
16 privacy channel that the woman from Google mentioned
17 earlier.

18 So, we're going to get some more exposure out
19 there to get this information out to consumers.

20 What I would add is that I think the value
21 probably comes from seeing all five of them, if not all
22 24 of the ones that were originally submitted. Because
23 even if there is an inaccuracy here or there, I think
24 there's a lot of good content, and when you view them
25 collectively you probably get the best big picture view

1 of what this thing is really all about.

2 MR. CHESTER: But I do think it behooves
3 Berkman to bring in other partners that are unaffiliated
4 with the industry. I mean, I know you -- Google is a
5 funder of your program and Google paid for some of the
6 expenses here. And I think it's very important that we
7 have a lot more public participation, which we're going
8 to encourage in all of this because young people really
9 do need to make a statement and we will be encouraging
10 them to do that about this ecosystem.

11 But as we have so-called privacy channels, it
12 is incumbent upon the people that organized them to
13 ensure that there is a broad array of perspectives, that
14 there's an honest discussion on that channel that is
15 prominently made visible on the home page, so it's not
16 just a kind of narrow definition of the problem.

17 MR. WEINSTEIN: Sure. Mike, an industry
18 response?

19 MR. ZANEIS: I'd like to thank Jeff for
20 pointing out the fact that it actually is a partnership
21 between the consumers and the businesses. Somebody needs
22 to provide the platform for the user-generated content.
23 We're not talking about industry having any sort of
24 editorial control over this. It just makes the point
25 that because of the ad-supported Internet, it empowers

1 consumers to go out and do things like this. So, but for
2 that advertising, you don't have the platform to do it.

3 MS. DYSON: Frankly, I was expecting a lot more
4 negative videos that -- you know, weird people in the
5 corner sniffing around and so forth. And I thought that
6 would have led to a better discussion, somewhat along the
7 lines of what Jeff was talking about. With luck, those
8 will show up. People should understand what happens when
9 things go wrong, and that will enable them to protect
10 themselves better.

11 This was vis-a-vis Lorrie's comments much
12 earlier. I think people pay some attention to a privacy
13 statement, but let's face it, they pay a lot more
14 attention to who the website is. You probably haven't
15 bothered to read American Express' privacy statement. If
16 you go to some little website that offers a great deal on
17 something, you may be much more likely to be concerned
18 and you probably shouldn't believe their privacy
19 statement anyway. So, it's a very large and complicated
20 thing.

21 MR. MAGEE: It's hard to judge whose tent is
22 up, but there's one down there.

23 MR. CHESTER: It's me. I want to just respond
24 for a second to Mike and the ad-supported Internet and I
25 think Kathryn said this yesterday. I had to leave.

1 Look, the Internet is more than just the ad-supported
2 system. I agree we have to have the monetization machine
3 and it is advertising. Right? I think it has to be
4 responsible advertising which includes good privacy, but
5 the Internet serves more than just a forum for ads.
6 Indeed, YouTube, in a way, was kind of envisioned in part
7 as a kind of public forum and the web really developed in
8 a way as a public forum and it remains a public forum.
9 It is, in fact, where our democracy, the digital media
10 system, rests, and not all of digital democracy should be
11 advertiser-supported.

12 We have to have spaces and places and practices
13 and policies where we can have this debate without it
14 being funded and for industry so as to tout, well,
15 without the advertisements, there goes democracy. That's
16 not the way it should work.

17 MS. DYSON: So, will you fund it with the
18 profits from your book or how will it get funded?

19 **(Laughter)**

20 MR. CHESTER: Well, to be honest with you, we
21 have funded a tremendous amount of work on this topic,
22 including a report we released yesterday. Tens of
23 thousands of dollars we have funded, including the report
24 last year we filed, including my book. There have to be
25 policies and rules and, frankly, some greater willingness

1 on the part of industry to make the contributions
2 necessary so there can be a vital set of spaces in the
3 digital media that promotes citizenship and civic
4 expression without it having to be ad-supported.

5 MR. WEINSTEIN: I want to focus a little bit on
6 the technology piece and ask what is the right way for
7 consumers to protect their privacy within the narrow
8 context of cookies? We have seen suggestions in the
9 videos that range from choosing to accept each cookie
10 individually to deleting all your cookies after the fact
11 to refusing to accept cookies in the first place,
12 refusing to accept third party cookies. That's a lot of
13 options. Which one is the right one?

14 MR. PEGORARO: I'm a fan of the block third
15 party cookies approach, which may not be good since our
16 website, Washingtonpost.com, has quite a few of them.

17 **(Laughter)**

18 MR. PEGORARO: I think that is the simplest way
19 overall. You don't suffer the real hit to just the
20 utility of the web by having to look at every single
21 cookie. If you do that, it's a mind-numbing task. You
22 might as well not go on the web at all.

23 Trying to track the reputation of individual
24 advertising networks, do I trust DoubleClick? How about
25 this other one that, how about this other one, that

1 requires a lot of research that I don't have time to do
2 and I'm sort of paid to do that. It also has the
3 advantage -- a lot of web browsers are already set up to
4 block most or all third party cookies. Apple Safari, for
5 instance, blocks them by default. Firefox used to let
6 you click to block third party cookies and for some
7 reason they took it out in Firefox 2. It's not too hard
8 to do in Internet Explorer 7 either.

9 MR. MAGEE: Speaking of the alternatives, the
10 protagonist in the video "Cookies 101" noted some
11 alternatives to cookies, but he spoke pretty quickly at
12 the end and I didn't catch them. What are the
13 alternatives? And what are the pros and cons of those?
14 Lorrie?

15 MS. CRANOR: I listened to that ending a few
16 times to try to understand it. I actually played all
17 these videos in my class on Tuesday. I teach a privacy
18 class at Carnegie Mellon, and we had a big discussion
19 about that. Some of the alternatives are actually
20 alternatives that I'm not sure they're really any better.
21 They're different than cookies, but I'm not sure, from a
22 privacy perspective, that we really want to encourage
23 people to do that, and they may even be worse because
24 there are fewer control for the consumers to do those.

25 MR. MAGEE: What are they? What are you

1 referring to?

2 MS. CRANOR: By using other mechanisms that
3 essentially still tag you but not through the cookie
4 mechanism. I think there was something about watching
5 your IP address was in there, and there are a number of
6 mechanisms where you can effectively put a cookie on a
7 user's computer but it's not in the cookie folder. So,
8 when you delete your cookies, it won't get deleted.

9 MS. DYSON: And, of course, those are not at
10 the consumer's option. So, it's kind of like that's what
11 advertisers can do, but it's not what consumers can do.

12 MS. COOPER: Or if they are at the consumer's
13 option then the control is just impossible to find or not
14 very clear.

15 I wanted to respond to your previous question
16 about what's the best way and, obviously, Rob deals with
17 everyday consumers all the time, so he has that
18 perspective. But I think the real answer is it depends.
19 Right? So, as we talked about this sort of false paradox
20 of having ad-supported free content or paying for the
21 content and not having ads, if you're someone who likes
22 getting relevant ads, then maybe your choice is going to
23 be different than someone who is more concerned about
24 their privacy.

25 So, I think the answer is -- and you can see

1 the diversity of answers given across all 24 videos -- is
2 it really depends on the consumer and what the consumer
3 wants to be able to do and also probably the level of
4 tech savviness of the consumer, although it would be nice
5 if that wasn't such a factor and the controls were easier
6 so that if you chose that you wanted to be really privacy
7 protected, it could be one click instead of three or five
8 or ten or however many it maybe.

9 MR. ZANEIS: I think that's right. I would
10 characterize it a little bit differently. We're talking
11 about how you protect yourself. I think that's a little
12 bit of a false promise than cookies make you more
13 unprotected. I'm not sure that's right. I think it's an
14 intimately personal decision, and the wonderful thing is
15 that you have a number of choices as a consumer on what
16 that level is and everybody gets to make that decision.
17 I think that's the right way to do this, right?

18 We're going to have a self-regulatory panel
19 next. I think the best form of self-regulation is when a
20 consumer regulates themselves and has the empowerment to
21 do that. So, I think that's where we're at with cookies.

22 MR. WEINSTEIN: I suspect Jeff would disagree,
23 but I'm not putting words in your mouth, Jeff.

24 **(Laughter)**

25 MR. CHESTER: No, no, I do think this is, in

1 part, a privacy issue, but it's not a privacy issue. But
2 I do want to sort of underscore it. The fact that the
3 ecosystem, as they call it, has been designed to track us
4 through a variety of ways to determine what content
5 drives users to engage, relate to the brand product
6 marketing sell has profound implications for the quality
7 and diversity of editorial content because, indeed, the
8 industry wants to fund content that it knows it drives
9 user behavior.

10 So, to the extent that we are also concerned
11 about having a healthy online medium that fully funds
12 news, public affairs, civic content, investigative
13 reporting, holds institutions such as mine and Esther's
14 accountable. This issue of the metering is directly tied
15 to what happens with that content brought to us by
16 advertisers.

17 MR. MAGEE: Esther, if you've got one more
18 maybe to finish up and then I think what we're going to
19 do is do our vote and the judges are going to, with Max,
20 come up with their winner and then I'm going to, with our
21 counters, get a public vote.

22 MS. DYSON: I just wanted to respond to Jeff's
23 comment by bringing in a third party, which is you have
24 advertisers and funders on the one side and the poor
25 consumers on the other who are no longer getting what

1 they want. But there's one thing the Internet has
2 enabled and, to a large extent, it's being funded by
3 Google's AdWords, is the tremendous rise of personal
4 publishing. People who aren't trying to maximize their
5 ad revenues, though some of them can still help fund
6 their lives through AdWords who are writing about
7 whatever it is they please. I'm talking primarily about
8 the blog-o-sphere, the profusion of content that is
9 created not for money but for self-expression or
10 sometimes for marketing your carpentry business or
11 whatever.

12 But it's exciting and it's exactly what you
13 wanted. It's not funded by a public interest group,
14 whatever its goals are, it's not funded by large media,
15 it's funded by individuals who have something to say.
16 That's probably the best antidote to all this.

17 MR. ZANEIS: Twelve million Americans have
18 blogs. That's 8 percent of the population. That's a
19 pretty powerful statement. I couldn't agree more.

20 MR. MAGEE: Does anyone in the audience have
21 questions about any --

22 MR. CHESTER: Can I just respond for one second
23 or are we out of time? But I do want to sort of
24 underscore that the interactive advertising system put in
25 place is going to have an impact. Yes, there's a long

1 tail, but it's going to have an impact on the funding and
2 diversity of content. Already advertisers on blogs,
3 including the company that Google bought, Feedster, they
4 can start blacklisting. You can start blacklisting
5 blogs.

6 I'm just suggesting to you, Esther, we need to
7 look at these issues very carefully and have a larger
8 public debate. There's no easy answer here necessarily.

9 MR. MAGEE: There's never any easy answer. Do
10 we have questions from anyone in the audience?

11 MS. DYSON: For the creators as well as for the
12 panelists.

13 UNIDENTIFIED FEMALE: I would love to hear from
14 the creators a little bit. I don't know if you could
15 describe in a minute or so just the thought process that
16 went into your work and really -- exactly, how did you
17 think about this?

18 MR. CHESTER: They should come up here, I
19 think. Come on up.

20 **(Applause)**

21 MS. DYSON: Did you do it just for the money?

22 **(Laughter)**

23 MR. MAGEE: Just go ahead and jump in.

24 MR. SCHAACK: I did "Got Cookies", along with
25 Kristin here. Our thought process behind it is we kind

1 of were going off the idea of like grandmas, grandpas,
2 you know, people that just have no idea what a cookie is.
3 They watch the nightly news and they hear oh, cookies,
4 those are bad things. And when you do the research, it's
5 not necessarily so. And that, you know, they weren't
6 necessarily created for bad things, but like most things,
7 things can be exploited and used in a negative way.

8 MS. SCHAACK: So, we just wanted to sort of
9 break it down and have a simplistic way to explain it
10 creatively so the masses would be able to understand at
11 least the basics of what cookies are and how they're used
12 or misused.

13 MR. WELCH: Mine was pretty much the same
14 thing, keeping it simple. Of course, the humor was one
15 part. One of the things I found that was interesting,
16 Aaron and I talked about this, was through the editorial
17 process of getting it down to two minutes, we ended up
18 cutting a lot of things that we've heard are concerns
19 from you guys.

20 So, it was really funny how as consumers we
21 were worried about what the content of our videos ended
22 up showing whereas you guys were concerned about
23 completely other things.

24 **(Laughter) (Applause)**

25 MR. WELCH: I know that even in my video you

1 talked about the options I had at the very end, the
2 reason why they're really fast is I needed it under two
3 minutes.

4 **(Laughter)**

5 MR. WELCH: And then I realized, holy cow, I
6 just dumped out all these words and now I've got to
7 explain this and that's a whole seven other minutes of
8 explanation. The two minutes was enormous difficulty and
9 the scope of just -- we should have just left it with
10 what is a cookie and then dealt with all the other stuff
11 first. But, yeah, it was just mainly to keep it simple.

12 MR. PAYNTER: I'm online here with Madame Levy
13 in France and she said she was trying to answer the six
14 questions that they posed on the Berkman site in two
15 minutes or less. But I can also say that for her and her
16 daughters, this kind of work is as much about art as it
17 is about technology. And those kids that she brought in
18 to play on it are part of that generation to whom this is
19 all simple and they were born and raised with this
20 technology.

21 MR. SURING: Yeah, as I have been here for the
22 past couple of days listening to all this, there was a
23 lot of stuff I left out that seems more relevant to your
24 discussion here and I kind of wish I had left it in. But
25 we started more like a level past like the most basic.

1 We figured people knew what a browser was and it's more
2 extending past that and trying to get as much information
3 as we could in there. It was hard to do.

4 MR. MILLER: I think one of the central things
5 in mine was that I wanted to recognize there's definitely
6 a diversity, as has been mentioned, a diversity out there
7 of individual -- I mean, I would say comfort levels,
8 thresholds, of what individuals feel is how much
9 information they want to share with different
10 organizations. And so, yeah, kind of one thing that I
11 tried to hone in on is that these are not necessarily
12 bad, they can be bad for some people, good for other
13 people depending on how they related to the companies
14 involved.

15 MR. MAGEE: That's great. I think we should --
16 this really felt like a town hall. I think we should go
17 ahead and we'll do our audience vote and the judges will
18 do theirs.

19 **(Brief pause)**

20 MR. MAGEE: All right. If this section could
21 just on a show of hands what was your favorite video?
22 Video number 1 was the one with the great animation.
23 Video 2 was the young girl. Video 3 was the man with the
24 plate of cookies. Okay, we're going to vote.

25 UNIDENTIFIED FEMALE: I don't think the

1 audience over here is --

2 MR. MAGEE: I'm just going to do it section by
3 section. We'll go across. All right, I'm sorry. That's
4 what I'm going to do. I'm going to go through all five.
5 The man with the plate of cookies is video 3. Video 4
6 was Aaron's, the one we showed twice, and video 5 was Tim
7 Welch sitting on the couch with the Post-It notes.

8 So, who votes for video 1? Okay. Who has got
9 video 2? Video 3? Keep them up for a second, please.
10 And video 4? Okay. Video 5, Post-It notes?

11 All right. If we could get the middle of the
12 room to do it. Who votes for video number 1? This is
13 just this section right here. Video number 2?

14 UNIDENTIFIED FEMALE: Can you repeat the
15 videos?

16 MR. MAGEE: I'm sorry. Video number 1 was the
17 animation. Video number 2 was the little girl. Video
18 number 3 was the man with the plate of cookies. Video 4
19 is the one we showed twice. Video 5 was the Post-It
20 note.

21 So video number 1? Video number 2? Video
22 number 3? Video number 4? And video number 5?

23 Do you need me to repeat them again? Okay.
24 Who votes for video number 1? All right. Video number
25 2? Video number 3? How about video number 4? And video

1 number 5?

2 So, we're going to give them a moment to
3 compile the audience choice here.

4 **(Brief pause)**

5 MR. MAGEE: I'm just going to announce the
6 public's choice. We wanted the public to weigh in on
7 which one they liked best. The Berkman Center has got
8 its own prize and the judges have voted for theirs. So,
9 this is just for our internal purposes here. Public voted
10 number 3 was the winner.

11 **(Applause)**

12 MR. MAGEE: Cookies 101. The fifth video was
13 second.

14 **(Applause)**

15 MR. MAGEE: And the first and Aaron's, the
16 fourth, were tied for 3rd. And I just wanted to thank
17 all the creators. They were all fantastic.

18 **(Applause)**

19 MR. MAGEE: So I'm going to ask Erica to bring
20 up the plaque for our grand prize winner. I did not
21 mention in the introduction, but it should be made clear
22 that the panelists, in addition to the great job they did
23 discussing the videos, actually has a very important role
24 in choosing the grand prize winner which, thanks to our
25 sponsors, is actually \$5,000 that they're going to get in

1 addition to the pride and joy of winning. So, we're very
2 excited about it.

3 It was actually a pretty close vote, but our
4 winner is Clayton Miller for the first video, Cookies.

5

6 **(Applause)**

7 MR. MAGEE: Congratulations and thanks,
8 everybody.

9 Just a quick announcement. We're going to take
10 our lunch break now. There's information about
11 restaurants in the area out at the front desk where you
12 checked in. We're going to start again promptly at 2:00,
13 and please remember that you got to go through security.
14 So, give yourself a couple of extra minutes. Enjoy your
15 lunch and we'll see you back at 2:00.

16 **(A lunch recess was taken.)**

17

18

19

20

21

22

23

24

25

AFTERNOON SESSION**SESSION 8: THE REGULATORY AND SELF-REGULATORY LANGUAGE**

1
2
3 MS. RICH: Welcome to Panel 8. We've still got
4 a lot of people here, which is great for a Friday
5 afternoon. I'm very happy to see everybody. I'm Jessica
6 Rich of the FTC and this is Stacey Brandenburg, and we're
7 your moderators and we'll be introducing everyone
8 shortly.

9 Our hope is that this is the panel where many
10 of the issues we have been discussing over the last
11 couple of days are going to come together and
12 everything's going to be crystal clear. As you know,
13 we've laid out a lot of the issues raised by behavioral
14 advertising in this whole event, and now, we want to
15 focus on the question of what standards govern or should
16 govern the practice.

17 In this panel, we're going to discuss the
18 existing standards and both self-regulatory and legal
19 models for managing privacy issues in this area, as well
20 as I hope new ones that are being developed as we speak,
21 the limits and merits of the various approaches and any
22 next steps as these models are being developed.

23 There are, of course, different ways, as we've
24 discussed, to approach privacy issues in this area and
25 what standards should govern. We have talked a lot about

1 many models that build on the notice and choice
2 structure, and we heard earlier today that that has a lot
3 of challenges and proponents and opponents.

4 Others take a more harm-based approach, for
5 example, prohibiting certain practices that are viewed as
6 harmful, or rather certain uses of data that are likely
7 to lead to harm. And I'm hoping that in this panel we
8 can explore perhaps some models that might be based on
9 that.

10 But we're going to begin today with three
11 panelists that represent different perspectives in this
12 area. Then we'll move to a roundtable discussion and,
13 again, not a round table so it's a challenge here. And,
14 hopefully, we have some audience questions in the end as
15 we have had throughout the day.

16 First, Trevor Hughes of the Network Advertising
17 Initiative is here to discuss the NAI principles. Then
18 we're going to have Pam Dixon of the World Privacy Forum
19 here to represent the consumer perspective, and I think
20 she's got a recent study she just did, which I haven't
21 had a chance to read.

22 Did you release it this morning? Yes? I'm
23 looking forward to reading it.

24 And, finally, we'll hear from Reijo Aarnio,
25 Data Protection Ombudsman of Finland on how the EU's

1 legal framework applies to these practices. We had a
2 little bit of a discussion about it yesterday. We'll
3 hear more.

4 So take it away, Trevor.

5 MR. HUGHES: I want to thank you all for coming
6 to this roast of the NAI.

7 **(Laughter)**

8 MR. HUGHES: If only that weren't so true.

9 I actually am here today to talk to you about
10 the NAI principles, and broader than the NAI principles,
11 the layers of protections that I described yesterday in
12 my speech yesterday. Because I think that there are
13 layers of protections and I think the NAI principles are
14 a part, small part, big part, a part of those layers of
15 protections and I think when we talk about self-
16 regulation, certainly I'm here to represent the Network
17 Advertising Initiative and I'll share that with you. But
18 we can't miss the big picture of all of the things that
19 happen in the online space.

20 So, let's start. I want to make sure that you
21 all are aware, and as we talked about before, probably
22 the broadest layer of protection today in the online
23 space is the layer of privacy policies that we have
24 worked so hard over the past 10, 12, maybe 15 years to
25 try and put in place. And while there are always

1 companies, always organizations, always websites that
2 we'd like to have posting privacy policies, privacy
3 policies do exist, and we have been telling the
4 marketplace for a long time to post privacy policies.

5 They are up there, I know that there will
6 always be issues with regards to readability and consumer
7 engagement. But I think Marty Abrams' comments were
8 notable earlier today that privacy policies have not only
9 been a vehicle for notice, but they are an incredible
10 vehicle for accountability because organizations take on
11 significant responsibility by posting those privacy
12 policies.

13 We also talked extensively about browser
14 control. The last panel was a great exploration of the
15 various controls that exist with regards to cookies. And
16 we certainly have the opportunity to talk about other
17 state management tools, but I want to make sure that we
18 don't miss the fact that there are many, many, many
19 controls available to consumers, most of them within just
20 two or three clicks and regardless of which browser you
21 are in, you have the ability to block, delete, in some
22 cases, manage first versus third party cookies. You have
23 the ability to do a lot of things.

24 I also want to point out that there is in the
25 primary browser in the marketplace today, which is IE 6

1 or 7, Internet Explorer 6 or 7, the ability for consumers
2 to really determine what their own public policy posture
3 is with regards to many of the issues that we have been
4 discussing.

5 If I'm a privacy complacent as Larry described
6 it, I may decide to accept all cookies. If I'm a privacy
7 pragmatic, I may decide to set an opt-in or opt-out for
8 cookies on my system. I may decide to segment between
9 first or third party cookies. If I'm very, very
10 concerned about privacy, I can block them all or I can
11 block just third party cookies.

12 I think it's also notable that in the default
13 setting, which is the setting that generally stays in
14 place for the majority of consumers, Microsoft blocks
15 third party cookies that do not have a P3P statement
16 attached. So, if you don't have a privacy statement
17 associated with your third party cookie, you're blocked
18 in 75 percent of the browsers around the world.

19 More than that in Safari, another major
20 browser, third party cookies are blocked in the default
21 setting. So, behavioral targeting is essentially not
22 happening in those browsers because Safari is blocking
23 those third party cookies basically preventing any
24 behavioral targeting from occurring.

25 So, consumers have control. Now, certainly,

1 certainly, certainly, industry, the advocacy community,
2 the FTC, all of us could be doing a better job at
3 educating consumers about the availability of these
4 controls. But let's not forget for one second that these
5 controls are very strong and they're there and they're
6 available for use.

7 I also want to make sure that I mention some of
8 the other tools that are available. Anti-spyware
9 software, anti-malware programs, many of them have
10 privacy control features. There are also privacy
11 protecting software. Privacy enabling type technologies
12 that we have seen many, many iterations of.

13 We have seen web seals and certifications.
14 TRUSTe is a great example. Colin O'Malley spoke on the
15 last panel. I think it's notable how many sites TRUSTe
16 has certified in today's marketplace. These are agents
17 of trust and they are valuable to all of us in the layers
18 of controls that we have.

19 But what I want to spend the most of my time on
20 is the NAI principles. The Network Advertising
21 Initiative was formed some seven years ago, and it was
22 formed really in the caldron of concern surrounding what
23 we called profiling back then, what we call behavioral
24 targeting today. Formed originally with seven or eight
25 companies, and soon after the formation of the NAI, the

1 dot-com economy really deflated and membership dropped
2 pretty precipitously at that time.

3 I want to share with you, though, that the NAI
4 is built on many of the fundamental principles that we
5 have talked about over the past two days. Notably, it is
6 built on the concept that consumers deserve notice and
7 they need to have the ability to exercise choice with
8 regards to the practices of NAI members.

9 I do need to mention to you, though, that the
10 NAI principles are built for a very specific function.
11 That's something that we call online preference
12 marketing. So, the NAI is not a silver bullet for the
13 entire online advertising industry. It is not a one-
14 size-fits-all solution for every single practice that
15 exists. But for those companies that are engaged in
16 online preference marketing, as it's defined in the NAI
17 principles, which is basically the gathering of data
18 across a broad network of websites for the purposes of
19 aggregating a profile so that that profile can be
20 targeted back. It certainly is and has been working.

21 We also have layers of controls. So, the
22 amount of notice, the level of choice increases with the
23 amount of personal data that you're using in the NAI
24 principles.

25 Further, we have special protections for

1 personal data associated with sensitive consumer
2 characteristics.

3 I want to show you how it works. The NAI
4 principles required that notice be provided on websites
5 that are using the services of NAI members. This occurs
6 in one of two ways, it occurs where a link is provided
7 back to that NAI member or back to the NAI gateway site.

8 We've talked about the Washington Post over the
9 past couple of days, here is their notice. I'm two or
10 three slides away. So, if I can just sneak through.
11 Thanks.

12 So, this is notice on the Washington Post with
13 regards to NAI practices from our member companies. We
14 also have some companies, weather.com was mentioned
15 previously as well. Here is a link back to the NAI
16 Global Gateway site. When a user reviews the privacy
17 policy in that site and clicks through -- and based on
18 our understanding, there are over 20,000 references to
19 the NAI opt-out page out across the web, so over 20,000
20 places where this link appears.

21 A consumer clicks through, they come to this
22 page. We tried to make the opt-out very noticeable, it's
23 a big red button right there. If you click on consumer
24 opt-out, you're presented a page where you are told
25 whether you have an active or have no active cookie from

1 the various NAI members. You have the ability to opt out
2 of one, two, three, all of the NAI members. You click on
3 submit and you're presented with a page that tells you
4 whether your opt-out was successful or not.

5 Now, this is technology. The vagaries of
6 browser settings, of the various types of operating
7 systems, of connections between all of these different
8 systems can sometimes result in a failure of the opt-out.
9 Well, you're told that, too.

10 When an opt-out fails, we have information
11 right below that tells you what you can do as a next step
12 to try and ensure that the opt-out is effective. We have
13 an extensive set of FAQs. And if all of those things
14 don't work, we have the ability to talk to the NAI as a
15 self-regulatory organization.

16 Over the past two years, we have averaged
17 between 600 and 700 in-bound support requests, and of
18 those, we find that about 70 last year and about 70 so
19 far this year actually turn into complaints where
20 functionality doesn't seem to be working. We have been
21 able to resolve those with the consumer, either it's an
22 issue of their side, they're blocking cookies, their
23 spyware is set to block cookies, in some way they're not
24 set up to accept the opt-out cookie served by our member,
25 or, alternatively, one of our members has a glitch

1 somehow in their opt-out cookie serving at that point in
2 time. We have successfully resolved all of those
3 concerns and we focus heavily on complaints and
4 functionality for NAI members.

5 I do want to close, though, by saying that the
6 NAI was formed at a time when this issue was very hot,
7 and we have not been complacent nor silent over the past
8 six years. In fact, as the behavioral targeting world
9 sort of came apart during the dot-com crash, we turned
10 our attention to other efforts. We worked
11 collaboratively with many of the advocacy organizations
12 here on web beacon guidelines, best practices for the use
13 of web beacons.

14 We worked extensively on the trusted download
15 program in the adware and spyware debate. We worked
16 extensively in the email industry to try and promote best
17 practices in that industry and heavily promote it through
18 the use of email authentication.

19 Now, with a number of mergers and some
20 constructive criticism from our advocacy friends, the
21 time is, again, appropriate for us to review and look at
22 the NAI principles. And I'm happy to report today -- we
23 actually weren't intending to release a document today --
24 but we have been working for the better part of the last
25 year on essentially a plug-in or a set of best practices

1 for the NAI principles related to the use of sensitive
2 consumer characteristics in non-personal behavioral
3 targeting. That has obviously been a hot issue over the
4 past couple of days, and we look forward to engaging with
5 many of the stakeholders on that issue in the weeks and
6 months ahead.

7 I do want to close --

8 MS. BRANDENBURG: That's what we look forward
9 to doing, Trevor. I don't mean to cut you off, but we
10 need to allow everybody an opportunity to speak. Thank
11 you.

12 MR. HUGHES: Thank you.

13 MS. DIXON: First off, thank you for inviting
14 me and thank you, FTC, for holding this really important
15 meeting. I think Trevor got it just right. This is the
16 time for this meeting. We looked at these things a long
17 time ago and things have changed and I think he set it up
18 beautifully.

19 So, I'm really focused on the actual NAI body
20 and agreement. I think we've got to take a look at that.
21 And I'm very interested in just focusing on that for
22 approximately five to six minutes and just discussing
23 what we've really seen about the past history, of what we
24 know now about the NAI and its current operations.

25 So, the World Privacy Forum is actually a

1 public interest research group. We're a bunch of
2 researchers. We actually don't lobby or do legislation,
3 so we're not advocates, we're researchers. So, I just
4 want to point that out.

5 We released a report today and, basically, the
6 report is a look, it's an analysis of the NAI today. So,
7 I want to discuss a few things and just talk about those
8 and see if we can't learn something and move forward.

9 So, first, some of the things that I have heard
10 today -- one of the things that I've heard so much is
11 that the consumer can control what they're doing. I
12 think in 2000 when the agreement was published, I think
13 that most web browsing and cookie deposits and whatnot, I
14 think it was being mediated on the web and I think that
15 was true. But I don't think it's true any more.

16 What we're really seeing is that the NAI opt-
17 out cookie has failed in a number of ways. One of the
18 most principle -- the principle way it's failed is that
19 consumers aren't really using it. We don't have a lot of
20 numbers on this. Trevor was talking about a few, but if
21 you ask people that you know on the street, do you have
22 an NAI opt-out cookie -- I would dare you to do that
23 because I think you'll find that the answer is usually no
24 and people don't really know what they are. And what
25 tends to happen with the NAI opt-out cookie is it's very

1 fragile and it's very susceptible to deletion.

2 So, for example, if you have a computer
3 protection program on your computer that's just
4 automatically deleting third party cookies, it tends to
5 wipe out the NAI opt-out cookie as well.

6 So, we have a core protection as part of the
7 NAI agreement that's not really very, very persistent. I
8 think this is a problem that AOL and Tacoda have
9 acknowledged with their efforts to do the quote, unquote
10 "hardened opt-out."

11 But, anyhow, I think we really need to look at
12 the cookies and how many consumers are actually using
13 those cookies, how many consumers are actually able to do
14 the opt-out.

15 We did a test over the past six months on that
16 opt-out page that you saw and we found that consumers
17 really have trouble opting out. In our tests we found
18 that -- and we used every platform. We used PCs, we
19 used Macs and we used Spark UNIX workstations behind
20 firewalls. So, if a corporate person was trying to opt
21 out we wanted to see what happened there. And we
22 basically found that it is really tough because -- and,
23 Trevor, you will probably say the same thing.

24 I mean, when you try to study how that opt-page
25 actually works, it's tough because it doesn't work very

1 often and it's really variable depending on your browser
2 setting, depending on your firewall settings, so a lot of
3 variables. So, the simple opt-out is not a simple
4 opt-out. In comments that have been filed for this
5 meeting, that has been acknowledged. So, I think we know
6 we have a problem there.

7 But there's a further problem, and that is
8 this, there are new tracking -- actually, old tracking
9 technologies that are being used in new ways that extend
10 far beyond cookies. So, for example, let's say a user
11 has downloaded an NAI opt-out cookie successfully, they
12 somehow manage to hear about it and they downloaded it
13 and they haven't deleted it. If they go and watch a
14 video online, they can very well get a flash cookie. A
15 flash cookie has more tracking capacity than an NAI
16 opt-out cookie.

17 How do you address that within the NAI
18 structure? The answer is the NAI structure doesn't
19 address it at all and it wasn't meant to and it doesn't.
20 So, we have a tracking technology that's in use of 98
21 percent of the computers today that's not addressed.
22 That's an issue.

23 We also have the Tacoda hardened cookie to talk
24 about. So, we actually did a technical packet sniff
25 analysis of how the cookie worked. What happens is that

1 it's going in and resetting the NAI opt-out cookie. So,
2 someone deletes the cookie and then the technology goes
3 in and says, oops, that cookie is gone, let's reset that
4 cookie.

5 So, in Tacoda's case, they're doing it to
6 protect privacy. But the principle is that you have a
7 member of industry going in and reading a user's mind and
8 saying, I don't think they wanted to really delete that
9 cookie, so we'll make it right for them again. So, I
10 don't think they're causing any harm.

11 However, what happens when a company goes, oh,
12 you know that tracking cookie we deposited, someone
13 deleted that. I'm not real happy with that, I think I'll
14 just go in and reset that. I think that it would be fair
15 to say if there is an ad company -- and I don't think
16 they're here today by the way. If there's an ad company
17 that sets a targeting cookie and then a user deletes it
18 and they reach into the browse cache and reset it, I
19 think that does constitute an unfair and deceptive
20 business practice. I think we can say that very, very
21 clearly.

22 But the other thing is that this is a whole
23 realm that the user doesn't know about. If a user wants
24 to actually delete everything, now they have to delete
25 cookies and their browser cache. And there's also two

1 other categories of cookies. One is called the silver
2 light cookie, one is called a super cookie or an XML user
3 data cookie. We have all this material in our report.

4 But the bottom line is this: There are
5 multiple ways of tracking users now that extend far
6 beyond that old fashioned NAI cookie.

7 And then, finally, the membership of the NAI is
8 very, very problematic. Two years after the NAI was
9 formed, there were only two members of the NAI. So, we
10 used webarchive.org. In the report, you'll find a
11 listing of the history of the NAI membership, and what's
12 extremely apparent is that the industry itself has not
13 embraced self-regulation. And I think we have to ask,
14 why are companies jumping on board a ship that isn't
15 working? We know the NAI opt-out cookie isn't working.
16 We know the NAI doesn't cover all the new technologies
17 and the NAI has a very challenging membership history.

18 And then there's other issues such as the
19 enforcement. Currently, if you go to, for example,
20 TRUSTe watchdog reports of NAI, when they first started,
21 they reported the number of opt-out cookies and number of
22 OPM problems, and this was good and this was appropriate.
23 But over the years they just stopped reporting on it.

24 So, now, we don't know what's happening. If
25 you're a consumer, it's a very opaque process. So, I

1 think from the consumer perspective the real issue here
2 is, is this a program that's working to protect consumers
3 and is it a true robust self-regulatory program? I think
4 you have to answer it, at this point based on the factual
5 evidence, I think you have to say no. I think it has
6 failed and I think we need to take a new look at it.

7 Thank you.

8 **(Applause)**

9 MR. AARNIO: Ladies and gentlemen, it's great
10 to be here again with some European perspectives for you
11 here.

12 So, gentlemen, Friday afternoon, please raise
13 your hand if you attempt this. As we know, this
14 technology is there in your pockets right now. We have
15 our mobile phones. So, in this picture, the technology
16 is ansium (phonetic). So, the European perspective in
17 this case is who makes the decision? Either the wife on
18 the left side or the husband on the right side.

19 Who are these guys? If they are not a couple,
20 they might be employer and employee or business unit and
21 its customer and so on.

22 So, anyway, the European perspective is that we
23 have a legal dispute. And since there is legal dispute,
24 mister here in this picture says no, I do not accept to
25 use this kind of technology, and the wife says that yes,

1 I want you to use, we need to have rule of law to solve
2 this kind of dispute. So, this is very simple, isn't it,
3 like this?

4 There is no definition about what privacy means
5 as such. But since we are talking about data protection,
6 we can define data protection as a cluster of rights.
7 And here you have the list. I suppose this is more or
8 less exhaustive, this list, and as you can see, we start
9 with the right to control and decide how. So,
10 self-autonomy or self-determination. This can be
11 understood as an opt-in or opt-out or consent or
12 whatever.

13 Then since we want to access these rights we
14 need to know who is data controller. So, we have the
15 right to be informed.

16 Then the next point is very, very challenging
17 since I was telling you about the right of law. This
18 means, this third point, that the parliaments are key
19 role players in this game.

20 The next one, the right to be able to evaluate
21 it on the basis of correct and relevant information as
22 opposed -- this is something very useful, also, for the
23 business, and so on.

24 So, this morning at the University of
25 Georgetown Law School, we spent a lot of time talking and

1 discussing about data security. And it's very simple to
2 define data security as a right which secures these other
3 rights.

4 So, why do we need all these rights? Well,
5 simply, therefore, that our human dignity should be
6 respected, our autonomy should be respected, our honor
7 should be respected and nobody shouldn't be discriminated
8 and our equality as citizens is secured as we all know.

9 Now, can we put a price label on this? Some
10 people say that they do not have anything to hide, other
11 people are very, very precise with their privacy, with
12 their data protection. So, we are talking about quality
13 of life, which means that this is a very personal
14 question. If somebody wants to exercise these rights,
15 then let him do so, or her.

16 Here is the global environment and national
17 states and how this affects. So, as we can see, we have
18 a general data protection and, on the other hand, access
19 to public documents legislation. Then we have a lot of
20 legislation on different functions like marketing,
21 communication and so on. We have sectoral legislation,
22 health care sector, public sector, social welfare sector
23 and so on. And the latest instrument is codes of
24 conduct.

25 In Europe, we have this three pillar system

1 which are now getting closer to each other since there is
2 a brand new framework. This isn't data protection, it's
3 applied also on police and security matters. But Lisbon
4 Treat, which is mentioned here, means that the 19th of
5 October, so two weeks ago the leaders of member states
6 approved a new treaty where there is a list of these
7 basic human rights which lists include data protection
8 and privacy protection as well. So, this means that data
9 protection is considered as a basic human right, and if
10 something goes wrong, data subject always can claim or
11 complain finally even to the European Court of Justice
12 and European Human Rights Court of Justice, too.

13 This seems to be a mess-up but this is the
14 diagram of this Data Protection Directive and our
15 National Data Protection Act, which we use as part of our
16 privacy impact assessment tool. And, by the way, there
17 is a statement or attachment from the European Court of
18 Justice where the Court says, these articles should be
19 interpreted simultaneously and not alternatively.

20 Thank you for listening.

21 **(Applause)**

22 MS. RICH: Reijo, I'm playing Oprah here in the
23 audience. Before you run away, as these laws -- did I
24 hear you say yesterday that this whole framework would
25 only apply if it was personally identifiable information?

1 So, to the extent we have been talking about information
2 that's not personally identifiable in the traditional
3 sense, the data directive would not apply.

4 MR. AARNIO: Well, actually, this legal
5 framework is about personal data, so identifiable data,
6 but also traffic data, so communication data. And, now,
7 this regulation means, in some cases, you are not allowed
8 to know who is part of a communication.

9 MS. BRANDENBURG: We are going to turn to the
10 roundtable portion of this session. I'm going to
11 introduce from the far end the roundtable participants.

12 We have at the end Jerry Cerasale from the
13 Direct Marketing Association; Peter Swire, Moritz College
14 of Law at Ohio State University; Jeff Chester, Center for
15 Digital Democracy; Karen Geduldig, who is from the Office
16 of the New York Attorney General; Ari Schwartz, Center
17 for Democracy and Technology; Brad Schuelke, Office of
18 the Texas Attorney General; Mike Hintze from Microsoft;
19 Mark Cooper from the Consumer Federation of America; and
20 Mike Zaneis from the Interactive Advertising Bureau.
21 Then, of course, our presenters, and you know Jessica
22 Rich and myself. She's moved over there.

23 So, we have just heard three approaches or
24 takes on the issues that we have raised dealing with
25 behavioral advertising. We wanted to get out, at the

1 beginning of this session, any other models for
2 self-regulation that may be out there. So, I'm going to
3 direct this question to Mike Zaneis, if you could start
4 us off.

5 MR. ZANEIS: Sure, I appreciate it. Obviously,
6 Trevor did a good job of covering NAI and I'll let Jerry
7 talk about DMA and you've heard from others, such as OPA,
8 earlier in the program. So, what I might just touch on
9 is sort of the success story we see on individual company
10 self-regulation and the number of companies that are now
11 really competing on privacy. And it's not a new
12 phenomenon, I just think you hear a lot about it because
13 of good events like this. But I think it's something
14 that we've really seen incentivized recently. There
15 seems to be disconnect today. People seem to say that
16 consumers don't know what's happening and they don't know
17 about privacy policies and they don't know about cookies,
18 and I think that's probably borne out by some of the
19 consumer survey data that we've seen.

20 But one thing that the private sectors figured
21 out is that being strong on data security and on privacy
22 practices is just good business. So, you see some of the
23 announcements such as what AOL is doing. You heard
24 earlier from eBay where they're actually embedding
25 notices and the opt-out right there in the advertisement.

1 And I think it's a great way, what we really have is now
2 fertile ground for competition and innovation within the
3 private sector. And what you see is people devoting
4 real resources and attention to this.

5 And I think what we'll see is sort of this
6 blooming of a thousand flowers of different models
7 because the Internet is so diverse and there's a reason
8 that a one size fits all doesn't necessarily work on here
9 because there's so many different platforms, there's so
10 many different business models, whether it is the 12
11 million bloggers out there in the United States, many of
12 whom are able to sustain their infrastructure and their
13 time and resources because of a plug-in from Google or
14 anybody else, that's a real success story.

15 So, what we want to do is allow the competition
16 within the private sector. Again, you know, I said it
17 before, the key here is to provide consumers with options
18 and with tools. And the more that you try to regulate
19 and just to have one single solution, I think the more
20 you're just sort of doomed to fail here.

21 MS. RICH: Mike, do you want to talk just a
22 little about -- IAB has its own principles, right? Do
23 you want to just briefly describe what those are?

24 MR. ZANEIS: We do, and they follow the basic
25 tenets of privacy online that you would think. So, our

1 best practices state that every member should have a
2 privacy policy, it should be clearly worded, it should be
3 easily accessible from the first page and subsequent
4 pages on your site. Those things, consumer choice,
5 strong data security, I mean, this is -- we had a
6 conversation about cookies before and there we're not
7 talking about sensitive information. But on various
8 platforms you're going to have businesses that collect
9 different types of information. Right? You can't have
10 an ecommerce website without collecting certain financial
11 information, credit card number and such.

12 So, data security has to go hand in hand with
13 that. That's where IAB's best practices really focus
14 attention.

15 MS. RICH: And how many members do you have?

16 MR. ZANEIS: We have over 350 members.

17 MS. RICH: And do you do anything to enforce
18 the standards?

19 MR. ZANEIS: It's just best practice, it's not
20 regulatory. We don't kick people out necessarily. We
21 have been looking at the potential for -- we certainly
22 have partnered with TRUSTe on a number of their programs.
23 As I said, we support NAI and DMA and OPA, but we've
24 looked at maybe seeing if it's feasible to roll out some
25 sort of privacy compliance program, whether it's a

1 privacy seal or something like that working with --
2 similar to what you see BBB online doing.

3 MS. RICH: Thank you. Jerry, do you want to
4 talk about how DMA's best practices may touch on these
5 issues, specifically behavioral advertising?

6 MR. CERASALE: Sure. DMA has some best
7 practices, but we also have guidelines which are
8 requirements for members to follow. And we also have a
9 self-regulatory framework with ethics committees and
10 adjudication, and self-regulation is viewed more as not
11 punishment but corrective action to try and stop the
12 practice, get it stopped and get it going. And we have
13 sent many a case to perspective Attorneys General and the
14 Postal Inspectors and the Federal Trade Commission.

15 In online marketing, our whole thing goes on
16 notice, and if you're using -- I think our thing says
17 cookies or any other passive means of data collection,
18 whether the data collected is used internally or whether
19 it's transferred to third parties, there are things that
20 have to be noticed in the privacy policy of all DMA
21 members.

22 We have found in writing this that you had
23 to -- we started doing these quite a ways back, that you
24 could not just leave it to cookies and we had to try some
25 other language because there is going to be successors

1 coming along, even beyond what we know today. Tomorrow,
2 there may be a new form to try and get it to fit within
3 the guidelines. So, we have all of that.

4 We also have special guidelines sensitive for
5 health data, data received from an individual, inferred
6 from practices and things from the doctor/patient
7 relationship, and putting in, in a sense, in that area
8 opt-in, must have express consent in order to use and
9 move that data forward.

10 So, that's what DMA has in place and we've done
11 it for a long time and have actually kicked some members
12 out and publicly kicked them out.

13 MS. RICH: Does anyone know about any other
14 industry-wide standards that would be worth throwing out
15 on the table? I sort of want to get the inventory out on
16 the table before we start debating anything. How about
17 individual companies? We saw that AOL said that it was
18 going to be implementing some sort of do not track, maybe
19 different from your proposal, but what other possible
20 individual company initiatives have we seen where they're
21 trying to address some of the behavioral advertising
22 issues? Mike, do you have anything on that?

23 MR. HINTZE: Sure. Well, in July of this year,
24 we announced a set of principles that we are going to be
25 following in the online behavioral advertising space, as

1 well as search, around issues around transparency and
2 user control and protecting the data and how we anonymize
3 data, which we followed up on with a white paper that we
4 released this week in terms of describing in more detail
5 how we anonymize data and how we protect data while we
6 have it.

7 And, so, I think that there's a lot of
8 companies that are doing really interesting things. We
9 saw from eBay, we saw AOL's initiative. The advocates
10 have thrown out some great ideas. I think there's
11 probably no one silver bullet here. There's a lot of
12 things that go into protecting data, protecting privacy
13 in this area and that ranges from regulation, the FTC
14 using their existing authority under Section 5 or in
15 merger reviews to the extent that consolidation of data
16 or data collection raises competition as well as privacy
17 issues, technological solutions that we're seeing,
18 consumer education is an important part as well.

19 I think all those things need to play together
20 when we look at overall solutions in the space.

21 MS. RICH: So, we have international standards,
22 we have FTC unfair, deceptive acts or practices, we have
23 NAI, we have IAB, we have DMA, we have individual
24 initiatives. Let's round it out, the states. What are
25 the tools and the standards that you would use possibly

1 to address these practices? What are the standards
2 you're measuring them against? Brad and Karen.

3 MR. SCHUELKE: I guess before I start, before I
4 make any comments, I unfortunately have to make the
5 disclosure that nothing I say is official opinion of the
6 Texas Attorney General or the Texas Attorney General's
7 Office.

8 I think in general right now the states are
9 looking at a couple of things. I think, first and
10 foremost, it would be the states' deceptive trade
11 practices and unfair practices statutes, similar to the
12 FTC's Section 5. I know California has a specific
13 statute regarding consumer's ability to opt out of data
14 collection, but I think that right now as current, those
15 are the two primary things.

16 MS. RICH: So, it sounds like we have a fair
17 number of standards in this area, but maybe not that many
18 that apply specifically to behavioral advertising, is
19 that right, and address these practices. So, maybe to
20 come at it from a different angle, and this would draw on
21 everything we have been talking about yesterday and
22 today, in the behavioral advertising area, are there
23 practices we can agree are off-limits or in-bounds? I
24 think we heard -- which could form the basis for some
25 sort of consensus or standards.

1 I think we heard a few things over the past
2 couple of days. There was a lot of talk about sensitive
3 information. There was talk about merger of offline and
4 online, merger of PII with non-PII. There were possibly
5 other avenues. It looks like Ari is itching to talk.

6 MR. SCHWARTZ: The problem that I see just on
7 that point is there are a number of companies -- I mean,
8 we've outlined this our way and Pam has numbers on this,
9 too -- that do not follow the NAI guidelines and they're
10 perfectly within the law in not following the NAI
11 standards. What happens to those companies that don't
12 offer opt-outs? What do we do then? There's nothing
13 illegal about what they're doing, right? But users have
14 no controls in that case.

15 In fact, if you look at the studies, a study
16 that hasn't been mentioned today, the Annenberg-Berkeley
17 study that just came out that says that consumers don't
18 know what's going on in behavioral targeting, and when
19 they find out, they don't like it and they don't know
20 what to do. So, you have those pieces together and you
21 have all these standards, but there's also -- I just got
22 a flash cookie the other day from this company called Ad
23 Gardener on the Drudge Report site. So, anybody that's
24 been to Drudge Report, go look at your flash cookies.
25 They're not easy to find because the controls are not

1 very good, and you'll see that you have a tracking flash
2 cookie that's set for you.

3 It's being used today. We're not making up
4 these technologies that are being used besides cookies.
5 There's a whole range of things that are going on out
6 there that are outside of the scope of all of those other
7 -- all of the protections that you mentioned today.

8 MS. RICH: But I'm trying to -- we're putting
9 on the table various models and that includes a notice
10 and choice model and we have NAI, which is a notice and
11 choice model. But I'm trying to just throw out on the
12 table, is there another model like a harm-based model
13 that would take certain practices just off the table? And
14 regardless of what consumer's preferences are, like you
15 can't use sensitive information in behavioral
16 advertising, period. That's the clearest example because
17 everyone seemed to talk about that.

18 But are there others that one would be able to
19 agree on in sort of a harm-based model?

20 MR. SCHWARTZ: Well, I mean, our point of view
21 is that it should be under the user's control. If we
22 could get an NAI practice that was universal, that was
23 technology neutral, and actually played on a marketplace,
24 allowed the marketplace to innovate in the space rather
25 than sticking with something like the way the NAI opt-out

1 works, which is stuck in the cookies world which only
2 applies to the NAI companies, and in some ways those are
3 the best -- I mean, the leaders. The only company we
4 have on the panel here is Microsoft and they have some of
5 the best practices in the space. You have the best --
6 you have the --

7 **(Laughter)**

8 MR. RICH: It was worth coming, right?

9 MR. SCHWARTZ: You have the leaders who are
10 here at this session, but the concerns from consumers are
11 all those outliers and what do we do about them? Larry
12 Ponemon said this on the panel yesterday, do we go after
13 the good guys or the bad guys? I'd hope we'd go after
14 the bad guys and we do it in a way where we can make sure
15 that the good guys still want to do what they need to do
16 without harming the bad guys.

17 MS. RICH: Jeff? And then maybe we'll move
18 into a discussion of what we think about the various
19 models. But Jeff first.

20 MR. CHESTER: I don't want to talk too much
21 because I've had too much -- I've a great opportunity,
22 which I thank the Commission. But, look, there are
23 certain practices that should be not allowed at all,
24 particularly in the children's area, particularly in the
25 youth area. I don't have to get -- we talk about the

1 health area, we talk about the obesity area. There are a
2 number of practices that should not be permitted at all,
3 and we will make sure that these issues get addressed
4 over the next several years and, hopefully, the industry
5 will come and agree to work with the privacy community to
6 make sure that those practices don't further evolve.

7 MS. RICH: What are those practices? I would
8 love to hear everyone's view on what are those practices.
9 Does anyone else want to venture forth? What are
10 practices, Mike, that your companies shouldn't be doing?

11 MR. ZANEIS: Well, let me answer that question
12 by also answering your last question. I think we
13 actually do have a harm-based model, don't we? It's
14 called the FTC Act, and it works well and on a number of
15 occasions. And what we haven't seen is that real harm,
16 right?

17 We have heard speculative, this might happen or
18 I hear that somebody is doing this. Absolutely.
19 Sometimes there will be outliers. The technology allows
20 a lot of data collection. That's the way the Internet
21 works. So, what we need to do is focus on the folks who
22 are causing harm. And we have had this debate with
23 spyware, and what the FTC found was that they had all the
24 authority they needed to go after the people who were
25 causing harm to consumers. I think that's a positive.

1 So, specific models, we've talked about them.
2 You're right. We need to not be violative of whether
3 it's COPPA or the Fair Credit Reporting Act or HIPAA or
4 something like that. It's not the wild, wild west.
5 There are laws out there. There are practices and people
6 are following those. So, let's at least be
7 intellectually honest about what the landscape is.

8 MS. RICH: Let's move in to sort of what we
9 think about --

10 MS. BRANDENBURG: Mark?

11 MS. RICH: Oh, Mark?

12 MR. COOPER: Well, I want to challenge the
13 assertion that the notice and choice model works well.
14 You've put these the dozen or half a dozen models on the
15 table. I'm recent to this space. I'm a consumer
16 advocate of long standing. Let me tell you what I have
17 heard about the nature of the problem in the last two
18 days of this conference.

19 After seven years of self-regulation, what you
20 have is a situation in which somewhat less than 5 percent
21 of the population can protect itself. If it's
22 interested, literate, informed and skilled, why they
23 might actually be able to weave their way through these
24 models that out there. Unfortunately, the vast majority
25 of the population lacks one of those four

1 characteristics.

2 I have heard this in three key factors that we
3 have heard over the last two days, and this is the model
4 that is on the table as the main means for protecting
5 consumer privacy. First, I heard that things are good
6 because online markets you can go in and opt out with
7 three clicks. I think the -- no more than three clicks.
8 I think the actual average is probably five. But I've
9 sat in many meetings with ecompanies where they swear
10 that each click costs them 10 percent of the market share
11 and that's why they have to be the default. They all
12 want to be the default because each click costs them
13 market share.

14 Consumer privacy is losing at least 30 percent
15 market share and probably 50 percent. I have heard that
16 85 percent of the companies have privacy statements, but
17 99 percent of those statements are incomprehensible.

18 Now, there's not one advertising company in
19 this room who would take the language of those privacy
20 statements in to a client and say, here, use this to sell
21 your product. They would be kicked out and out of
22 business in the blink of an eye. That is the status of
23 this situation.

24 Finally, I heard survey evidence that
25 demonstrated a remarkable gap between what consumers

1 expect and what marketers think they deserve. There was
2 a huge gap between what the marketers said consumers
3 should have for privacy and what consumers wanted. And,
4 of course, the presenter suggested it was a uninformed
5 consumer. But what it is is a concerned consumer.

6 So, I've heard the word "accountability" a
7 hundred times. But accountability without actionability
8 is meaningless. And we have seen the numbers. There is
9 no actionability for the vast public and, therefore, the
10 marketplace cannot possibly effectuate the solution
11 because consumers cannot act on what the industry claims
12 these models are providing.

13 So, I think the fundamental from premise here
14 of wanting to move on from notice and choice to the other
15 aspects of behavioral marketing missed the point, that
16 the model we have already does not work, the consumer
17 does not think it works, and the consumer expectation,
18 perception, belief, is actually what this is about.

19 MS. RICH: Well, I have been trying to get a
20 discussion going on a model that wouldn't necessarily put
21 so many burdens on the consumer, but I'm not hearing a
22 lot of principles that everyone can agree on that would
23 just be kind of off the table for the consumer. I'm
24 hearing a lot of support for the notice and choice model.

25 MS. DIXON: I would like to jump in. I have a

1 question. I mean, I thought we were going to talk about
2 existing models. The existing model is the NAI. That is
3 the model that the FTC recommended to address behavioral
4 marketing. I mean, that's the model.

5 And it hasn't worked. There's documented
6 failure of that model. I think we've got to be really
7 careful. I think we need to be very careful before we
8 just say, okay, that didn't work, let's just try
9 something completely new. I mean, I think we need to
10 look at the ways it failed and address that.

11 So, for example, if there are a thousand new
12 models blooming, should a consumer have to visit a
13 thousand places to opt out? I mean, what do we want the
14 end consumer experience to be? Maybe we should start
15 there.

16 MS. RICH: Okay. I think Trevor has indicated
17 an openness to hearing feedback about how he can improve
18 his model.

19 MR. SWIRE: Jessica, if I could have a first
20 chance to talk.

21 MS. RICH: Peter, okay.

22 MR. SWIRE: Maybe I'll wait until the next hour
23 when I'm not on the panel. At some point, choice is
24 going to be involved because if you get a consumer to
25 swear after he cuts his finger and puts blood on it that

1 he wants something or she wants something, you're going
2 to let them do it.

3 The questions are what are the choices? I
4 respect Trevor and I was around when NAI was created. I
5 worked in the government then. And that was a guess at
6 2000 about what might work and it was accompanied by a
7 very clear signal that the merger of online and offline
8 database wasn't going to happen. Now, we have the world
9 offline where there's many, many ways in which stuff
10 that's not readily identifiable at point one is hooked in
11 through an email or something else and is fully
12 identifiable to lots and lots of people.

13 So, now, we're in the place online that we
14 prevented happening in 2000. And the question is, how
15 well do our guesses in 2000 bind us today? I think for
16 the last couple of days and everybody getting ready for
17 this meeting, it's pretty clear that the choices that we
18 had as of six or eight months ago were lousy for
19 consumers. No ordinary human being could figure it out.
20 Sorry, but that's pretty much it.

21 And the public policy goal it seems -- whatever
22 you call the model, I think the public policy goal goes
23 something like this: We know from Larry Ponemon and Alan
24 Westin that there's people with diverse privacy
25 preferences. There's some people who go on Rivera and

1 Jerry Springer and they're not caring about privacy.
2 They say amazing things. And there's other people
3 that -- and depending on the numbers it's 20 or 30 or 40
4 percent -- have high privacy preferences. And the FTC
5 ran the do not call list for telephones and what's the
6 number, a hundred million or something. There's a lot of
7 people on that one.

8 So, we know that when it's workable, there's a
9 whole bunch of people, pick your number of tens of
10 millions of people, who have privacy preferences. The
11 public policy goal, roughly speaking, is letting the
12 system work so it matches their privacy preferences. If
13 they want to be personalized and they want the sign up
14 and they know what they're getting and all that,
15 hallelujah, let that happen. It's pretty clear if you
16 give folks a chance they don't want something it ought to
17 be workable for them.

18 You can call that notice and choice, you can
19 call it harm to me, if I don't get what I want, you can
20 call it whatever model you want, but at a public policy
21 level somehow it ought to be that normal people more or
22 less can get what they want. That's a good goal for the
23 FTC.

24 And then in terms of how to get it -- and I'll
25 just go for just a couple sentences -- I think that it

1 has to do with the leadership. And I think this workshop
2 is the FTC stepping in and acting as leaders to bring
3 folks together that maybe could have talked about a year
4 or two or three earlier. I was talking to one company
5 who had their engineers working nights and weekends to
6 get ready for today because they knew they had an
7 announcement.

8 And that kind of we need to focus, we need to
9 get to decisions, and if we don't, then there's going to
10 be something that comes from it, is something the
11 government can do, not to be heavy handed on industry,
12 but to help the best people in industry get to know where
13 they should go anyways.

14 If the companies that are able to make
15 announcements because they're able to get their
16 management to give them their resources to be ready for
17 today, if the companies who are good, who are able to
18 come to the meeting and say, look, we're proud of what
19 we're doing, and I think the government, the FTC has a
20 role in helping bring out the best of the industry so the
21 choices are closer to what real people want.

22 MS. RICH: Well, along those lines, why don't
23 we talk about how the existing model might be improved.
24 We've talked about some of the problems. How it might be
25 improved, what might be missing in that existing model or

1 how it might be expanded to be better, and also move to
2 talking about the do not track proposal and whether the
3 diverse group here thinks that could be feasible on a
4 broader basis than just one company, whether it be
5 voluntary or something else.

6 So, who would like to start mentioning in a
7 constructive way?

8 MR. COOPER: I'll try. We have six principles.
9 Let me outline what I think the principles are having
10 been one of the signatories of the document yesterday.
11 What I would call six principles for the uninterested,
12 illiterate, uninformed and unskilled. Those are folks
13 who need your protection. We don't need to protect the
14 other guys.

15 So, here are the six principles as I see them
16 from yesterday's announcement. A simple consumer
17 friendly interface to declare across all platforms that
18 you do not want to be tracked.

19 Two, robust notification about how to make that
20 declaration and contextual notification if that wish is
21 perhaps to be violated or to remind you what you decided
22 to do in case you want to change your mind.

23 Three, a consistent set of basic privacy
24 protections and definitions that consumers can understand
25 across platforms.

1 Four, teeth to enforce compliance so consumers
2 can trust the system.

3 Five, an effective right to correct information
4 about and categorization of consumers that is used in
5 online marketing.

6 And, six, an organized process for overseeing
7 and updating the protection of consumer privacy. Seven
8 years is far too long to wait to keep up in a space as
9 dynamic as this.

10 I think those six principles were outlined
11 yesterday in that statement and, frankly, a lot of my
12 constituents fall into that category of people. Now,
13 don't tell them I said that about them, but actually
14 that's why they hired me to protect their interests here
15 in Washington, and I think those will, in fact, go a long
16 way.

17 That doesn't mean there aren't people who
18 choose not to opt-in and, therefore, can do other -- you
19 know, you can treat them otherwise. But this needs to be
20 there because the number of people who fall in that
21 category is very large and, therefore, they need
22 protection.

23 MS. RICH: Trevor.

24 MR. HUGHES: So, certainly, we are happy to
25 engage in the dialogue. Let me just make sure that I

1 clarify a few things about the NAI principles. First of
2 all, the NAI principles are not technology-specific.
3 They are technology-neutral. They don't say anything
4 about cookies. So, to the extent that someone is using a
5 flash cookie, XML silver light, cascading style sheet,
6 whatever it might be and they are doing behavioral
7 targeting, they should be a member of the NAI, and if
8 they're not, shame on them.

9 And when they come to join the NAI, we will
10 work with them to implement the principles, the
11 constitutional concepts that we have within the NAI to
12 provide the availability of an opt-out, to provide
13 notice, to provide the same protections that we have now.
14 That would be a case of first instance for us. We have
15 not had a non-cookie member applicant approach us yet.

16 Second, most definitely our membership did ebb
17 and flow as did the industry. Soon after the NAI was
18 formed the dot-com economy deflated, 9/11 occurred, and
19 we did go down to two or three members. Since then, we
20 have seen a resurgence in interest and behavioral
21 targeting, though. Not for nothing, but I think the many
22 billions of dollars of M&A activity have sort of resulted
23 in a lot more focus.

24 And I'm happy to say that Yahoo! was approved
25 for membership this week, AOL is a member twice over with

1 two of their subsidiaries, Tacoda and Advertising.com,
2 and Microsoft and Google both have pending applications
3 that we're working through right now, and we look forward
4 to both of them being members. So, we do have
5 significant breadth, I think, in terms of behavioral
6 targeting online within the NAI.

7 And then, finally, just in the sort of
8 responsive points. We're not hard to find. We're not
9 hard to talk to. We're pretty well-known and visible
10 within the privacy community particularly and no one
11 talked to us. Had anyone talked to us, we would have
12 been able to say we've got over a million hits on our
13 website this year. The opt-out page is getting a million
14 hits a year. We would have been able to say, there are
15 over 20,000 references to the NAI opt-out page across
16 privacy policies around the world even.

17 Certainly, we can do better. Certainly, there
18 are other issues that we can tackle. But to throw the
19 baby out with the bath water, to label this as a failure,
20 I think is inappropriate given that the NAI was built to
21 do a specific thing for a specific set of practices and
22 it has been doing that for six years.

23 Now, on to what can we do better, because I
24 think we can do things better. I mentioned sensitive
25 data. I think that there is room for us to talk as a

1 community about the use of sensitive data in even
2 non-personal behavioral targeting.

3 So, are there sensitive categories that we can
4 identify where, as Peter Swire so rightfully suggested,
5 we should require a cut finger, a seal on paper and a
6 signature in blood that someone really means that they
7 want to let us target on those things?

8 We can create a de facto use limitation on
9 those practices by putting a consent standard in that's
10 so high as to be unfeasible for the marketplace. So,
11 sensitive data for non-PII practices, I think we can
12 certainly put in place.

13 I will mention that PII-based targeting within
14 the NAI principles is not permitted.

15 MS. RICH: Can I -- Ari?

16 MR. HUGHES: Sure. The last point I just want
17 to make is that I still think, though, that there is a
18 distinction between PII and non-PII practices. We should
19 be recognizing that there are practices that are
20 connected to personal data that should require higher
21 standards. We have an architecture for that within the
22 NAI principles, it has remained unused. But the non-PII
23 piece of NAI principles certainly has been used for the
24 past six years.

25 MS. RICH: Thank you. Ari?

1 MR. SCHWARTZ: Let me first start by saying
2 there are several things I agree with Trevor about,
3 including the fact if companies are network advertisers
4 and they're not NAI members, shame on them. They should
5 join. And Trevor and his staff do great work and they've
6 done great stuff on web beacons and emails and have
7 consulted with us and other groups on that.

8 However that doesn't make up for the fact that
9 there have been no changes to the basic implementation of
10 the guidelines of the principles since they were put into
11 effect, including the fact that it is cookie-focused.
12 And there's a basic problem in giving the opt-out to the
13 individual in the same structure in which they are being
14 tracked. Individuals want to delete them so they
15 disappear.

16 I don't even have to go much further than to
17 say look at the videos we saw today about cookies. Do
18 you remember how many of them mentioned the NAI in the
19 video, in going to the NAI to opt out? None of them did.
20 In fact, I saw a lot more of them than just the five that
21 we watched here and none of those mentioned the NAI
22 either.

23 The NAI is not the way that people are opting
24 out today and the other methods are cumbersome as well.
25 So, the question is, what can we do to make things more

1 universal, more technology neutral, and something that
2 can build a marketplace for Consumer Protection in this
3 space? We suggested the opt-out. If I can have just two
4 minutes to describe the do not track list, I would like
5 to do that because --

6 MS. RICH: Well, I would like to move to the do
7 not track list, but I first want to understand whether
8 people think that that NAI is something that can be fixed
9 and improved because a lot of complaints we're hearing is
10 it's not known or not used or it's --

11 MR. SCHWARTZ: Well, there's also a range of
12 things in the principles that we complained about
13 originally that we still have concerns with. We could
14 probably come down to -- and I haven't read Pam's report
15 fully yet, but I know that it hits on a lot of these
16 points. You probably come up with about nine different
17 complaints from CDT about the NAI. I don't know if it's
18 fixable or not, for that purpose. Like I said, some of
19 the other work they've done has been very successful.

20 MS. RICH: Pam.

21 MS. DIXON: Look, I think that we really have
22 to look at all the options here and really look at the
23 facts. I don't think we can just speculate and say,
24 okay, well, let's see, let's see how we can possibly
25 foresee into the future.

1 One of the things that we proposed in our
2 consensus document is that there be some kind of
3 oversight committee so this wouldn't happen again. I
4 think it is very difficult to draw a line in the sand and
5 say, okay, we're going to ask that technology stay here.
6 We can't do that. Technology is going to move on no
7 matter what we do. Since we know that that's going to
8 happen, we should be able to mitigate for that going
9 forward because we know all the things that happened this
10 time around.

11 The NAI was crafted at a period of time after
12 which there was extraordinary change. So, I think it's
13 very difficult to then try to put so much weight on it
14 that it would survive now. But I think Ari is correct, I
15 think that we need to look at all the options.

16 MS. RICH: Brad?

17 MR. SCHUELKE: Well, I think there are a number
18 of issues and it certainly may be difficult to fix. I
19 think the one problem that I don't know is addressable in
20 the model is the fact that it's sort of not mandatory
21 membership. And sort of just like the do not call, I
22 don't know that there's any way that you can fix that
23 telemarketers don't have to be a member of DMA or direct
24 marketers or behavioral marketers don't have to be a
25 member of NAI, and if there's nothing beyond that, you

1 always have those outliers, you always have the bad guys
2 that we really want to look at anyway. Those are going
3 be the ones that aren't a member of NAI, and I don't know
4 how you fix it strictly in the NAI principles.

5 MS. RICH: So, that's an inherent problem with
6 self-regulation. So, to the extent -- if you were to
7 conclude there's -- I mean, all self-regulation, right?

8 MR. SCHUELKE: Sure. Well, I mean, you could
9 have it as a safe harbor and so this will be self-
10 regulation within a safe harbor and outliers have
11 different standards. So, I mean, you could still have
12 self-regulation in a regulatory model.

13 MS. RICH: Jerry?

14 MR. CERASALE: Seven years ago, we heard the
15 same thing, that gathering information, following where
16 people are going was going to undermine the Internet,
17 undermine consumer confidence. If I sat here today and
18 just came here to listen to this panel, you would think
19 the Internet was an absolute total commercial bust and
20 that people were being harmed constantly.

21 You know, people are going there. Three
22 quarters of Internet users that we found prefer to go to
23 free sites that don't charge them, that they're paid by
24 advertising. So, people understand -- and 86 percent are
25 going to buy more off the Internet than they did before.

1 So, it's not a bust. The self-regulation that has
2 occurred since in those seven years has been positive.
3 The Internet has grown and so forth. We have more things
4 to do.

5 One of the things that I didn't say on DMA's
6 guidelines, and I think is an important thing to look at
7 in the future, is a basic requirement for all of DMA is
8 that marketing data, data obtained from marketing
9 purposes can be used only for marketing purposes. Lots
10 of things we've heard about others using it, it can be
11 used for different types of requests, not to just give
12 you an offer, those are things I think that we have to
13 try and pull into this as well.

14 And the other thing is, in support of Trevor,
15 we didn't have the technology back then that we have
16 today. As a matter of fact, technology has moved to
17 actually help consumers and it's going to continue to
18 move in that direction, as we see with Microsoft's
19 Internet Explorer changes and so forth going forward.
20 Those things are actually making things better in that
21 sense.

22 So, as you look at self-regulation, you also
23 have to look at what is technology doing. That's a big
24 part of self-regulation in its own right.

25 MS. RICH: I know we've got some volunteers,

1 but in further support of Trevor maybe I should have Mike
2 say why Microsoft is joining NAI? What motored that
3 decision? I guess the acquisition. But what --

4 MR. HINTZE: Because we didn't want Ari to beat
5 up on us.

6 **(Laughter)**

7 MR. HINTZE: We acquired a company that was a
8 founding member of NA, and they're actively engaged in
9 being a third party ad network and behavioral targeting.

10 Separately, we've been looking at expanding our
11 own activities in this area and we decided early on that
12 once we did move into that area we would join NAI in our
13 own right. We think that NAI is a good forum to discuss
14 these issues. Despite what the membership may have been
15 in the past, today the major players are there, the
16 responsible players are there.

17 It's a good self-regulatory framework. It's
18 not perfect. As we've seen in the latest wave of
19 consolidation, the environment has changed a lot. NAI
20 was formed in a time where these third party ad networks
21 didn't have direct relationships with customers, for
22 example. Now, most of the big ad networks have been
23 bought by companies that do have direct relationships
24 with customers and have an awful lot of PII.

25 So, maybe one of the things that we need to

1 look at in NAI is where is that line between PII and
2 anonymous data? Do we have to revisit that? Should we
3 rethink that and think about the protections that need to
4 be in place to keep some data on the anonymous side of
5 the ledger as opposed to the PII side of the ledger?

6 So, I think there's a lot of things we need to
7 think about, but I think NAI is the right forum for that
8 and it's a good start and we shouldn't be throwing out
9 the baby with the bath water, as Trevor said.

10 MS. RICH: Are there plans underway to reform
11 NAI or to expand it or to adjust it?

12 MR. HUGHES: Certainly. Again, we are working
13 now and have been for the better part of the past year on
14 sensitive consumer characteristics for behavioral
15 targeting. And we saw this event as an opportunity to
16 engage in this discussion. Again, the interest in this
17 issue has really peaked in the past 12 to 18 months and I
18 think that's largely been driven by certainly the
19 complaint from CDD and US PIRG and also from the M&A
20 activity in this space. It's been front page of the
21 business section at least for the better part of this
22 year.

23 So, certainly, we look at this forum as an
24 opportunity to examine the NAI framework and to consider
25 future changes and future opportunities for us.

1 MS. RICH: So, everyone send their suggestions
2 to Trevor.

3 I would like move in to do not track, which I
4 think is a really interesting idea and I want to make
5 sure we have time to talk about it.

6 MR. HUGHES: Can I just add one really quick
7 thing? That is, I think it's incumbent on all of us, and
8 to the point about the inherent weakness of
9 self-regulation that is voluntary, it's incumbent on the
10 entire marketplace to shame those companies that are not
11 participating into participating. So, if you know of a
12 company that's doing behavioral targeting that's not a
13 member, we're trying our best -- my staff's here with me
14 -- trying to bring them into the organization. Many of
15 them are small shops, many of them aren't willing to make
16 the investment because they're not generating revenue
17 yet. But it should be just a cost of doing business to
18 join the NAI and participate in these self-regulatory
19 programs. They only work when we all focus folks into
20 joining.

21 MR. CHESTER: Just one -- can I have one --

22 MS. RICH: Well, I'm worried because I want to
23 open it up to the audience. So, let's just move to do
24 not track and we can come back.

25 Ari, you wanted to just briefly describe the

1 proposal?

2 MR. SCHWARTZ: Yes, because there's been a lot
3 of misreporting on it and I'd like to try and clarify it
4 up in people's minds a little bit.

5 The basic idea of the do not track list is
6 similar to the do not call list in that both the
7 companies and the consumers engage and there's actually a
8 list that's kept. The difference being that it is the
9 companies, in this case, a list of servers from companies
10 that are engaged in behavioral targeting for advertising
11 purposes who put their servers on to the list, and then
12 you have a list that works across different kind of
13 technologies, so not just cookies, it would be any server
14 that's doing behavioral targeting, and they would submit
15 that list for service to the FTC.

16 The FTC keeps the list. The consumer would go
17 with their browser to the list, be able to pull down the
18 list. And we foresee a marketplace of tools that would
19 come out of that. We're not expecting the FTC to build
20 the tool, as some have reported out there. We expected
21 the marketplace will build the tools. Today, you could
22 take that list and paste it into your exceptions folder
23 to block sites. But we think that there could actually
24 be more granular tools if you let a marketplace go out
25 there and build tools to implement the do not track list.

1 MS. RICH: But are you contemplating this is a
2 legislative idea that would be implemented through the
3 market or could it be self-regulatory?

4 MR. SCHWARTZ: Well, I think that it could be
5 self-regulatory. The question is, who is going to run it
6 in the self-regulatory way that it would actually work?
7 I mean, you get Brad's question of -- I mean, the people
8 that we most want on the list are the people like the Ad
9 Gardeners that are using flash cookies to avoid having
10 their regular cookies deleted because those are the tools
11 that we have today, and they're going to move something
12 else when we come up with better tools for flash cookies.

13 So, how do we go about doing that without
14 having something that works universally and that's truly
15 technology-neutral in implementation as well as in the
16 principles itself?

17 MS. RICH: Since this is a nice concrete
18 proposal that we can talk about, why doesn't everyone
19 take a second to say what they think of it, whether as a
20 self-regulatory or regulatory options. I'm going to
21 start with Karen because she hasn't had much chance to
22 talk, and then we'll go down the line.

23 MS. GEDULDIG: I have to also make the same
24 qualifying remarks as Brad. My statements are my
25 statements, they're not a reflection of the Office of the

1 Attorney General or the Attorney General himself.

2 That said, I think that the do not track
3 proposal is an important one because it focuses on more
4 what we are learning today especially is really the
5 problem. We have learned over the past couple of days
6 that consumers seem to like targeted content but they
7 also want to have control over their privacy. And what
8 the problem with the opt-out of behavioral marketing is
9 that it doesn't really take into account the fact that
10 they've already lost control of their privacy if they're
11 opting out of the marketing but not the actual collection
12 of their data.

13 What do not track focuses on is it's not that I
14 have a problem with the targeted content, I have a
15 problem with you running around after me while I'm online
16 and I have a problem with you following me when I'm
17 online, which is really a step before the marketing.
18 It's the collection. I think that that's an important
19 focus because it allows a consumer to say -- it might not
20 be they don't want to be tracked, it might be that they
21 just want to know that they're being tracked or if you
22 have a different preference, it might be that you don't
23 want to be tracked at all, and I think that that's an
24 important way to look at this issue.

25 MS. RICH: Great, thanks. How about Trevor?

1 Everyone should be very brief so we can open it up to the
2 audience.

3 MR. HUGHES: Am I going to get graded?

4 MS. RICH: No.

5 **(Laughter)**

6 MR. HUGHES: So, I think the do not track
7 concept is intriguing, but when I think about it from an
8 implementation standpoint and when I have talked to our
9 members about it from an implementation standpoint, it is
10 a daunting idea to conceive of how it could actually
11 work. When we think of all the versions of browsers, all
12 of the different technologies that may be used for
13 various types of behavioral targeting -- and I'm not
14 talking about the difference between cookies and flash
15 cookies, I'm talking about mobile devices and all the
16 different channels that we have -- the implementation of
17 a single opt-out mechanism sounds challenging.

18 I also have real concerns about consumers
19 needing to download on to their system an application
20 provided by the Federal Trade Commission, that by the
21 nature of the report would have to call back and get a
22 new list of IP addresses that needed to be blocked on a
23 fairly regular basis. That would be an unprecedented
24 type of technology and I think it has some real
25 challenges.

1 I think we have better controls today in our
2 browsers and I think we should be focusing on consumer
3 education on those controls.

4 MS. RICH: Pam, I think you were a signatory on
5 this proposal.

6 MR. SCHWARTZ: Can I just respond to that one
7 very last point, which is that there are anti-virus and
8 anti-spyware tools that do that today.

9 MS. RICH: Pam?

10 MS. DIXON: There's a couple of things. First,
11 you know, can the industry police itself? That's a
12 question I have and I think that's a very real question
13 we need to grapple with. We've had seven years and it
14 hasn't policed itself well and I think that's an issue.

15 Where is the consumer input into the business
16 practices? Trevor was talking about the NAI, and this is
17 great and I'm glad you're going to look at it again. But
18 where are the real consumers' input? The NAI was built
19 by industry for industry and it's managed by industry.

20 So, this proposal really puts a balance back
21 into the conversation. That's what it's about. It's
22 about, yes, we really think it's quite important not to
23 change the model of the Internet. We think ads need to
24 remain. But consumers need something easy, simple, one
25 place so that they're not confused, so that they don't

1 have to go to the thousand flowers blooming. Innovation
2 is fabulous, but simplicity for consumers is also
3 fabulous.

4 I think the do not track list is about finding
5 a balance.

6 MS. RICH: Reijo, quickly.

7 MR. AARNIO: Thanks. Article 29 working party
8 and the Federation of European Direct Marketing
9 Association's dialogue went on for ten years for creating
10 a code of conduct for direct marketing business and
11 sector. This system of code of conduct is made of
12 abidingness (phonetic) aspect, supervised by business
13 branch itself aspect, and it's like moving from general
14 directive to more precise regulation.

15 So, my understanding is that in Europe we have
16 a regulatory minimum level and then this code of conduct
17 which can be technology-neutral or can include something
18 about technology. This code of conduct always should
19 bring some added value to the business and to customers.

20 MS. RICH: Mike, do you think your companies
21 would be willing to do this?

22 MR. HINTZE: Well, Trevor might be a little
23 ahead of me. I haven't had, in the last 36 hours, a
24 chance to go back to my 350 plus members. I think if
25 they were serious about moving this to implementation,

1 they would recognize the partnership that industry has
2 with consumers and they would have brought us into the
3 process. But it makes very good headline. Everybody has
4 been looking since do not call, they have been looking
5 for the next flash in the pan.

6 So, I'm not going to get too detailed about how
7 it will work. I think I share Trevor's -- you know, at a
8 top level implementation on the technology side, I think
9 it would be challenging and I would say that we've
10 probably got a pretty darn good consumer mechanism in
11 your browser filters that -- thanks to Microsoft,
12 whatever their market share is, 85 percent -- everybody
13 has available, and we're not talking about blocking
14 cookies, we're talking filtering them out before they
15 ever get put on somebody's computer. So, I think that's
16 a pretty good mechanism right now.

17 I would just say this: If we're talking about
18 blacking out large swaths of the Internet, ecommerce
19 sites, free news sites, blogs, social networking sites, I
20 think we've failed consumers if that's the solution.

21 MR. SCHWARTZ: That's no suggestion to block
22 any content. Not even the ads.

23 MR. COOPER: The sites that engage in the
24 unacceptable behavior will be blocked.

25 MR. SCHWARTZ: It would be the choice of the

1 content server to do the tracking from the same place
2 that they provide their content.

3 MR. COOPER: I find it incredibly ironic that
4 this industry, which is represented to me as being
5 incredibly innovative in its ability to surveil and
6 target, suddenly couldn't possibly figure out how to
7 register.

8 Let's be clear. The browser is a great
9 example. Microsoft's new browser is a great example. All
10 we're doing is giving people an easy access to a list
11 that will populate that browser. That's all we're
12 talking about. And I guarantee you that if we do the
13 other platforms, if they know -- and here's where you
14 have to give them incentive to cooperate -- if they know
15 that if they fail to register and they engage in the
16 behavior, they're in trouble, they will have the
17 incentive to populate the list and participate in the
18 register and we will have solved the problem.

19 I don't think it's a hard technical problem to
20 create that list, especially when I know people can
21 invent easy ways to download it.

22 MS. RICH: Jerry and Mike, do you think this is
23 something that's feasible?

24 MR. HINTZE: Well, I think we certainly share
25 the goals that are being articulated here of workable

1 user controls that put the user in control of their
2 experience, and we think it's absolutely wonderful that
3 the consumer groups are throwing out these proposals to
4 get this conversation jumpstarted. We have to go back
5 and look at sort of the specifics of the proposal to
6 determine whether or not it's workable.

7 It's not a hard technical problem, but whether
8 economics, et cetera, support this to create dual
9 infrastructures, dual servers, where one may be used
10 today for delivering content and advertising. But,
11 absolutely, we're anxious to work with groups on this to
12 help come up with the best possible solution and
13 implementation.

14 MS. RICH: Jerry?

15 MR. CERASALE: I know enough technically to get
16 in trouble here. So, I'm going to stay out of the
17 technical side, although the fact I think technology has
18 come along and given choices and, so, I have faith in
19 technology. But I think we have to take a look at all
20 the downward consequences of the double kinds of servers,
21 two choices on the ads. I don't know how it works.

22 I do know the one thing that I can see that
23 bothers me is Europe is larger than the United States,
24 Europe has greater broadband than the United States,
25 Europe has greater penetration of mobile Internet than

1 the United States, and yet Europe's spending on
2 advertising is one-half of what's happening in the United
3 States. That spending, that money that comes in to
4 Google's, others -- to the Washington Post allows them to
5 have free content. And I'm very worried about that.

6 I'm worried about it in the following sense.
7 In an FTC -- I think it was FTC workshop or whatever, who
8 knows what it is they call them all the time, way back on
9 public information on the Internet, and it was talking
10 about property records and how people said having it on
11 the Internet changes the nature of the data because
12 anybody can receive it. So, rather than going to each
13 town hall looking it up, I could go on the Internet and
14 that made it a major problem. That was a privacy problem
15 issue.

16 And someone, I think it was the head of the
17 NAACP of Baltimore, came in and said, look, I can now
18 look and find out who owns that piece of property, but if
19 you don't allow it on the Internet, only the rich guy can
20 pay for someone to go to each town to try and find it.
21 So, I disagree with Jeff on his view of democratization
22 and I think free --

23 MR. CHESTER: It's a red herring.

24 MR. CERASALE: I think free -- please, Jeff, I
25 never interrupted you, Jeff.

1 And I think that free content is something we
2 have to watch out for when you look at any type of forced
3 regulation on the net and to try and keep it open because
4 I think that free content is democratization.

5 MS. RICH: Peter hasn't had much of a chance.
6 Let's take Peter, and then open it to a question or two.
7 We've run late.

8 MR. SWIRE: I had prepared various things to
9 talk about, none of which I talked about yet, which is
10 fine. We have a big panel with many different people.
11 But the free content point was something I wanted to talk
12 about, so maybe I'll just do a minute on that.

13 Content has to do with what newspapers you
14 read, what political sites you go to, things of that
15 sort. It includes that. We actually have a history in
16 the United States of laws about what is considered very
17 sensitive information, which is when you go and exercise
18 your First Amendment right to go see things and read
19 things, we have a whole set of laws in the United States
20 about that.

21 So, one of them is the Cable Television
22 Protection Act that was passed in the 1980s when cable
23 got big, and the instinct there was that we didn't all
24 want what we were watching on cable told to everybody. I
25 don't know why, I'll tell you what I'm watching, but

1 there might be somebody else who didn't want that. Then
2 next thing that happened was in 1988 when Judge Bork was
3 nominated for Supreme Court Justice is some enterprising
4 reporter went to see what movies he had rented at
5 Blockbuster, and some of you might remember the report
6 was extremely boring. He watched John Wayne movies
7 apparently. But, apparently, some members of the United
8 States Senate had watched some other stuff.

9 **(Laughter)**

10 MR. SWIRE: And within a couple of weeks
11 Congress passed the Video Privacy Protection Act that
12 said -- a hundred to nothing. They usually can't find a
13 hundred senators for anything, but they found a hundred
14 senators for this one. And that was sort of an
15 interesting thing.

16 There's similar rules to certain respects about
17 -- in phone companies under some of the CPNI rules, et
18 cetera, and there's similar rules where courts, such as
19 in the Tattered Cover Bookstore case, that put heightened
20 rules about seeing what a bookstore content has had.

21 So, I just sort of point this out if we're
22 talking about the Washington Post as our poster child for
23 the two days, is that when it comes to what you're doing
24 politically which is related to First Amendment, that's
25 actually been considered sensitive content under privacy

1 laws in the United States of America in the sense that
2 this has to do with your democratic, your political
3 views, is your boss going to see your political views, a
4 whole series of concerns like this.

5 So, part of the context that I don't think
6 we've heard in the last two days is that this editorial
7 content that's been used as we need wide open profiling
8 so that we can give you the Washington Post, is really a
9 funny thing to put around news and political debate, to
10 have widespread profiling on that. So, that's just a
11 different take on free editorial content.

12 There might be a lot of differences between
13 Europe and the United States. One thing I notice is that
14 languages are different, so the market for advertising in
15 Finnish is different from the American advertising in
16 English. And there's a lot of different reasons why
17 markets get big or get small and we have some advantages
18 in the United States. But I think this point that
19 profiling around people's what they're reading and what
20 they're saying and their political expression, there's a
21 history in the United States that that's been considered
22 something to be careful about. And I don't think that
23 theme has come out much in the last two days.

24 MS. RICH: But now it has. Do we have any
25 questions from the audience? Yes? No? Somebody is

1 adjusting the microphone.

2 MS. BRANDENBURG: Jessica, there's one over
3 here.

4 MS. RICH: Oh, excellent.

5 MR. BOHANAN: Mark Bohanan with the Software
6 and Information Industry Association. I apologize, I
7 missed some of this discussion. So, if this was
8 answered, forgive me.

9 I had a chance to study, I guess I got it from
10 Ari on Wednesday, the proposal. I think I'm still trying
11 to digest the diagram, but I look forward to
12 understanding it better. I just want to make sure I
13 understand the scope of the proposal because I think what
14 I've learned over the last two days is, in fact, we're
15 labeling as behavioral advertising, in fact, many
16 different things that are occurring.

17 And one thing I just want to be clear about, is
18 the proposal meant to address not only the kind of
19 advertising that we've described that is site specific as
20 well as network specific? Are we talking about requiring
21 people who do any kind of behavioral engagement with
22 their customers that is site specific? Is the
23 expectation they will need to register for this, too, if
24 technologically this is going to work?

25 MR. SCHWARTZ: I mean, you're right. I think

1 the proposal is somewhat vague on that point. And it's
2 not meant to be words that can be taken and put into
3 legislation. We meant it as a discussion document, and I
4 mean that more to address Mike's point that he wasn't
5 brought in. This is meant to start a dialogue, not to be
6 the end of a dialogue.

7 MR. BOHANAN: And my question is more just one
8 of information.

9 MR. SCHWARTZ: Right, no, I completely
10 understand that, Mark. And I think the response to you
11 is, I think, at least from my perspective, it was meant
12 to be a network-specific piece, not for specific sites.

13 So the question is, does that apply to sites --
14 to a company that has a network within itself? I think
15 that that's an open question. But in terms of a single
16 site that's doing behavioral targeting within that site,
17 I don't think anyone -- and I might be wrong and other
18 people here that worked on it with us can say whether
19 they meant it for a single site -- but I don't think that
20 that's what was intended. But it was intended mostly for
21 networks.

22 MR. BOHANAN: Just so I'm clear, for networks
23 as we traditionally understand the term as opposed to say
24 two related companies that may, in fact, engage in what
25 is very legitimate and appropriate consumer advertising

1 information. Again, we look forward to understanding
2 more, but that was one of the first questions I got which
3 was just what's the scope of this because, inevitably,
4 the good actors are the ones that are penalized. It's
5 the bad actors who are ultimately going to --

6 MR. SCHWARTZ: Exactly, that's true.

7 MS. BRANDENBURG: Let me suggest, because we're
8 running over and we have one more question from the
9 audience, that I encourage all of you to continue this
10 discussion both offline and later. This is a new
11 proposal and a very interesting one. So, let's hear from
12 our final question from the audience.

13 MS. GRANT: Hi, Susan Grant, National Consumers
14 League. Not a question so much as food for thought.

15 I'm a little troubled by some of the things
16 that I have been hearing today and yesterday. One is
17 that if consumers were that bothered by behavioral
18 marketing, they wouldn't be using the Internet so much.
19 But people want to use the Internet because of the great
20 benefits that it offers. Probably many of them don't
21 even know that behavioral marketing is happening. But
22 those who might, we've heard it's difficult for them to
23 do anything about it anyway. So, I think it's a fallacy
24 to say that this isn't a consumer issue.

25 The second thing that troubles me is what I'm

1 hearing from the Federal Trade Commission that let's try
2 to carve out some solution here that focuses on harm as
3 we would define it, that is sensitive information like
4 health information, and not taking into account the good
5 point that Peter made about civil discourse and not
6 taking into account the fact that as is enshrined in
7 Finland, people just have a basic human right to dignity,
8 to autonomy, and to be left alone.

9 So, if, as Mark greatly pointed out and as some
10 of the marketers have said over the last couple of days,
11 the aim is to give consumers what they want, let's find a
12 way to truly give consumers what they want, whether it's
13 this no tracking proposal or some other proposal which
14 I'm sure the smart people here can come up with. I'm not
15 going to be satisfied if we're not able to solve this.

16 MS. RICH: Susan, I just want to respond. When
17 I was asking about whether we could identify certain
18 practices that would be off the table, I was really
19 reflecting what I thought were some of the statements
20 that have been made in the last few days and just talking
21 about another alternative way to approach this as I was
22 trying to get out on the table many approaches.

23 The FTC is not pushing it. I was seeing if
24 there was movement there and there really wasn't.

25 MS. GRANT: But I heard yesterday harm, harm,

1 harm, harm, harm, and how harm is defined depends on the
2 consumer.

3 MR. CHESTER: We need enforceable rights here.
4 We need to implement our version of the OECD guidelines.
5 We need enforceable rights and we need to structure the
6 business practices based on privacy not just -- we worked
7 with Pam on that, but we don't think technical solutions
8 work. You have to structure the market so that privacy
9 is protected from the get-go.

10 MS. BRANDENBURG: Great. Thank you so much and
11 for everybody's patience. I know this is a very dynamic
12 area and I am confident that we'll continue to discuss it
13 afterwards. We are going to take a break and be back
14 here at 3:45 for our final panel.

15 **(Applause)**

16 **(A brief recess was taken)**

17

18

19

20

21

22

23

24

25

1 **SESSION 9: ROUNDTABLE ON THE FUTURE OF**
2 **BEHAVIORAL ADVERTISING**

3 MR. QUARESIMA: We'd like to welcome everyone
4 to the final panel, Session 9 on the future of behavioral
5 advertising. Format, we'll begin with three brief
6 presentations, then we'll move to a moderated discussion.

7 MR. HINE: I'd like to first introduce
8 everybody who is on the panel. Starting from my far
9 right, we have Katherine Albrecht from CASPIAN. To her
10 left, we have Zulfikar Ramzan from Symantec. To his
11 left, we have former Commissioner Mozelle Thompson from
12 Thompson Strategic Consulting. To his left, we have
13 Jules Polonetsky from American Online. To my right, I
14 have Alissa Cooper from the Center for Democracy and
15 Technology.

16 My name is Jamie Hine. I'm an attorney with
17 the Division of Privacy and Identity Protection here at
18 the FTC. To my left, I have Rick Quaresima who's with
19 the Division of Advertising Practices here at the Federal
20 Trade Commission. To his left, we have Robert Gratchner
21 from aQuantive. To Robert's left, Scott Shipman from
22 eBay. To Scott's left, John Thorne from Verizon. To
23 John's left, Joseph DeMarco from DeVore and DeMarco. To
24 Joseph's left, Brad Schuelke from the Office of Texas
25 Attorney General. And last, but not least, on the far

1 left, we have Tim Lordan from the Internet Education
2 Foundation.

3 I'm going to turn it over now to Katherine
4 Albrecht.

5 MS. ALBRECHT: Great. Well, I'm going to kick
6 this off with a bang. I have very limited time, so I'm
7 going to go quickly through these slides.

8 What we're doing here in talking about online
9 marketing and tracking consumers online, I think is going
10 to be setting a precedent for what's going to be coming
11 down the road in the future involving people and real-
12 world cookies. There's a couple of examples of how
13 people tried to do this in the past.

14 IBM, at one point, actually took out a patent
15 and considered a way to spray tracking ink on people's
16 shoes so they could actually mark them in a way similar
17 to an online cookie and then track them around the store.
18 And the idea was that they would actually step on a
19 little hidden unit in the floor that would be an
20 applicator that would spray some electromagnetic ink on
21 their shoe and program an individual code to them and
22 then put a little puff of air and then dry it quickly so
23 that it would be unobtrusive, the consumer wouldn't
24 notice it. And then they would have little devices
25 around the store in the floor that would actually see

1 where they browsed, how long they stood and what they
2 looked at, so that they could be tracked. Of course,
3 this ink would be invisible and consumers would not know
4 about it.

5 Well, they're not going to have to go to all
6 that bother if things continue along this present path
7 because with RFID tags now being planned to replace the
8 barcode to be sandwiched into shoes and clothing, you can
9 do the same with less muss and a lot less bother.

10 An RFID tag, I'm sure most people in the room
11 are familiar with RFID, the idea is to, at some point,
12 place one of these on to every consumer product
13 manufactured on planet Earth. So, there would literally
14 be one in every pair of shoes, every belt, every
15 lightbulb, every Bic pen, you name it, would all be
16 equipped with their own remotely readable miniature
17 tracking devices containing information very similar to
18 what is in a cookie file.

19 Already they're appearing in passports. All
20 new passports issued by the State Department contain an
21 RFID tag. Over 20 million contactless credit cards that
22 have been issued in the United States contain this
23 technology. And, of course, loyalty cards already sort
24 of span that consumer marketing tool. It's a consumer
25 marketing tool that many people carry in their wallets.

1 In fact, it's the topic of my doctoral dissertation at
2 Harvard University.

3 I discovered by the way -- I'll just throw this
4 out apropos of some other topics that have been discussed
5 -- that 75 percent of American consumers do not recognize
6 that their loyalty card is used to collect their personal
7 information or to make a record of what they buy, and I
8 would be happy to provide that data to anyone who would
9 like to follow up on that.

10 One of the plans by NCR, the National Cash
11 Register Corporation, which is the technology partner for
12 Wal-Mart, is actually to use RFID on consumers in order
13 to track them around the store and charge them different
14 prices for different items depending on individual
15 characteristics of those consumers as gleaned from these
16 tags.

17 The idea is that if you have one of these in
18 your wallet or your purse or your backpack or your
19 pocket, because radio waves travel right through fabric,
20 leather and plastic, they would be able to read these
21 tags on your person without your knowledge, and
22 presumably without your permission, so that as you walk
23 through doorway portals -- and here you see one, the
24 normal one that we're used to seeing for anti-theft
25 purposes, those can be upgraded to become RFID readers

1 and read these tags.

2 They are also now creating ones that can go
3 horizontally so that they can scan you in a nice wide
4 open space and you would never even know it was there.

5 I'm going to skip this one because we're low on
6 time. IBM probably does the best job in one of their
7 patents in describing how this would be used to track
8 consumers, and they've patented something they call the
9 person tracking unit. What this person tracking unit is,
10 it's an RFID reader that picks up these signals from
11 people's belongings and they can place them in walls,
12 floor, ceiling tiles, shelving, doorways, literally
13 anywhere, and they discuss a desire to place these into
14 public spaces like museums, theaters, libraries, even
15 elevators and public restrooms. So, literally everywhere
16 you go, you could be scanned.

17 Now, the best way to understand how this works,
18 they spell out in their patent, is because each RFID tag
19 has a unique ID number, it's kind of like a unique cookie
20 number, and it can be linked to your identity. So, for
21 example, if you sell me a pair of shoes that has unique
22 ID number 308247 in a cookie embedded into the soul, then
23 any time in the future you see unique ID number 308247,
24 because that's the only object on Earth that will
25 transmit that number presumably, then you can look that

1 up in your database and you can say, well, that number
2 corresponds to a pair of size eight Nike running shoes
3 that Katherine Albrecht bought here last month.
4 Therefore, there's a pretty good chance she was standing
5 in it. So, you can use it to track people.

6 You can also use it, as IBM describes I think
7 very well here, to look inside of people's purses. Their
8 example was to look inside of a woman's sealed purse, and
9 because all of the objects in her purse would carry one
10 of these remotely readable tags on it, you could do an
11 inventory of everything she was wearing and carrying.
12 And their example if she's carrying a baby bottle then
13 you can presume she's a new mother and then you could
14 target her for other types of products. So, presumably
15 when she'd walk by a billboard, the billboard might run
16 an ad for diapers.

17 Japan has actually been testing this now with a
18 slight twist, and this is actually more like the video
19 that we saw in one of the earlier presentations, where
20 the guy had the Post-It notes stuck all over him. What
21 Japan has done, funded by the Japanese government in
22 conjunction with NTT DoCoMo, is they issued shoppers in
23 the Ginza shopping district in Tokyo RFID reader cell
24 phones and then they placed the cookie, the little RFID
25 cookies in the doorways of stores, and as people walked

1 into the stores their cell phones, unbeknownst to them,
2 would grab information from the cookie and keep a record
3 of everywhere they had been. Then when they walked into
4 other stores, all of that information could be
5 downloaded. So, a complete record of their travels,
6 their interests, what they had browsed and where they had
7 been would be available to other stores that were part of
8 the system.

9 Bank of America has a similar plan, this is
10 also a patent. And this particular device, you walk up
11 to a billboard and it would identify, collect, gather,
12 and use personal information about you, again, using
13 these real world cookies in your belongings.

14 There are plans to scan the tags in people's
15 garbage developed by BellSouth. This is an idea when you
16 throw these things away -- because the industry says,
17 well, we'll just put them on the packaging, don't worry.
18 Well, when you throw them away, they came up with a plan
19 to actually scan your garbage at the dump and figure how
20 long it had taken you to use up that bottle of shampoo or
21 whether you traveled with that bag of dog food. Those
22 are literally examples that they provide, and making that
23 information, of course, available to retailers,
24 manufacturers, distributors, and the like for marketing
25 purposes.

1 This was one of my favorites. Phillips
2 Electronics actually looks forward to the day when in
3 consumer's homes they will have appliances hooked up to
4 the Internet so that they can use the RFID reader
5 capability. So, their idea here on a saw is that you
6 could put some blueprints on there, download information.
7 Well, they say, well, wouldn't it be great, though,
8 because you could be able to capture hidden information
9 about other things people do in their homes.

10 So, if someone's eating cereal as a snack and
11 they set down the Cap'n Crunch -- they literally say this
12 -- on their table saw, that at that point you can capture
13 that, you can download it and you can make it available
14 to marketers who could then direct market to this person
15 who likes to eat cereal as a snack.

16 It is my belief that this is extraordinarily
17 harmful to consumers. The customer segmentation model
18 that says we want to know what people are doing all the
19 time so that we can scrape them off the hull of the ship,
20 this is from the Harvard Business Review referring to not
21 profitable customers as problematic and like barnacles on
22 the hull of a cargo ship that only create additional
23 drag. These, of course, are people who are not pulling
24 their weight by being profitable enough to the companies.

25 Then, finally, it appears to me that the

1 marketing industry, rather than opposing these practices,
2 has actually condoned them, referring to them as a
3 practice called digital redlining, meaning marginal
4 services and high prices designed to drive the
5 unattractive customer somewhere else.

6 So, I think if we allow this to happen in the
7 online world, if we do not take steps at this point to at
8 least say that these practices are objectionable and to
9 look more closely at them, then down the road we could
10 actually be creating an infrastructure in which
11 everything we do would be tracked all the time.

12 If you have any further questions on this, we
13 have two websites, spychips.com about product tagging,
14 and we have a new website up at antichips.com, which
15 deals with the actual injection of these devices into
16 human beings in the form of RFID implants.

17 We'll talk more when we get to the Q&A section.
18 Thank you.

19 UNIDENTIFIED MALE: What was the second one?

20 MS. ALBRECHT: Spychips.com and antichips.com.
21 Thank you.

22 **(Applause)**

23 MR. HINE: We'll have time for questions
24 afterwards.

25 We're going to move to the second presentation

1 from Zulfikar Ramzan from Symantec.

2 MR. RAMZAN: Thank you for making it this long
3 in the day. I was kind of worried about giving a
4 presentation at 3:30 on a Friday, but you've lasted.

5 So, I'll talk a bit about some of the new
6 consumer technologies. I'm only going to spend about
7 five minutes or so describing them. There are two
8 particular technologies I wanted to mention which I
9 thought were relevant to this particular discussion. One
10 is something called Browser Defender and another is
11 called Identity Safe, and I'll explain what these are
12 shortly.

13 So, let me start with Browser Defender. As we
14 all know, the web browser has now become the conduit for
15 most people's online computing experience. They don't
16 really talk about using the operating system or Windows,
17 or anything like that. It's all about what do I do on
18 IE, what do I do on Firefox, and so on and so forth.

19 Attackers have realized the same thing. They
20 know that if people are spending most of their time
21 online using the web browser, that is the most viable
22 place for attackers to try to target individuals.

23 What's interesting is -- I'm not sure if most
24 people know this, but the most commonly targeted person
25 on the Internet is the individual consumer. Ninety-five

1 percent of targeted attacks go after consumers. They
2 don't go after businesses or banks and that sort of
3 thing. It's all about the end person, which is something
4 most people don't realize.

5 So, oftentimes, these attackers are just trying
6 to leverage flaws in your browser. These are software
7 products out there, they often have technical
8 vulnerabilities. Those vulnerabilities can be exploited
9 by another piece of software. And, as I highlighted,
10 some of this software is available through toolkits.
11 So, in fact, you don't need to have technical
12 sophistication to compromise someone's website or
13 someone's browser. All you need is the ability to buy a
14 toolkit online or through an underground market.

15 The going rate for one of the most recent
16 toolkits, something called Impact, was about a thousand
17 dollars for the toolkit, and that actually included a
18 one-year support contract. So, if you had any problems,
19 you could contact customer support of the toolkit seller.
20 I'm serious actually. It did include a one-year support
21 contract.

22 So, the reality is that it's taken a lot of the
23 difficulty out of the equation. The whole market has
24 become, in some sense, commoditized. Attackers also are
25 not just going after free sites. It's not like I can

1 tell you don't go to some known site. The reality is a
2 lot of these attackers are going after well-known sites.

3 So, in fact, here are a few examples I've put
4 on the slide. The most famous one, I think, in the last
5 year or so was the Dolphin Stadium website being targeted
6 just around the time of the Superbowl. So, they were
7 compromised. The attacker was able to insert a piece of
8 code on the website so that if you visited the site and
9 your browser was not fully patched, your computer would
10 effectively become compromised and your attacker could
11 essentially control that computer remotely and make it do
12 whatever it wanted, which is a scary thought. You'd have
13 to do nothing more than just look at the site at the
14 wrong time.

15 The other thing that attackers are doing, this
16 really ties into this particular panel, is use of
17 advertising networks to make some of this happen. So,
18 the realities that advertising is not just about a text
19 image or it's not just about sound, the reality is
20 advertising has gotten so complex and so rich in terms of
21 content that there are effectively pieces of software now
22 running inside of an advertisement. So, that piece of
23 software can be malicious and an attacker can potentially
24 get that software on to a website, and this actually
25 happened with MySpace.

1 So, MySpace accidentally hosted an
2 advertisement that happened to contain malicious code.
3 That code could take advantage of a browser vulnerability
4 and could exploit that machine and essentially allow an
5 attacker to take control of it. It turns out when
6 MySpace had this happen to them, a million people
7 actually saw the advertisement. Now, those people --
8 maybe some of them had their computer security software
9 up to date and their browser up to date, but I think that
10 the odds are that most people didn't. So, it's a scary
11 thought.

12 With that said, the good news is that we have
13 technologies in place to try to deal with those kinds of
14 issues. We designed a new technology called Web Browser
15 Defender. It actually does proactive detection, so it
16 can detect any attempt by a piece of malicious software
17 to take control over your machine through your browser
18 and block that attempt. Actually, because it's proactive
19 and because it's behavior-based, it can not only detect
20 all the known threats, it can also detect many of the
21 unknown threats out there. I thought that was an
22 important type of detection mechanism especially since
23 most people are using the browser these days.

24 It's included in the Norton Anti-Virus line of
25 products and in the Norton Internet Security line of

1 products that are coming out in 2008.

2 Finally, I want to talk briefly about something
3 called Identity Safe. The reality is, as I mentioned
4 earlier this morning, most people have multiple online
5 identities. I have an identity with my email provider,
6 I've got an identity that's associated with, let's say, a
7 merchant I do banking with. I've got an identity
8 associated with any kind of social networking forum I'm
9 part of, so on and so forth. Each of those identities
10 contains with it a set of information about me, like an
11 email address, passwords and so on and so forth.

12 One of the challenges we're seeing is that
13 because people have so many identities, it's hard to
14 manage all of them. How many people here have multiple
15 passwords they use online and multiple accounts? I think
16 most of us do. How many people have more than five? I
17 would say some people have even more than that. So,
18 that's quite a few accounts you have to manage.

19 We've realized that's something that is very
20 difficult for consumers to do, so we're building a
21 technology now that has the ability to manage these
22 online identities, and that can include things like
23 taking care of your passwords, being able to detect if
24 you're about to enter your password into a fraudulent
25 website, automatically being able to switch between

1 different identities for different sites. So, you don't
2 need to manage that stuff any more.

3 The idea is that we're trying to use technology
4 to simplify a lot of the problems that users are facing
5 because the reality is most people, when they do transact
6 online, their interests are not in their own safety and
7 security and privacy. Their interest is in doing what
8 they want to do online, like buy a product, so on and so
9 forth. We want to take all the guesswork out and make
10 the decision much easier for typical end users.

11 So, that's actually all I wanted to say, and
12 thank you for your time.

13 **(Applause)**

14 MR. HINE: Thank you. Our final presentation
15 is Commissioner Mozelle Thompson from Thompson Strategic
16 Consulting.

17 MR. THOMPSON: Good afternoon, everyone. The
18 first thing I wanted to do is I wanted to thank the FTC
19 for holding these two days of sessions. It's been a very
20 interesting opportunity to have a good conversation about
21 where things are going in the world of advertising,
22 especially in targeted advertising.

23 I see Commissioner Harbour here, and it's nice
24 to know, at least for me, that I still have the ability
25 to clear the room.

1 **(Laughter)**

2 MR. THOMPSON: I thought a good place to start
3 was just a few observations, that it wasn't very long
4 ago, in fact November 1999, when the FTC did a workshop
5 in online profiling. Stemming from that workshop, in
6 July 2000, the majority of the Commission, including
7 myself, sent a report and recommendations to Congress on
8 online profiling outlining some of the NAI principles.
9 But, also, I took the step of saying that we should have
10 some legislation in this area to establish the baseline
11 of privacy protections.

12 Let's fast forward. I'm not a big one to say I
13 told you so, but I do think that this was an area where
14 we had an opportunity. The opportunity is different now.
15 Let's talk a little bit about what's happened since then,
16 and I'll tell you why.

17 The online industry has changed quite a bit.
18 We have a lot more privacy policies and privacy tools.
19 We have seen an array of free services that are available
20 to the public. We've seen interesting new ways that
21 users are generating their own material and finding ways
22 to distribute that among themselves. The technological
23 changes also means that there's greater ability to
24 transmit and gather information, and greater ability for
25 a lot of people to search for that information. But

1 there are also a greater array of tools to manage
2 information.

3 We also see that users have changed. You know,
4 we have a generation of people out there right now who
5 have always known the Internet, who have never known what
6 it was like not to be online, and they have a mixture of
7 impressions. On one hand, they may not be as
8 sophisticated in understanding some of their risks, but
9 they are much more savvy in how they use information and,
10 in a strategic way, to decide for themselves what value
11 they expect to get from their participation.

12 Now, we may have some differences about whether
13 it's a long-term value or a short-term value. But it's
14 clear to me that we have a lot more people out there who
15 are making those decisions every day. So, I thought it
16 was interesting also to sit through the past couple of
17 days, and I was struck by also a few things that remain
18 as myths, that remain unspoken. But I would like to talk
19 a little bit about them.

20 The first is the idea that profiling or
21 tracking users or consumers is new. It's not. It
22 happens offline, it happens online. Now, we may have
23 more tools available to do it, but ever since there's
24 been commerce and ever since there's been advertising,
25 people are trying to figure out a better way to reach

1 their target market and figure out the better way to
2 spend their money more efficiently to do so. That has
3 not changed.

4 How it manifests itself in an online world and
5 the tools available to do that, that may be a little
6 different and evolves over time.

7 Second, there's this lingering impression among
8 some people that the public is dumb, and they're not.
9 They are perfectly willing to exercise choices. Now,
10 some of them may be misinformed or uninformed, but they
11 make rational choices based on what they know and what
12 they assess is their own value at the time they exercise
13 their choices.

14 Another myth is that the FTC's role is somehow
15 to take legal action without clearly articulated harms,
16 and I don't think that's true either. What that means is
17 there may not be consensus on what those harms and risks
18 are, but the FTC has a broad number of mandates,
19 including the ability to shine the spotlight on the
20 issues that we hear of today. But in order to take
21 enforcement action, there has to be some clear
22 articulation.

23 And, finally, and this is the thing that
24 concerned me then and concerns me now, is that the
25 primary risk to consumers are not posed by the people who

1 are here in this room. They are people who are engaged
2 in unscrupulous practices, who have technologies that are
3 there to surreptitiously spy and take information from
4 people, and that they don't feel like they have any
5 obligation to comply with any of the self-regulatory or
6 regulatory codes that are out there.

7 So, what that means for us, I think, in the
8 future is a couple of things. There's still a large gap
9 between what consumers and users know and what they need
10 to know. And while there are various sites who are doing
11 an admirable job to try to better inform consumers and
12 also public interest groups who are trying to do the same
13 and governments, there's still a great opportunity, in a
14 coordinated fashion, to provide more sophisticated
15 information to users.

16 Second, there's still an opportunity for
17 government, consumer groups and businesses to innovate
18 this area because you guys are the experts in what's
19 going on and what are the things that people are
20 interested in. I think the opportunity is to spend
21 one-tenth of 1 percent of your creative talent trying to
22 figure out what are the new tools that you can come up
23 with that will make it better for everyone.

24 And, finally, this is a challenge that I see
25 advising especially technology companies, how do you

1 create a market that actually rewards or raises to the
2 top instead of the bottom? How do you create a
3 marketplace that rewards companies who give strong
4 privacy tools, that gives choices, that tell consumers
5 and users what they're doing with information?

6 I see that there are some companies who are out
7 there that are doing that, and I think what I am seeing
8 is more and more consumers are flocking to those
9 companies because they represent something that always is
10 important in any marketplace, the trust between the
11 consumer and the vendor. Thanks.

12 **(Applause)**

13 MR. QUARESIMA: Thank you. Well, thank you
14 again to all our presenters. I want to start with some
15 things that have been referenced earlier, but we haven't
16 had a chance to dig deep. Some of that right off the top
17 is are there alternatives to cookies likely to emerge as
18 identifiers of consumers' Internet behavior? So, I
19 thought we could make that a general question, but I
20 think I would like to begin with you, Jules.

21 MR. POLONETSKY: So, let me share some other
22 secrets about cookies because you heard about how the
23 opt-outs are imperfect and you heard of all sorts of
24 interesting challenges that cookies face. So, let me put
25 on the business hat as well.

1 The interesting thing about cookies is that
2 they're not perfect. They're not perfect for ad delivery
3 or targeting. In fact, there was some comment that only
4 5 percent of the people managed to understand how to
5 control cookies. The reality is, if you sit in a room of
6 advertisers and marketers, they'll tell you that, hey,
7 where are the cookies going? Twenty percent, 30 percent,
8 40 percent, the industry is sort of constantly debating
9 studies that wonder where are the cookies going.

10 Well, some are removed by Symantec and Macfee
11 and anti-spyware programs that automatically remove
12 cookies. A lot of them, apparently, are being removed by
13 people who somehow have figured out how to use the
14 browser controls. Lots of them are being blocked by P3P.
15 So, the disadvantage of cookies is, in some ways, a real
16 advantage.

17 Years ago, the fact that you had to send
18 lawyers to courthouses to get data gave us privacy.
19 Today, the limitations of cookies, which are reflected in
20 the imperfect manner to deal with them, is that there are
21 all these tools built around them and they're not
22 actually -- they're good enough, right? People have
23 built entire business models, all the big companies in
24 this room and all the networks have business models, and
25 the vast majority of ad delivery and content analytics is

1 completely built around this kind of shaky, good enough
2 because, frankly, it works, but it's quite imperfect.

3 So, I think it's a remarkable thing that seven
4 years later, from the conversations that we had years
5 ago, you still see people using cookies. One of the
6 reasons why I think some of the privacy compliance people
7 like me at many of the companies look at these flash
8 cookies and other novel tracking uses and we say, well,
9 wait a second, the cookie has some controls, it isn't
10 perfect. But until you come up with some really good way
11 to make an effective way for users to control that,
12 that's not something that's fair to use in an
13 extraordinarily robust way.

14 So, I think that looking into the future,
15 you're going to see technologies -- cookies or very
16 similar to cookies that actually have user controls.
17 People are looking at mobile today obviously, and there
18 are not yet ubiquitous mobile cookies. One of the
19 problems that's sort of being scratched and thought about
20 is, well, okay, probably mobile is an example where
21 people really will want my address remembered or the
22 things that I don't want to have to punch in so that I
23 can instantly get my directions or whatever the case is.
24 What are the ways that you're really going to put
25 somebody in control so as not to have them running in a

1 different direction?

2 So, my prediction is that both the -- we really
3 should spend a good deal of time focusing on how to
4 ensure that the cookie-handling model, which is going to
5 be with us for quite a while, the business models are
6 built around it and a huge amount of preferences and
7 control and browsers are built around it. So, we really
8 should engage more with getting the cookie structure
9 right.

10 MR. QUARESIMA: Tim, are new mobile
11 technologies using something else?

12 MR. LORDAN: Are they using something else?
13 Well, I think since 2000 -- we did our first
14 congressional briefing on location advertising back in
15 2000. It's remarkable to think back then that we
16 actually were doing congressional briefing as a
17 legislative issue on this issue seven years ago. I don't
18 think we kind of understood the issue, but we knew that
19 being built into phones were different triangulation and
20 GPS chips and, ultimately, after 9/11 we had the act that
21 allowed every one of these devices to be located for
22 E-911 purposes.

23 And every year since then I swear I have been
24 like, this is the year this thing is really going to open
25 up. And it just is this pregnant pause where this

1 marketplace of all this -- this becoming a new cookie
2 just doesn't happen. The marketplace is glacial in its
3 implementation. Probably for consumers that might be a
4 good thing.

5 The other thing is that for the past week I
6 have been carrying around a phone, it's one of the only
7 like location services, it's called Looped, Sprint uses
8 it, there's very few, some are for child protection, but
9 this one is like a social networking type thing. It's
10 pretty cool. I have a map on the phone, I can see where
11 all my friends are, and I was really excited about it.
12 And then after a few days, I realized that not only did I
13 and my friends live really boring lives, it didn't give
14 me the granularity that I want, that I thought would be
15 interesting. Basically I go from home, I go to work, I
16 go from home, I go to work. Then I go to the Federal
17 Trade Commission. Really exciting stuff.

18 **(Laughter)**

19 MR. LORDAN: So we have some 20 somethings in
20 the office and they were going on a trip to Los Angeles.
21 We have two of these phones. And they go, can we take
22 them to LA and we'll play around with it. I said, yeah,
23 sure, take it with you. We're going to a USC football
24 game. Can I see her on the other side of the stadium?
25 I'm like, no, no, it's not that granular.

1 Well, if we're in a different part of the bar
2 and I'm talking to some guy and she's talking to another,
3 can I see where she is? No, it's not that granular. And
4 I think the thing is that these things aren't that
5 granular, first of all, when it comes to mobile phones.

6 And, secondly, I've learned a lot here. If you
7 are going to track people, where they literally go in the
8 physical space as you do on Myspace or on the Internet,
9 you have to have some kind of delivery mechanism, right?
10 You have to deliver the ad somehow. And how do you do
11 that? Supermarket aisles have those coupon feeders,
12 you're walking down the aisle and they're shooting
13 coupons at you and you're like -- or you get a text
14 message. That's the really trite hackneyed example is
15 that I'm walking by a Starbucks and they're going to send
16 me a dollar off latte example. I think the professor
17 from Amherst had a chart that said the advertisements
18 that consumers find most annoying and I think the top one
19 was getting a text message, it's like getting a phone
20 call at dinner.

21 And how you present the advertisement -- and I
22 think there's a pretty compressed short window where you
23 could do that and actually convert a sale. Somebody said
24 data is good online for like three hours. If you're
25 walking by the Starbucks, you have like ten seconds where

1 they're on another block. How do you present the ad in a
2 way that doesn't annoy them?

3 So, I think that's a combination of factors
4 that's really making this process really glacial. I see
5 the most dynamic aspect of location, locating people, and
6 self-reporting. Online people are twittering, people are
7 disclosing their information on their blogs, on their
8 social network sites. And that is, by far, the fastest-
9 growing location technology there is, and that's
10 basically just pure social networking.

11 What I would say is if you don't want people to
12 know your location on a social networking site, don't
13 disclose it. One thing I find interesting in this new
14 paradigm of social networking is people are like just
15 vomiting their personal information, every aspect of
16 their lives online. It's like digital data diarrhea.
17 But even that is like diarrhea of the mouth, put it's
18 like diarrhea of texting and the keyboard. People have
19 to take responsibility for that. I think that's -- I'm
20 going to stop there on digital diarrhea.

21 **(Laughter)**

22 MR. QUARESIMA: Thanks, Tim. I'm glad we
23 didn't do this right after lunch. I'm actually going to
24 come back to mobile in a bit, but I would like to turn it
25 to Alissa. And, Alissa, if you see other alternatives to

1 cookies as far as tracking and monitoring Internet
2 behavior.

3 MS. COOPER: I think this came up yesterday and
4 it's a model that we, at CDT, have taken a great interest
5 in in recent months, and it involves ISPs.

6 So, a lot of what we have been talking about
7 the last two days at this workshop is all about
8 advertising on the web and how the big ad networks are --
9 they're big because they're on a lot of sites. So, if an
10 ad network can track you across the top thousand sites on
11 the web, the top 10,000 sites, whatever it may be, the
12 more sites where they can gather information about you
13 the theory is the better they can target advertisements
14 to you, the more they can collect about you.

15 If you think about your ISP, no one knows more
16 or is in a position to know more about what you do online
17 than your ISP because your ISP can see everything that
18 you do. So, if we're talking about competing with an ad
19 network that has visibility on a thousand sites, well,
20 your ISP has visibility on every site. And this is a
21 model that we started hearing about recently where, not
22 that I know of it actually happening on any of the major
23 ISPs in the U.S., but an ISP partnering with an ad
24 network company to serve the information that the ISPs
25 gather to the ad network and then the ad network can use

1 that information to target ads just like they do on the
2 web, except now they can see everything that you do.

3 So, some of the companies that are doing this,
4 there's one called Nabu Ad, which thanks to Jules I
5 learned about recently. Just got a second round of
6 funding, \$30 million venture funding for Nabu Ad.
7 Adzilla is an American company, \$10 million in venture
8 funding. There's a UK company called form PHORM, P-H-O-
9 R-M, which has a market cap of half a billion dollars.

10 So, it does seem as though this ISP model where
11 not just a few websites that you visit or your search
12 history, but everything that you do online could be
13 involved in the creation of the profile about you and
14 that certainly goes beyond cookies, it goes beyond flash
15 cookies, it goes beyond any of these other web-based
16 technologies.

17 MR. QUARESIMA: Just a point, if anybody in the
18 audience has any questions, the mics are open and please
19 step up. I'm actually going to come back to the
20 ISP-based technology shortly, but I just wanted to throw
21 this open to anybody else on the panel who is aware of
22 other technologies besides cookies that they believe is
23 going to become prevalent in the near future.

24 MR. THOMPSON: I wonder if the question is
25 really the cookie question, and I'll explain why. If

1 it's not a cookie, it will be something else because
2 there's still a demand, and it's ever increasing, for
3 what I call mass customization, that you have 10,000
4 users and each expect a different experience. And they
5 expect you to deliver to them on a real-time basis, and
6 what that means is that you're going to need to know
7 something about each one of those people.

8 So, if it's not a cookie, technology changes
9 every day, but as long as there's a demand for customized
10 services, especially in the online environment, that's
11 always going to be a challenge.

12 MR. QUARESIMA: Okay, I just want to revisit
13 the ISP model that Alissa had spoken about. This type of
14 model probably raises both legal and business questions.

15 So, first, I want to turn to the legal
16 questions. I'll throw this for Joe DeMarco. Joe, do you
17 see any different legal framework for this at the ISP
18 level?

19 MR. DeMARCO: I do, Rick, and just by way of
20 background, I was a federal prosecutor for ten years and
21 I headed the computer hacking unit in the U.S. Attorney's
22 Office in New York where I routinely prosecuted
23 wiretappers and computer hackers. And over the last few
24 days, I've sort of been listening to and listening for
25 the raising of the wiretapping and computer hacking

1 issues, as well as the associated intellectual property
2 rights issues. I think this really does hit the nail
3 right on the head.

4 That's because as complex and as difficult as
5 the issues are of consent and notice when you're dealing
6 with a consumer and another party like a website, and
7 those issues are very, very difficult, the difficulty in
8 terms of the legal analysis and the permissibility
9 becomes yet even more complex when you're talking about
10 the monitoring of content by a provider of pipe, whether
11 that pipe is an Internet service provider or a
12 telecommunications company.

13 And when you start talking about things like
14 deep packet inspection or any type of analysis of data
15 flows, as that is traversing the network by the network
16 provider, by an ISP or by the phone company, you
17 immediately raise the issue of the Wiretap Act. Now, the
18 Wiretap Act makes it a crime as well as a tort, a federal
19 tort, to listen in on people's conversations, whether
20 those conversations are on the phone or over the
21 Internet. It applies to content, and that raises a whole
22 host of tricky questions.

23 At one end of the spectrum you could say, well,
24 an IP address is not content so you're not really looking
25 at the contents of a communication if you're just looking

1 at people's IP addresses. At the other end of the
2 spectrum, if you're a provider, if you're an ISP looking
3 at the content of someone's emails and you're not a party
4 to that email, you probably are getting into some content
5 issues. But I think it raises very, very important
6 questions under the Wiretap Act.

7 My recommendation to everyone is as you think
8 about the deployment of these new technologies, which I
9 personally believe are going to involve things like deep
10 packet inspection, which of course is just carnivore
11 renamed. I mean, it's the same sort of technology which
12 looks at contents as they traverse a network. As you're
13 talking about that and thinking about that, from the
14 point of view of a provider, you really need to start
15 thinking about are you violating the Federal Wiretap Act.

16
17 Similarly, I heard in the last panel mention of
18 the ability of various companies to turn on cookies that
19 had previously been disabled. I think that raises issues
20 under the computer hacking statutes.

21 So, I'm not saying this technology is bad, I'm
22 not saying it's good. I think that as you do the
23 analysis about whether or not different legal regimes
24 apply, you have to consider whether you're monitoring
25 content, how you're monitoring it, who is consenting. And

1 interestingly, in the wiretap cases you have a very
2 robust and well-developed juris prudence of consent which
3 usually requires implied consent or actual consent. You
4 really need to be thinking about these things very, very
5 carefully and making sure that you get the legal analysis
6 right. Because if you get the legal analysis wrong you
7 not only have a business disaster, you've not only
8 committed a federal tort and are liable for damages, but
9 you could wind up in jail. And I think that is going to
10 be part of the future analysis of behavioral advertising.

11 MR. QUARESIMA: Just in the audience, Jeff?

12 **(Individual not at amplifying microphone)**

13 MR. CHESTER: I'm glad you brought that up,
14 because that (inaudible) -- I'm sorry.

15 Let's talk about rich media. Can someone talk
16 about the role of data collection via current practices
17 and future practices and the rich media, multi-media
18 units that are now deployed and will further evolve, and
19 also the role of virtual agents in terms of data
20 collection? Thank you.

21 MR QUARESIMA: Anybody want to take a crack at
22 that? No?

23 MR. THOMPSON: Don't all jump up at once.

24 MR. QUARESIMA: Okay. Then I'm going to
25 actually sort of circle back and just let me talk about

1 some of the maybe business ramifications. Assuming all
2 the legalities are there, what are the business
3 ramifications if this ISP model catches on? And maybe
4 I'll turn that over to Rob first since it's directly in
5 competition with yours.

6 MR. GRATCHNER: I just want to preface this by
7 saying at aQuantive we've just recently been acquired by
8 Microsoft, so the Microsoft ISP model is new to me and
9 I'm learning on a daily basis the new Microsoft model.
10 But I would like to go back to one thing about the new
11 technology and the law is is Jules is absolutely correct.
12 Cookies right now for online advertising and marketing is
13 the key technology. I don't foresee that changing any
14 time in the near future.

15 Now, that doesn't preclude other technologies
16 or other things happening in the future. So, every
17 business model may have different technology as we look
18 into video-on-demand or mobile marketing or other types
19 of technologies, as we evolve in the space, may require a
20 different type of technology besides the cookie.

21 So, one of the things that we need to make sure
22 as we go into this is that we understand what are the
23 consumer expectations. And the part of this that I think
24 has been left out is advertisers. What are the
25 advertisers' expectations and where do they play a role

1 in this? They've actually played a very big role in
2 this. As I've seen over the last two years I have been
3 at aQuantive, advertisers really want companies who are
4 doing the right thing. They want to make sure that
5 they're handling data appropriately. Not only do we see
6 it as a business value add to advertisers that we do
7 things right with privacy, but these companies are coming
8 to the companies that are doing things right like
9 aQuantive, like the other members of the NAI.

10 And, so, as we go and expand into these new
11 realms and these future technologies, we need to make
12 sure that we have things baked into our technology
13 similar to the Microsoft principles, as I'm learning, on
14 product development and understanding how privacy plays a
15 role around notice and choice. We have the same
16 principles at aQuantive and we want to make sure that as
17 we develop new technologies and go in new areas for our
18 advertisers, that we understand and we provide the notice
19 and choice to folks and that we're transparent.

20 MR. POLONETSKY: The big thing that has changed
21 when it comes to ad technology, because most of these
22 issues in the data collection and so forth again have not
23 substantially changed. What you couldn't do easily years
24 ago was actually the smoothness of the implementation.

25 So, let me give you an example. Banner ads,

1 years ago, were indeed a banner ad. We acquired a mobile
2 company maybe a year ago called Third Screen Media, and I
3 remember having conversations years ago when I was at
4 DoubleClick about, well, how could our mobile ad server
5 make sure that nobody accidentally sent us personal data
6 and kind of have like a screen that would catch stuff if
7 someone sent it that we didn't want and sort of going
8 through the issues.

9 And here we were years later and I said, okay,
10 I'm expecting all kinds of interesting, intricate, new
11 challenges, and it turns out their greatest advantage and
12 the reason they're considered sort of a leader is there's
13 lots of phones and browsers and this and all kind of
14 formats, and it is a bear to actually get a couple of
15 different creatives for one advertiser on to lots of
16 different phones in different structures. That's new,
17 and the leaders are first figuring that out on the mobile
18 side. That's what actually has happened in a substantial
19 way on the ad side.

20 So, whether it's rich media, whether it's the
21 ability to deliver video, the ability to create ads on
22 the fly, the implementation and the ability to actually
23 get the ad where you wanted it. So, perhaps years ago an
24 ad server could deliver one of 200 ads that it has for
25 the right advertiser. But if you were an advertiser and

1 you were going to deliver an ad with an ad server, you
2 didn't have 200 ads for 200 potential types of customers.

3 And if you somehow spent a lot of money with
4 all kinds of creative shops and you created 200 ads and
5 you had them sitting there, the ability to sort and get
6 the right one just wasn't possible. Today, sophisticated
7 advertisers indeed can morph together and create the ad.
8 So, the technology has smoothed out and so a lot of what
9 was envisioned years ago is actually finally happening in
10 a smooth way.

11 There used to be a career. It was called dart
12 trafficker, and it was people who went to sort of a
13 special training course to learn how to get their ads and
14 use the interface to get their ads, if you were an
15 advertiser, on a publisher site. That career is gone
16 because most of us in the room today, technical or not,
17 could sort of sit down and puzzle out and probably
18 accomplish running -- and, indeed, there are millions of
19 people around the world who run ads on Google and are on
20 Ad.com just by using some of the tools that are out
21 there. So, that's really what's happened with the
22 richness of media.

23 MR. DeMARCO: Could I add a point though on the
24 richness of media? And I don't know if this is where
25 you're going, Jules. But you're right, banner ads used

1 to be crude and they just used to be across the top of
2 your screen. But if what you're talking about is ad
3 delivery in a form which substantially modifies or alters
4 the website being viewed, for example, a blogger's
5 website which inserts ads into the blog spool, which may
6 or may not be clear to the extent that they're ads or
7 not, I think you've got a copyright issue out there.

8 And I know that copyright issue is not on the
9 radar screen of most lawyers concerned about things like
10 the Wiretap Act and computer law, but bloggers have
11 content rights in copyright and in their blog, and one of
12 those rights -- and it applies to corporations as well --
13 involves the right to control and the right to create
14 derivative works. So, if you're now talking about
15 advertising which is substantially modifying and possibly
16 creating a derivative work of the site being viewed,
17 whether it's the website of a big company or the website
18 of a blogger, I think you have to do a copyright
19 analysis, too.

20 MR. POLONETSKY: I fear something nowhere as
21 sophisticated, but rather I have a little blog that I
22 barely use and I was able to put a little piece of code
23 on it by grabbing it, just following some basic
24 instructions and putting it at the top, and all of a
25 sudden, sophisticated video ads from American Express and

1 all kinds of interesting stuff is running on my website,
2 and I don't know how it's happening. I didn't do
3 anything special.

4 And all of a sudden, click, click, and I'm
5 suddenly hosting some of these very creative ads that
6 seem to be delivered in an instant.

7 MR. HINE: So, let's actually take this legal
8 issue somewhere else.

9 **(Laughter)**

10 MR. HINE: No, no, no, very related.
11 Unfortunately, Declan McCullagh was supposed to be on the
12 panel, but could not, and recently Declan and CNET have
13 addressed the issue of ad blockers and, certainly, as
14 we're moving into an area where we can deliver multiple
15 versions of rich media and hopefully consumers get the
16 right version that the advertisers want to deliver,
17 consumers still have tools at their disposal to help
18 mediate the experience. Zully talked about those.
19 Five years ago, it was an anti-virus program. Today you
20 don't buy an anti-virus program. You have an all-in-one
21 solution.

22 Declan's article specifically talked about
23 Firefox and talked about this issue of ad blocking and
24 surmised that some people in industry are very concerned
25 about these tools, that in essence if consumers are

1 blocking the advertisements that maybe there are some
2 legal challenges that should be made to look into the
3 legality of some of these tools.

4 And I'm wondering, maybe Scott, if you have
5 some thoughts about this, particularly in light of your
6 AdChoice efforts to help reach out to consumers?

7 MR. SHIPMAN: Yeah, I don't know if I have a
8 comment as the privacy lawyer from eBay, but certainly as
9 an attorney trained in high-tech law, I think that one of
10 the challenges you've got, certainly as was already
11 raised, is copyright. You also have some claims
12 certainly against anybody that's altering the content of
13 your site without your permission, something that we run
14 into quite often and we defend vigorously against.

15 I think the challenge that you'd face with
16 respect to the ad choice model that we have rolled out is
17 in that in the ad context we are actually the ones that
18 are voluntarily creating a system where users would
19 continue to see the ads, but it's the data behind the ads
20 that would be altered based on the user's preference.
21 So, it's a slight nuance from what you're asking, I
22 guess, so it may not be a direct answer.

23 MR. HINE: Maybe, Rob, you can follow up on
24 that. I guess we would like to touch on some of the
25 ramifications. I mean, this changes the whole ecosystem.

1 And what happens if something like ad block catches on
2 much more than it does today?

3 MR. GRATCHNER: So I won't speak from a legal
4 perspective probably because I only play a lawyer on TV
5 and not in real life. But from an ad blocker perspective
6 from a business model, obviously, we want to make sure
7 that users are getting the content that they want to see,
8 and from user experience, is this going to affect the
9 content that they're going to see? So, if we're blocking
10 ads and not getting the advertising model out there, is
11 this going to affect what content is out there?

12 If that's the case that's not a good thing for
13 consumers. I think one of the things that I think I have
14 not seen -- actually seen it or seen the article or read
15 it, but one of the things is how do we reach consumers?
16 What other mechanisms are out there? And while there may
17 be some good players out there who do that, maybe there's
18 other mechanisms out there that I know at aQuantive we
19 wouldn't do, but others may do to go out there to provide
20 those ads, to get those ads out there. So, it might
21 provide some other model we don't know about today if
22 we're blocking banner ads on websites.

23 MR. HINE: Well, let's actually shift that.
24 Maybe, Zully, you would like to comment from Symantec's
25 perspective because you are developing tools that, in

1 some sense, empower consumers to control their online
2 experience.

3 MR. RAMZAN: Sure, I think it's an interesting
4 question. I was just thinking about ad blockers recently
5 because it turns out that you don't even need to install
6 any kind of special software on your machine if you want
7 to block ads. It's pretty trivial. You just have to
8 change one text file and add some information to it and
9 you can block a whole bunch of ads.

10 So, I think the core issues is that we're
11 trying to maybe attack with technology or attach a
12 specific instance rather than looking at the core
13 underlying principle, which I think Mozelle was alluding
14 to earlier.

15 A couple of other things I wanted to mention
16 that kind of came up that are related is that certainly
17 we've talked a lot about cookies and it's been pretty
18 clear that cookies are one part of the online privacy
19 issue, but they're certainly not synonymous with online
20 privacy. There are so many other ways to achieve the
21 same kinds of effects.

22 So, for example, it turns out that -- I'm
23 getting an echo here. So, it turns out, for example,
24 that if I wanted to implement a cookie instead of using a
25 traditional cookie, there are other mechanisms by which I

1 can do the exact same thing without resorting to
2 traditional cookies.

3 Maybe that's what it is. My voice sounds
4 really funny. I don't know why that is. Let's try that
5 again. That maybe is a little less annoying. Sorry
6 about that.

7 So, the point I want to make is that from a
8 technology perspective it's important not to just look at
9 a specific instance or a sensor-specific technology but
10 to look at the overall principle because some of these
11 technologies are inherent in the way the web is designed.
12 I don't think we'll be able to get rid of these concepts,
13 per se. So, I think that's important to keep in mind.

14 MR. LORDAN: Jamie, following up on that, this
15 isn't something new, the ad blockers. Back seven or
16 eight years ago when we were just kind of reaching the
17 threshold of dial-up and things like that, people were
18 using -- I think the largest penetration of ad blockers
19 at that time was really because people wanted to conserve
20 as much bandwidth as possible. So, the ad blockers at
21 the time weren't as much a privacy issue. I mean, it was
22 also served as stop annoying banner ads and tower ads.

23 But it was because people, they were bandwidth
24 intensive and people were on dial-up and the motivation
25 for them to download and use an ad blocker was that they

1 wanted a faster surfing experience. And, so, I think the
2 motivation for using those tools, I think what's the
3 difference between you're concerned about privacy so you
4 buy an ad blocker. Why wouldn't you just go in and
5 manage your cookies?

6 So, I think it's really the same equation now
7 in the absence of a bandwidth constraint.

8 MR. HINE: Well, I want to actually circle back
9 and come to you Commissioner Thompson. We've heard, for
10 example, some information about research, but
11 particularly Larry Ponemon's research that touches on
12 consumers and their desire to control their online
13 experience and to have more control over their privacy,
14 and this implicitly suggests that trust is an issue and
15 you've touched on some of these issues. But I think that
16 there has been an amazing explosion in the growth of
17 social networking sites. And as Tim eloquently put it,
18 people can't get enough about willing to share the
19 details of their lives. And, so, I know that you have
20 done some work with social networking sites, and if you
21 could talk a little bit about is there something unique
22 about social networking sites? Do they engender some
23 different or unique form of trust?

24 MR. THOMPSON: Well, it's no secret that I've
25 been advising Facebook and not all of social networking

1 sites are the same. They don't track the same audience
2 and the behaviors are different. But what I do think is
3 a myth is that people like to go to social networking
4 sites and just like throw up on a page. I don't think
5 that's accurate.

6 I think that the social networking sites
7 actually provide more granularity that allow you to
8 decide who is going to get what information and under
9 what circumstances. Is in some ways represents what the
10 new privacy model is. Because there are instances -- and
11 Joe kind of alluded to this when he was talking about
12 blogs and copyright. People want information about
13 themselves out to people, but they want to control who it
14 gets to and under what circumstances. And, so, when you
15 talk about copyright and blog, in some ways, a blogger
16 may have a copyright right that he has, but he may not
17 want to assert it because he wants people to pass it
18 along. Now, whether that's attached to advertising or
19 not may be a different question.

20 So, what we're seeing here -- what I don't want
21 this conversation to go too far in, it's not necessarily
22 a binary equation is to add yes or no or information yes
23 or information no. It's really a much more sophisticated
24 question than that. It's the circumstances and to whom
25 and from. And it's not going to come from the top down.

1 You're going to get information from your neighbor across
2 the street or your college roommate and that may include
3 advertisements or it may not. So, that's a different
4 kind of model than whether you're visiting a website and
5 they give you a cookie or not.

6 MR. QUARESIMA: Scott?

7 MR. SHIPMAN: So, it's not often that I
8 actually purposefully agree with Mozelle, but I think I'm
9 going to here, but also highlight that a lot of what
10 we're talking about is not new. Let's take eBay 1998, a
11 completely open marketplace for people to buy and sell
12 any --

13 MR. THOMPSON: Boy, do I wish I would have
14 bought into eBay.

15 **(Laughter)**

16 MR. SHIPMAN: Hey, you're early at Facebook,
17 Mozelle.

18 Any user at eBay that bought or sold or anybody
19 that registered for the community meant that when they
20 registered, they were willing to give their contact
21 details to any other member. It was a completely open
22 transparent marketplace. So that meant that any
23 registered member with the simple request via email would
24 receive the other and vice versa. The contact details.

25 Now, we fast forward, you know, in certain

1 aspects, parts of eBay's original social networking
2 capabilities to today and we've actually dialed those
3 protections up and removed some of that functionality
4 because, in fact, as we listened to the customer, they
5 didn't want -- and certainly as the site grew from
6 thousands of members to 250 million members, they didn't
7 want that information available to everyone. They wanted
8 that information available to people that they did
9 business with, people that bid on an item or that won an
10 item successfully and vice versa with the seller.

11 So, we look at the history, we look at the
12 transformation of how information has been provided on
13 the Internet. In many ways, it's no different than the
14 DDD acronym that we heard a minute ago, digital data
15 diarrhea.

16 **(Laughter)**

17 MR. SHIPMAN: But as Mozelle said it's context
18 based and people are providing information to other
19 people based on the context of the transaction whether
20 that's the social networking website, whether it's an
21 address so that an item can be shipped, payment
22 information, whatever it might be.

23 I think one of the challenges, and certainly to
24 jump back to the cookies question originally, is cookies
25 is the one way, and in many ways a very poor way, of

1 collecting information on the Internet. The most
2 efficient way is to collect the information directly from
3 the customer, and that's a server. That's not a cookie.
4 It's not being stored on the customer's computer, it's
5 being stored back in San Jose or back in whichever
6 location your servers are at. And that's the real way
7 that companies can collect and enrich a database is by
8 collecting the information directly.

9 So, this fear about a cookie, it's a technology
10 that is working adequately for advertising, it's not a
11 very good technology for collecting information or for
12 storing information. So, really what we're looking at is
13 the use practices and what we're talking about is how are
14 people using information for advertising? Are companies
15 providing choices with that information and how it's
16 used? And, certainly, that's what we're trying to do
17 with the AdChoice program is to provide customers with
18 that opportunity to reflect how the information is being
19 used with respect to ads.

20 MR. QUARESIMA: Katherine, you had something?

21 MS. ALBRECHT: In the last couple of minutes we
22 have left, I would kind of like to bring this back around
23 to consumers, if we could, because if we're talking about
24 the future there's more to this than just the technology.

25 I think we all agree that the technology will

1 evolve, it's going to evolve into the more online space
2 onto the real world. But I think the bigger question
3 that I have as a consumer educator and someone who deals
4 with consumers every day is, how do we help them
5 understand what it is that's being done?

6 I think one of the reasons why cookies and all
7 of these other technologies are so worrisome to people is
8 because they're invisible. They occur in the course of
9 doing something else, someone is sort of almost attaching
10 on to you like a parasite when all you're trying to do is
11 order a set of sheets for your bed or when all you're
12 trying to do is walk down the street, and other people
13 are taking advantage of your presence and your activities
14 for their own reasons. I think that's where we need to
15 do -- there needs to be an educational component here.

16 I was stunned that in something like a
17 supermarket frequent shopper card, that now 90 percent of
18 American households have these things and people use them
19 all the time, and yet here we are almost 20 years into
20 having this technology, this simple technology of a
21 shopper card and 75 percent of households don't realize
22 that their data is being collected.

23 So, we can sit here and talk all day long and
24 come up with terrific ways in technological run-arounds
25 to help people protect their privacy, but until they

1 understand that these invisible things are happening to
2 them, we're not going to get anywhere.

3 MR. HINE: Katherine, I know that you've done a
4 lot of work with shopping loyalty cards. Do you see any
5 analogies here in what consumers understand about the
6 value proposition, the trade-off?

7 MS. ALBRECHT: I think, in a way, what's
8 happening in the online world and why RFID is interesting
9 to me is because they're even more invisible. I wrote a
10 paper a while back for the Denver Law Review called
11 Supermarket Cards, Tip of the Retail Surveillance
12 Iceberg, because the supermarket card, that visible
13 plastic card people have hanging off their key chains,
14 for many consumers is their only tangible connection to
15 the fact that there is this entire universe of data
16 collection occurring that the average consumer has no
17 idea is even going on.

18 So, the tangibility there, you would think,
19 would translate into a greater degree of awareness, and
20 that's why I focused on that. I was stunned -- if you
21 actually ask consumers, why do you think supermarkets
22 offer frequent shopper cards, which I did in my
23 dissertation research -- I said, can you tell me why you
24 think they offer you that, and they said, because, first,
25 they want to reward me; second, they want to offer me

1 deals and get me into the store and, third, they just
2 love me.

3 **(Laughter)**

4 MR. ALBRECHT: And at each opportunity I said,
5 can you think of any other reasons, can you think of any
6 others. I prompted them three times and only 14 percent
7 of consumers said because they want to know what my
8 shopping history looks like. And even when I came out
9 then after that and we did something called prompted
10 knowledge on -- spontaneous knowledge was that, do you
11 know it, and then prompted knowledge was if I tell you,
12 do you know it.

13 So, I said to people, does the supermarket make
14 a record of your purchases every time you scan the card?
15 And 75 percent of people said no. And, in fact, many of
16 them said, oh, come on, I'm not a conspiracy theorist,
17 I'm not paranoid, it's not like they're the CIA, blah,
18 blah, blah. And people were really adamant in absolutely
19 insisting that their supermarket would never do something
20 so despicable to them.

21 Now, this is a tangible thing that -- you know,
22 they sign a little form and you would think that they
23 would understand that, but they don't. And the reason, I
24 think, is because when I looked into how the supermarket
25 frequent shopper card was introduced throughout the mid-

1 1990s and the late '90s, it was not introduced as a data
2 collection card, big surprise, it was introduced as a
3 join the club we want to reward you, we love you. And
4 most people, for good or for bad, they believe what you
5 tell them.

6 So, if you say, come on our website because we
7 love you and we want to have you shoot the little bonobo
8 and be part of our contest or whatever, they will believe
9 you. So, I think there needs to be a greater degree of
10 openness of saying, here is the trade-off that we're
11 making very openly. We want your data.

12 MR. QUARESIMA: Okay. Jules, you had something
13 you want to say?

14 MR. POLONETSKY: Yeah, to carry on that point
15 in terms of consumer education, I want to take you back
16 to something that happened a couple of years ago. The
17 FTC helped put an end to a practice of sort of a spammer
18 who was using a flaw that allowed him to trigger pop-ups
19 on people's computers that looked like they were coming
20 from the operating system. They were and sometimes the
21 offers were, help make this pop-up stop happening, and it
22 used a security exploit.

23 So, when we became aware of it, we started
24 getting lots of calls from our members saying, hey, stop
25 these pop-ups, what are you doing to me? And we said,

1 what's going on? We're not doing it, we're not
2 responsible for this. And we came up with a little
3 script and people were really annoyed. We started
4 marketing this script, we ran banner ads, hey, are you
5 getting these? And we showed them pictures, are you
6 getting these ugly pop-ups? You want to not get them,
7 click here so that we can run this script. And a lot of
8 people did.

9 And guess what? A huge majority of the people
10 kept calling us, which was expensive, saying turn off
11 those pop-ups, and we kept running these ads and,
12 finally, we said, you know what, let's just roll out a
13 script and turn it off to everybody. And one or two of
14 the security people said, ew, why did you do that? Don't
15 do that to somebody's computer. I'm like, wait a second
16 we just stopped this terrible thing happening to so many
17 people. But just think about the education. People
18 really didn't like it and in the same context here we
19 were saying to them, hey, stop the pain, click here and
20 we'll fix it.

21 So, we need to do so much more and I think
22 we're all sort of guilty in industry and coming a little
23 too late in really putting a little bit more energy into
24 this.

25 I urge people to look at a site called

1 Carabella which I've become enamored with lately. It's a
2 virtual avatar. It's created by Privacy Activism. And
3 it's a college student, she's sort of a Goth, and she
4 goes to college and has to make privacy decisions about
5 whether she gives her data and her Social Security, and
6 it does a pretty good job at sensitizing kind of a jaded
7 audience about what they should and what they shouldn't
8 do.

9 So, whether the banner ads that we're going to
10 run work or the videos, clearly the Web 2.0 notice that
11 Esther was talking about is the lead challenge that I
12 hope everybody across the spectrum agrees with.

13 MR. QUARESIMA: Okay. We only have about five
14 minutes left. So, I'm just going to try to move quickly
15 to a final topic. That is, we've heard a lot of talk
16 about trust. Consumers will do business with trusted
17 websites and companies are going to compete on trust.

18 So, I wanted to throw that out generally. How
19 can we encourage companies to compete on trust? But also
20 I'd like people to sort of think about how consumers can
21 verify that their trust is well placed. Some famous
22 person said, trust but verify. So, I think we want to
23 throw that out. I think I'll start with John.

24 MR. THORNE: Well, first of all, thanks for
25 including Verizon in the conversation. The town hall has

1 been terrifically valuable, I can tell you, from my being
2 here two days.

3 Something that Mozelle said earlier deserves
4 echoing that answers your question, and that's that
5 consumers actually respond to different levels of
6 privacy. We follow very closely the third party
7 reputation surveys, like the Ponemon survey. Verizon has
8 been on the most trusted list every year since it's been
9 done. We've been the number one in our category of
10 telephone company/cable company for the last couple of
11 years running. We used to get measured on whether we're
12 at the top of that list.

13 But two small anecdotes. One is our wireless
14 business was invited to put all the cell phone numbers
15 for our wireless subscribers into a central database
16 where you can have a directory then, and I think we were
17 going to get a little bit of money. Somebody offered
18 some money for this. You could call up all the wireless
19 subscribers in a white pages or a 411 kind of service.
20 Debbie Streegle (phonetic), the head of our wireless
21 business, said, no, our customers aren't going to like
22 that. We got a bunch of people switching from I think it
23 was AT&T and Sprint and T-Mobile to come over to our
24 service when they heard that we were not going to
25 participate in something that turned their telephone

1 numbers over to a central agency.

2 Sara Deutsche, who's in the back of the room,
3 and I had a fairly public fight a couple years ago on
4 behalf of our Internet service provider with the
5 recording industry. I'm not going to re-fight copyright
6 issues although they -- some people think that what the
7 recording industry was doing with automatic robots
8 searching the web and then issuing subpoenas was a
9 privacy concern. We thought it was just illegal, and we
10 fought the IRA. Again, the experience was users wanted
11 to switch from -- I'm not going to name names down the
12 table there, other ISPs who were less confrontational
13 with some of the copyright holders about turning over
14 names.

15 So, we have found in our experience, you get
16 more customers if you protect privacy. It's in our
17 interest to be good with this. It's a way to grow the
18 investment we're making.

19 MR. QUARESIMA: Commissioner Thompson?

20 MR. THOMPSON: Well, that trust comes at
21 various levels. It begins with how you talk to your
22 user, your customer, about what your obligations are.
23 Then for every piece of technology, every piece of
24 functionality that you do something that's consistent
25 with what that promises. And I really like your

1 comments, Katherine, because it really is true that it's
2 not -- it's a series of things that consumers test on a
3 regular basis.

4 The FTC knows more than it wants to about
5 supermarkets. And, so, that's one example. But I can
6 tell you, for example, in the social networking space
7 that there's robust privacy protections on Facebook and
8 people actually use it.

9 Now, is there a gap between some people who
10 should be using it more and they don't? Yes. So, one of
11 the things that could happen that would really be
12 fruitful is for the FTC to shine its light on good
13 practices, because there are companies out there who are
14 doing good things so that consumers know that they have
15 choices and that where things look like practices that
16 are helpful to them and tools that are available to them,
17 that the FTC can actually talk about it. I think that
18 that's valuable.

19 And I also think it's valuable for the online
20 industry generally to talk to itself about what those
21 array of tools are that might be useful. Because it
22 really is hard to get after the bad actors. But if you
23 can begin to isolate what some of the good practices are,
24 that's fruitful. And I think it's a real challenge to
25 create a race to the top because a lot of business would

1 find it easier to deal with mediocrity.

2 MR. QUARESIMA: Anybody have a response to the
3 second portion of that question, which was sort of
4 verify? I mean, we've heard issues about that there are
5 possible harms associated with and about discriminatory
6 pricing. So, let's say you have a consumer who has now
7 opted in to everything that they wanted to opt in. How
8 can this consumer make sure that some of the bad
9 practices that we've identified earlier may not be
10 happening to them? Anybody want to take a crack
11 at that?

12 MR. POLONETSKY: Mozelle and I are Facebook
13 friends and I implicitly trust him with my data.

14 MR. QUARESIMA: Well, since we're out of time,
15 we began with homework.

16 MR. THOMPSON: I won't comment on that.

17 MR. QUARESIMA: Well, we began with homework
18 and we're going to -- oh, we do. Brad?

19 MR. SCHUELKE: I mean, I would just sort of go
20 back to -- and, again, my disclosure from the last panel
21 carries over to this one as well. But I think that is
22 one of the biggest difficulties in this area is the lack
23 of transparency, the fact that consumers don't understand
24 cookies and the fact they can't see it and they can't
25 verify it.

1 I think that's one of the things that in this
2 area makes self-regulation a little bit more difficult
3 than maybe even other areas is that if consumers don't
4 have the technological ability to verify on their own an
5 opt-out or some other procedure, then they're going to
6 look for a third party to be able to do that verification
7 for them and to give them some form of trust.

8 I think transparency is really the key and the
9 issue.

10 MR. THOMPSON: Can I just add one other thing,
11 though? One thing that has changed that's really
12 important is there are more people out there with easier
13 access to --

14 MR. QUARESIMA: We're running over, so we've
15 got to take one minute. One minute.

16 MR. THOMPSON: They speak up now. If consumers
17 don't like something, if you're doing something that
18 people get wind of it will be on a blog and there will be
19 100,000 users in two days complaining about it. That's
20 got to be encouraged and not discouraged.

21 MR. GRATCHNER: Everyone is absolutely correct.
22 Transparency and choice is very important, but I think
23 there's also a combination of other good work that
24 organizations are doing and others are doing. But people
25 are going to vote with their wallet, and if they feel

1 they're being misused or misguided on a website, they
2 won't go back and visit it.

3 MR. QUARESIMA: It is now three minutes past
4 5:00, so we're going to have closing remarks. Eileen?
5 If everyone could stay, we're going to have closing
6 remarks. Just stay here.

7 MS. HARRINGTON: This will take a nanosecond.
8 Thank you all for staying until the end here. This has
9 been, I think, a wonderful effort. And, again, we want
10 to thank the people on our staff who worked so hard on
11 this.

12 **(Applause)**

13 MR. HARRINGTON: And I'm going to name them one
14 more time, in no particular order. Peder Magee, Jamie
15 Hine, Lori Garrison, Rick Quaresima, Jessica Rich, Mary
16 Engle, Joel Winston, Stacey Brandenburg, Mamie Kresses
17 and Tracy Shapiro, and numerous of our wonderful honors
18 parallels.

19 MR. THOMPSON: Will they have cookies waiting
20 for them?

21 **(Laughter)**

22 MS. HARRINGTON: Well, no, I have a suggestion
23 for everyone in that regard. We're very pleased, I
24 think, with the good start that we've made over the last
25 two days. We have learned a lot more about behavioral

1 advertising including some about how it works and the
2 consumer protection issues that it raises.

3 We have had some debate on the issues
4 including whether disclosures work at all in this area
5 and whether existing models for managing privacy are
6 adequate.

7 We enjoyed the YouTube videos and greatly
8 benefitted from the participation from all who attended
9 and hope that you found that the town hall nomenclature
10 really carried with it a difference in your ability to
11 participate, ask questions and interact with other
12 participants.

13 We heard some general agreement, I think, about
14 certain issues which should help our efforts as we go
15 forward. First of all, behavioral advertising is clearly
16 a growing practice and it is largely invisible to
17 consumers. Although reasonable minds can differ as to
18 whether the practice itself raises concerns, there
19 appears to be a fair amount of agreement that greater
20 transparency and consumer control would be a good thing,
21 recognizing, of course, the limitations on notice and its
22 value.

23 There are also legitimate concerns about what
24 happens to consumer data, very legitimate concerns, that
25 is collected for advertising. Is it limited to use in

1 advertising or could it be used for some secondary
2 purpose? What if it falls into the wrong hands,
3 especially if the data are sensitive or personally
4 identifiable?

5 Now, everyone who was here at this town hall is
6 obviously thinking very seriously about the challenges
7 here and what the best approach might be for managing
8 privacy in this area, and so are we. Based on what we
9 have heard, we would like to see a reasonable approach to
10 this issue that is flexible, that doesn't stifle
11 innovation, that gives consumers information and control
12 without placing unrealistic demands on their time and
13 their willingness to study and analyze long disclosures,
14 that prevents any harms from arising from the collection
15 and storage of the personal data collected, and that
16 creates accountability among businesses that are
17 collecting and using the information. We think these are
18 not unattainable objectives.

19 Some of the ideas that we have heard over the
20 last two days are promising. They include a do not track
21 program, reforms to existing NAI requirements, and better
22 consumer education as illustrated by the YouTube contest,
23 and we need to examine these and other ideas more
24 closely, and we will and we encourage you, all of you, to
25 do so as well and to continue to engage with us and

1 suggest new ideas.

2 Now, at the same time that we think this has
3 been enormously productive, I think that we also have a
4 sense that we haven't yet seen or heard enough of the
5 concrete and specific facts about information collection
6 in connection with behavioral advertising and its actual
7 and planned uses nor have we seen or heard concrete
8 suggestions for improving consumer protection and privacy
9 in these areas. So, we are going to keep coming back
10 asking for the concrete.

11 I think that there has been a certain
12 guardedness on the part of many of the companies that are
13 involved in behavioral advertising in describing, in this
14 forum, exactly what it is that they're doing and maybe
15 this is not a forum for, as our old boss Jodie Bernstein
16 liked to say, open kimono, but we want the kimono opened.
17 So, we're going to keep coming back and we're going to
18 keep asking questions here.

19 Finally, you all should go out and have a
20 drink. **(Laughter)**

21 MS. HARRINGTON: Or whatever it is that you do.
22 I, myself, I would go for ice cream. But this has been a
23 long haul, intense information packed, and everybody here
24 has worked hard. So, it's 5:00 on Friday afternoon and
25 now you should all go off and do something far less

1 wholesome than sitting in this room. So, thank you,
2 everyone, for your participation.

3 **(Applause)**

4 **(At 5:11 p.m., the town hall was concluded.)**

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

C E R T I F I C A T I O N O F R E P O R T E R1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25MATTER NUMBER: PO75401CASE TITLE: EHAVIORAL ADVERTISING TOWN HALLDATE: NOVEMBER 2, 2007

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

DATED: NOVEMBER 16, 2007

LINDA D. METCALF**C E R T I F I C A T I O N O F P R O O F R E A D E R**

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

ELIZABETH M. FARRELL