

**OFFICIAL TRANSCRIPT
PROCEEDINGS BEFORE**

FEDERAL TRADE COMMISSION

DKT/CASE NO.: P954807

TITLE: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL
INFORMATION INFRASTRUCTURE

PLACE: Washington, D.C.

DATE: June 4, 1996

PAGES: 1 through 269

Meeting Before the Commission

C O R R E C T E D C O P Y

HERITAGE REPORTING CORPORATION

Official Reporters
1220 L Street, NW, Suite 600
Washington, D.C.
(202) 628-4888

Date: June 4, 1996
Docket No: P954807

FEDERAL TRADE COMMISSION

I N D E X

WITNESS:

EXAMINATION

(None)

E X H I B I T S

FOR IDENTIFICATION

(None)

FEDERAL TRADE COMMISSION

In the Matter of:)
) Docket No.: P954807
 PUBLIC WORKSHOP ON CONSUMER)
 PRIVACY ON THE GLOBAL)
 INFORMATION INFRASTRUCTURE)

Tuesday,
June 4, 1996

Room 432
Federal Trade Commission
601 Pennsylvania Avenue, N.W.
Washington, D.C.

The above-entitled matter came on for hearing,
pursuant to notice, at 9:03 a.m.

BEFORE: ROBERT PITOFISKY, Chairman
JANET D. STEIGER, Commissioner
CHRISTINE A. VARNEY, Commissioner
JODIE BERNSTEIN, Director,
Bureau of Consumer Protection

APPEARANCES:

SESSION 1

DAVID MEDINE, Associate Director for Credit
Practices, Bureau of Consumer Protection
 MARTHA LANDESBURG, Bureau of Consumer Protection
 JANLORI GOLDMAN, Deputy Director, Center for
Democracy and Technology
 LINDA GOLODNER, President, National Consumers
League
 PETER HARTER, Public Policy Counsel, Netscape
Communications Corporation
 EVAN HENDRICKS, Editor/Publisher, Privacy Times
 DANIEL L. JAFFE, Executive Vice President,
Government Relations, Association of
National Advertisers, Inc.
 JOHN KAMP, Senior Vice President, Washington
Office, American Association of
Advertising Agencies

Heritage Reporting Corporation
(202) 628-4888

APPEARANCES: (Continued)

SESSION 1

KATHERINE KRAUSE, Senior Attorney US WEST, Inc.
JACK KRUMHOLTZ, Interactive Services
Association
RONALD PLESSER, Piper & Marbury
ARIEL POLER, Chairman and Founder, I/PRO
MARC ROTENBERG, Director, Electronic
Privacy Information Center
SHIRLEY SARNA, New York State Attorney General's
Office, National Association of Attorneys
General
ROBERT ELLIS SMITH, Editor, Privacy Journal
ROBERT SHERMAN, Paul, Hastings, Janofsky
& Walker, General Counsel, Direct
Marketing Association
ALAN WESTIN, Privacy & American Business

SESSION 2

MARTHA LANDESBURG, Bureau of Consumer Protection
DAVID MEDINE, Associate Director for Credit
Practices, Bureau of Consumer Protection
BRIAN R. EK, Vice President, Government Affairs,
Prodigy Services Company
JANLORI GOLDMAN, Deputy Director, Center for
Democracy and Technology
LINDA GOLODNER, President, National Consumers
League
PAUL HARTER, Public Policy Counsel, Netscape
Communications Corporation
EVAN HENDRICKS, Editor/Publisher, Privacy Times
DANIEL L. JAFFE, Executive Vice President,
Government Relations, Association of
National Advertisers, Inc.
JOHN KAMP, Senior Vice President, Washington
Office, American Association of
Advertising Agencies
STEVEN KNIGHT, Tennessee Attorney General's
Office, National Association of
Attorneys General
KATHERINE KRAUSE, US WEST, Inc. Chair,
Privacy Committee, Information Industry
Associates
PIERCE REID, Production Manager 1,
CompuServe, Direct Marketing Association

Heritage Reporting Corporation
(202) 628-4888

APPEARANCES: (Continued)

SESSION 2

PAUL RESNICK, Technical Staff, AT&T Research,
Platform for Internet Content Selection
ARIEL POLER, Chairman and Founder, I/PRO
MARC ROTENBERG, Director, Electronic
Privacy Information Center
ROBERT ELLIS SMITH, Editor, Privacy Journal
ALBERT VEZZA, Associate Director, Laboratory
for Computer Science, MIT, Chairman,
World Wide Web Consortium
DANIEL WEITZNER, Deputy Director, Center
for Democracy and Technology
ALAN WESTIN, Privacy and American Business
JOEL REIDENBERG, Associate Professor,
Fordham University School of Law

SESSION 3

MARTHA LANDESBURG, Bureau of Consumer Protection
DAVID MEDINE, Associate Director for Credit
Practices
TRUDIE BUSHEY, Director, Legislative Affairs,
TRW Information Systems & Services
KAWIKA DAGUIO, Federal Representative, Operations
and Retail Banking, American Bankers
Association
KATHLEEN FRAWLEY, Director, Washington D.C.
Office, American Health Information
Management Association
JANLORI GOLDMAN, Deputy Director, Center for
Democracy and Technology
EVAN HENDRICKS, Editor/Publisher, Privacy Times
MARSHA KRAMARCK, Delaware Attorney General's
Office, National Association of
Attorneys General
JANET KOEHLER, Senior Manager, Electronic
Commerce, AT&T Universal Card Services,
Smart Card Forum
ROBERT MEROLD, Vice President, IMS America, Ltd.
MARC ROTENBERG, Director, Electronic Privacy
Information Center
ROBERT SHERMAN, Paul, Hastings, Janofsky &
Walker, General Counsel, Direct Marketing
Association

Heritage Reporting Corporation
(202) 628-4888

APPEARANCES: (Continued)

SESSION 3

ROBERT ELLIS SMITH, Editor, Privacy Journal
ANDREW J. STRENIO, JR., Hunton & Williams
ALAN WESTIN, Privacy & American Business

SESSION 4

DANIEL L. JAFFE, Executive Vice President,
Association of National Advertisers, Inc.
MARTHA LANDESBURG, Bureau of Consumer Protection
DAVID MEDINE, Associate Director for Credit
Practices, Bureau of Consumer Protection
TERESA SCHWARTZ, Deputy Director, Bureau
of Consumer Affairs
DOUG BLANKE, Minnesota Attorney General's Office,
National Association of Attorneys General
MARI ANN BLATCH, Consumer and Government
Affairs Consultant, Reader's Digest
ROGER COCHETTI, Program Director, Policy &
Business Planning, Internet Division,
IBM, Interactive Services Association
GARY I. FRIEND, Vice President, Government
Relations and Marketing, The Dun &
Bradstreet Corporation
JANLORI, GOLDMAN, Deputy Director, Center
for Democracy and Technology
ALBERT VEZZA, Associate Director, Laboratory
for Computer Science, MIT, Chairman,
Worldwide Web Consortium
EVAN HENDRICKS, Editor/Publisher, Privacy Times
JOHN KAMP, Senior Vice President, Washington
Office, American Association of
Advertising Agencies
SCOTT MCCLELLAN, Director of Communications,
Canadian Direct Marketing Association
RONALD PLESSER, Piper & Marbury
JOEL REIDENBERG, Associate Professor,
Fordham University School of Law
ROBERT ELLIS SMITH, Editor of Privacy Journal
ANDREW J. STRENIO, JR. Hunton & Williams
BARBARA WELLBERY, Chief Counsel, National
Telecommunications and Information
Administration, U.S. Department of
Commerce
ALAN WESTIN, Privacy & American Business

Heritage Reporting Corporation
(202) 628-4888

APPEARANCES: (Continued)

SESSION 5

MARTHA LANDESBURG, Bureau of Consumer Protection
DAVID MEDINE, Associate Director for Credit
Practices, Bureau of Consumer Protection
JERRY BERMAN, Executive Director, Center for
Democracy and Technology
WILLIAM BURRINGTON, Assistant General Counsel &
Director of Public Policy, American
Online, Inc., Interactive Services Assoc.
STEVEN J. COLE, Senior Vice President and
General Counsel, Council of Better Business
Bureaus, Inc.
MALLORY DUNCAN, Vice-President, General Counsel,
National Retail Federation
BETH GIVENS, Project Director, Privacy Rights
Clearinghouse, Center for Public Interest
Law, University of San Diego
JANLORI GOLDMAN, Deputy Director, Center for
Democracy and Technology
LINDA GOLODNER, President, National Consumers
League
CONNIE HEATLEY, Senior Vice President, Public
Relations/ Communications, Direct
Marketing Association
EVAN HENDRICKS, Editor/Publisher, Privacy Times
JOHN KAMP, Senior Vice President, Washington
Office, American Association of
Advertising Agencies
MARC ROTENBERG, Director, Electronic Privacy
Information Center
ROBERT ELLIS SMITH, Editor, Privacy Journal
ANDREW J. STRENIO, JR., Hunton & Williams
JACKIE WARD, Maryland Attorney General's
Office, National Association of Attorneys
General

1 Consistent with being a privacy program, I have to
2 say in full disclosure we are both videotaping and
3 transcribing this session, so everything you say will be
4 recorded. And as we have done in the past, we plan on
5 posting the transcript onto the Commission's web page for
6 future reference.

7 In terms of some housekeeping details, our FTC
8 cafeteria is temporarily in hibernation. So if you want to
9 proceed for some snacks out of vending machines, you can
10 proceed to the seventh floor. If not, try to work the
11 community and local restaurants and carry-outs.

12 The workshop today is designed to be a dialogue,
13 as we have done in the past. That translates into
14 discussions and not speeches. And as the Chair, I am going
15 to exercise my prerogative to gavel anyone who speaks more
16 than three minutes or four minutes, at most, other than some
17 of the early presenters.

18 Also, I want to mention that we have had an
19 ongoing dialogue on the Internet through our privacy List
20 Serve, which has been very valuable input to the Commission,
21 and I would encourage anyone who is interested in joining
22 that discussion to check our web page for information.

23 We have to date received over 2,000 e-mail
24 messages expressing views on privacy issues, and we found it
25 a very valuable dialogue for us.

1 I would also like to thank the many, many people
2 at the Commission who have helped make this event possible.
3 In particular, I would like to mention Martha Landesberg,
4 who is sitting in the middle there, from my staff, who has
5 been tireless, and everyone probably has spoken to her at
6 some point repeatedly about today, and I want to thank her
7 for all her efforts in putting today's program together.

8 It is a real pleasure to introduce Chairman
9 Pitofsky, Chairman of the Federal Trade Commission.
10 Chairman Pitofsky's tenure at the FTC has been marked by
11 willingness to tackle emerging technology issues and global
12 trade issues, both of which merge together in the Internet.

13 I would like now to call upon Chairman Pitofsky to
14 make some opening remarks.

15 CHAIRMAN PITOFSKY: I think I will stay right here
16 if you can hear me.

17 Good morning and welcome. This turnout is
18 evidence that if you mention the word "Internet," you get
19 people's attention. If you mention "marketing" on the
20 Internet, eyebrows go up. And if you mention "marketing" on
21 the Internet and "privacy," you draw a crowd.

22 Over the next day and a half we will pick up where
23 we left off last November when we held several days of
24 hearings devoted to the impact of new information
25 technologies and globalization of consumer protection

1 concerns, and where we left off last spring during the
2 workshop on the global information infrastructure.

3 I am delighted the Bureau is hosting this workshop
4 to explore the special challenges to consumer privacy posed
5 by the emerging online marketplace. This type of setting
6 enables us to bring together a broad range of groups and
7 individuals to discuss the challenges that lie ahead.

8 The challenges for consumer privacy posed by the
9 online marketplace are special, because the new technology
10 enables marketers and others to gather information about
11 consumers that is far richer and detailed and more easily
12 tied to individuals than information available to the
13 traditional marketing media.

14 Electronic information transmitted in online
15 transactions can easily be stored, analyzed and used, and
16 can travel more quickly and globally, in ways that have
17 either been impossible or prohibitively expensive in the
18 more traditional contexts.

19 These facts suggest that issues related to online
20 consumer privacy merit analysis apart from similar issues
21 raised with respect to other media.

22 In the course of the Bureau of Consumer
23 Protection's year-long study of these developments, in
24 concert with industry, privacy advocates and consumers, a
25 number of themes have been highlighted which form the basis

1 for today's agenda. The morning begins with a discussion of
2 how personal information provided in consumer transactions
3 is being used online. It will be followed by demonstrations
4 and analyses of various technological approaches to the
5 question of how to protect online consumer privacy.

6 In the afternoon the discussion shifts to the
7 question of whether sensitive information, such as financial
8 and medical information, should receive special treatment in
9 the online context. The day ends with a discussion of
10 strategies for educating consumers and industry about the
11 implications of the new technology for consumer privacy, and
12 for the growth of the online marketplace.

13 Tomorrow the workshop turns to the special issues
14 raised by information obtained from and about children in
15 the online medium.

16 This project has met with much enthusiasm and,
17 quite candidly, some concern about how privacy issues mesh
18 with the FTC Act Section 5's prohibition against unfair or
19 deceptive acts or practices.

20 Let me state a few parameters for our discussion
21 this morning. As we saw during the just completed Global
22 Competition Hearings, projects and research endeavors
23 designed to gather facts and highlight issues are an
24 important part of this Agency's mission. It makes sense for
25 the Commission to invite various groups to exchange views on

1 privacy questions that implicate several consumer protection
2 concerns.

3 We may or may not find in this process that there
4 are privacy issues that are troubling from a law enforcement
5 perspective because they violate traditional rules
6 concerning deception or unfairness. But this is a fact-
7 finding workshop, designed to provide a forum for discussion
8 and debate.

9 We are not here to lay the groundwork for any
10 government rules, guidelines or otherwise. Rather, we would
11 like to learn more about industry and consumer initiatives
12 that have emerged over the past year. I hope the Bureau
13 will contribute to self-regulatory efforts, and to the
14 Commission's understanding of online privacy issues by
15 providing a report about the issues discussed today and
16 tomorrow. That is our goal.

17 Let me add another point. The Federal Trade
18 Commission has always paid attention to industry views of
19 proper business behavior. Let me remind you, however, that
20 Section 5 enforcement is independent of and does not
21 automatically reflect voluntary codes. It does not
22 necessarily follow that failure to follow industry guides
23 will lead to FTC enforcement actions, or that compliance
24 with such guides will exempt business from the unfairness
25 and deception standards of Section 5.

1 Finally, let me say one more thing. All of the
2 commissioners have been supportive and have contributed to
3 the design of this agenda, but I must especially acknowledge
4 my colleague, Commissioner Christine Varney, who has
5 sensitized us to these issues and energized us to conduct
6 these hearings.

7 You have before you a very ambitious agenda and a
8 distinguished group of panelists. I turn the program over
9 to David Medine, Associate Director for Credit Practices in
10 the Bureau of Consumer Protection, who will moderate this
11 morning's discussion.

12 David.

13 MR. MEDINE: Thank you, Chairman Pitofsky.

14 Just to elaborate on our format today, we will not
15 be using a traditional format of one speech, as I mentioned
16 earlier. Each session will start with two or three
17 crystallizers, that is, people who will help focus the
18 issues, and then it will be open to all panel members for
19 discussion.

20 Again, we have brought together a very exciting
21 panel. I will ask each person to introduce themselves as
22 they speak later in the morning, but I would first like to
23 start off exploring the issue of what information is
24 available online now and could potentially be gathered as a
25 threat to privacy. And I would ask the Center for Democracy

1 and Technology to do a demonstration for us. Janlori
2 Goldman is the co-founder and Deputy Director of the Center
3 for Democracy and Technology.

4 MS. GOLDMAN: Thanks. Before we get into the
5 demonstration I just want to try to give you a little
6 context of why we created this demonstration in the first
7 place.

8 For many, many years, we have worked to achieve a
9 number of goals in the privacy area. One is to make sure
10 that when people divulge personal information in any context
11 that they know what the information practices are of the
12 entity to which they are divulging the information, and a
13 critical piece of that is that they then be able to have
14 some control over that information once they have divulged
15 it.

16 Again, the older conception of privacy is that in
17 order to protect yourself you have to retreat from society
18 and we believe, as do most people in this area, that
19 critical to enhancing privacy is allowing people to step
20 forward and participate fully while not having the cost of
21 that participation be the loss of control over their
22 personal information.

23 This is not only critical to protect their
24 privacy, but also to enhancing other critical democratic
25 values such as free speech, the right to receive

1 information. Again, people will be wary about taking risks
2 and deterred from taking those risks, about exploring new
3 ideas and communicating with others and receiving
4 information, if they are concerned that the information
5 about those explorations and about those communications is
6 revealed to others.

7 Now, on the Internet, particularly on the
8 Worldwide Web, we have a few new wrinkles in the privacy
9 area. Let's just take a very basic example.

10 If I go into a bookstore and I am browsing around
11 and I pull out a book, the title is catchy. It might be a
12 little racy, who knows even for me. And I pull out the book
13 and I open it up and I am looking at it. I may decide to
14 look through a few pages, close it up, put it back on the
15 shelf and leave the bookstore. I haven't bought anything.
16 I have just browsed.

17 Now, when you browse on the Web something
18 different happens. You not only have a record, what they
19 call the mouse droppings or click stream data, every single
20 move that you make in walking through that bookstore, but
21 every page that you look at is captured by the site that is
22 offering you the information.

23 Now, most of this is done invisibly and unknown to
24 the user. Most of this is done without people having any
25 control over whether it's happening. Some of it is done

1 innocently. It's not necessarily done with the intent to
2 capture the information and use it for some other purpose,
3 but it is certainly built into the architecture and the
4 software that makes up the Internet.

5 Now, not only can information be collected at each
6 site, but profiles can be developed by comparing and pulling
7 together that information from various sources. So you can
8 get a fairly detailed picture of somebody's activities
9 online, which may or may not represent who they are as an
10 individual, but certainly judgments will be made of them on
11 that basis.

12 The reason that we put together the demonstration
13 is to educate the public about the detailed personal
14 transactional information that is captured on them when they
15 search the Web, and to create a demand for the creation of
16 privacy policies and practices to reverse this trend, to
17 allow people to decide at the front-end before they ever go
18 to a site what their privacy preferences are, how they want
19 their information collected, if they want it divulged at
20 all, and to put them into the process of that transaction,
21 to make them a necessary and critical partner to that
22 transaction.

23 Now, we have an opportunity, obviously, and this
24 is, you know, a big part of our discussion today, to up-end
25 the dynamic that we have had in the traditional information

1 collection area to not necessarily have the information
2 collected, whether it be the government or the private
3 sector or a nonprofit, say here is your notice, here is your
4 opportunity to opt out. Please sign here and then we will
5 give you the benefit. But we have an opportunity in the
6 online digital environment for people to say, here is my
7 privacy preference, here is whether I want the information
8 about me collected, here is whether or not I want it reused
9 for some other purpose, and that then becomes the starting
10 point for the discussion.

11 So Bob Palacios, who is our fabulous systems
12 administrator, online organizer and helped put this
13 together, our goal, as I said, was to educate the public,
14 make people aware of what's really happening when they are
15 online and to create a public demand based on this
16 information. For people will be so incensed when they see
17 this, and it will create this powerful public demand for the
18 development of policies and practices.

19 If you come to our site, which is
20 WWW.CDT.ORG/Privacy, if you don't remember that there are
21 cards out there to remind you. And what you see if you go
22 to our site, I would be welcomed personally. My name is --
23 my mail address is [JLG @ CDT.ORG](mailto:JLG@CDT.ORG). I am affiliated with CDT,
24 located around Washington, D.C. I use a PowerMac. My
25 browser is Netscape, and I have linked from Yahoo.

1 So you not only get the information that is
2 revealed at that site, but you know they are referring you
3 around, the site from which I came.

4 Now, obviously, you know, as a small, nonprofit we
5 do not have -- we don't have our own server, and if we did,
6 we could probably learn a lot more about the people visiting
7 our site. And again, some of this is done unintentionally,
8 and some of it is just done as part of how the Net works.

9 Now, there will be some variations. If you visit
10 our privacy demo, if you are coming from, for instance, an
11 online service, you may not be greeted personally. You may
12 be greeted as an online service subscriber. If you are
13 coming from behind a fire wall, or an organization, again,
14 some of that personal data is stripped off when you go out
15 onto the Net. So that it will vary, depending on the
16 browser that you are using and the sites from which you are
17 coming.

18 That's our demo.

19 The second thing that we have done is not just to
20 make people feel here is what happens out there, but what
21 are the policies and practices that do exist on the Internet
22 today to protect personal information. And what we have
23 done is create an online clearinghouse of policies that
24 operate on the Web.

1 We started with the online services, and the
2 reason that we started with the online services is because
3 there was a body of privacy policies in that sector where
4 there isn't in any other sector on the Internet. And there
5 are a number of reasons why there were privacy policies and
6 information policies in that area, but we thought that it
7 would be a good place to start.

8 And so what we have done is we have taken the four
9 major online services, and on the left-hand part of the grid
10 we detailed the fair information practice principles that we
11 consider to be the fair information practice principles that
12 need to be addressed where there is any collection of
13 personal information.

14 The first one, obviously being notice. And we
15 then put whether or not there is written statement that
16 would put that information policy in the online service's
17 terms of agreement, in terms of service, privacy policy. If
18 you then click on, say AOL first, we have got it
19 alphabetically, of course. We then click on the relevant
20 portion of that policy. So you can see it. If you want to
21 see the whole thing in context, you can do that too by
22 clicking at the top, or you can just read through the Fair
23 Information Practices and click on the relevant portions, so
24 you can see.

1 Now, part of what we found is that, with a few
2 exceptions, the privacy policies of the online services are
3 not in one place. And so it was necessary to kind of move
4 around a little bit and link to the relevant portions.

5 But, again, our goal in doing this is that our
6 next step will probably be focusing on Internet service
7 providers, and we want to push in the interim the
8 development of privacy policies in that sector so we will
9 actually have something to show and not some blank boxes
10 where we have no relevant policy or no written policy at
11 this time.

12 So that's essentially what we have done. Feel
13 free to visit the demo. As I say, the site will be updated
14 as new policies are developed, as policies are refined, as
15 we focus on other sectors that operate on the Internet, and
16 happy to take any questions, or we can go on.

17 Thank you.

18 MR. MEDINE: Thank you, Janlori.

19 I visited the site last evening, and it revealed
20 that I was from the Federal Trade Commission, which raised
21 some interesting issues about our law enforcement efforts in
22 the future.

23 (Laughter.)

24 MS. GOLDMAN: You will have to link to the
25 anonymizer which I forgot to mention. You can link to the

1 anonimizer first, David, and then go out there and do your
2 law enforcement.

3 MR. MEDINE: Thank you.

4 I would next like to call on Marc Rotenberg to
5 help again crystallize issues. Marc is the Director of the
6 Electronic Privacy Information Center, and he also teaches
7 the law of information privacy at Georgetown University Law
8 Center.

9 MR. ROTENBERG: Thank you, David, and thank you to
10 the FTC commissioners for the chance to be here today.

11 I would like to put up a different web page which
12 is epic.org. I guess this is the equivalent of saying "next
13 side, please."

14 With a better interface, I could just think the
15 correct URL and it would appear. I think Microsoft is
16 working on that.

17 Okay, if you could -- thank you. If you could
18 scroll down just a little bit on this page. This is EPIC's
19 home page, and if you could go right there. I am going to
20 follow on Janlori's comments and say a few more words about
21 privacy policy on the Internet, and what is really the
22 urgency today in the United States to move aggressively to
23 establish privacy safeguards that would not only be good for
24 consumers, but good for business.

1 We have seen a great deal of privacy activity, and
2 not only the hearings today and tomorrow. Marc Klaas was on
3 The Today Show this morning and Ram Avraham's case is a very
4 important case. It goes before the Virginia Circuit Court
5 on Thursday.

6 If you could scroll down one more line, and if you
7 don't have enough to do this week I recommend a very good
8 book by Ellen Alderman and Caroline Kennedy called "The
9 Right to Privacy."

10 Now, let's scroll down to our privacy archives.
11 The EPIC web site is set up so that at the top you get
12 important information about privacy issues. Here are our
13 policy archives, and if you click on privacy, please, we
14 call this the A to Z use of privacy. It's very important
15 never to lose sight that when we are talking about privacy
16 in the United States we are talking about a core social and
17 political value described once by Justice Brandeis as the
18 right to be let alone. The most comprehensive of rights,
19 and most valued by people.

20 Now, if we could go on down, and this would be the
21 key -- it's a little bit of an Easter egg hunt going on
22 here. Privacy, general privacy information, if you could
23 scroll a little bit further. Thank you. Now, we are in our
24 A to Z's of cable TV information, caller ID, counter-

1 terrorism, keep going. It's a big topic. It covers a lot
2 of ground, as it should.

3 Okay, stop here. That long and awkward looking
4 acronym, "Everything you always wanted to know about privacy
5 in America but were afraid to hear" is the core of my brief
6 comments this morning, so let's click on that.

7 Let's scroll up so the five points -- thank you,
8 stop. Okay, I am going to make just five points at this
9 point in the presentation.

10 And the first point to make is that the voluntary
11 approach to privacy regulation in the United States has
12 failed. It failed in 1990. You will notice that Lotus
13 proposed the release of a product called "Marketplace,"
14 which violated the industry's guidelines. The industry
15 association did not object to the release of the product.
16 Consumers and the most savvy users of technology, people on
17 the Internet, eventually organized a boycott that led to
18 30,000 messages to the CEO of Lotus, and the product was
19 withdrawn.

20 This occurred most recently when an investigative
21 reporter in Los Angeles was able to obtain the names of
22 5,000 children in the Pasadena area, using the name Richard
23 M. Davis, the most notorious child molester in the State of
24 California, the person who currently stands on trial for the

1 murder of Polly Klaas. The person responsible said simply a
2 mistake was made.

3 My second point is that consumers will demand
4 legal control over personal information. There is nothing
5 surprising or controversial about this point. In fact, if
6 you look at consumer polls from the 1991 Time/CNN poll to
7 the 1995 Yankolovich poll, if you ask the question, "Do
8 companies have the right to sell your personal information
9 without your consent," nine out of 10 consumers in the
10 United States would say "No." Ask that question. I can
11 tell you what the answer will be.

12 My third point concerns technologies of privacy;
13 without question a critical part of getting the
14 infrastructure for commerce in the next century. Now, you
15 have to be very careful when you use this phrase. It's a
16 very inviting phrase, because it calls for technological
17 solutions. If they can be found, they are in fact
18 applicable to government's regulation.

19 But not all technology is technologies of privacy,
20 and technologies that simply promote access to digital fine
21 print do not help consumers. They simply place more burden
22 upon consumers. Technologies of privacy limit or eliminate
23 the collection of personal information. These are the
24 technologies that are gaining support in Canada, and Japan,
25 and in the European Union where the top technological

1 achievement award last year went to David Shoum, the
2 inventor of Digicash, and the person who makes possible
3 payment systems from electronic commerce, to parking, to
4 shopping, completely and anonymously. Those are
5 technologies of privacy.

6 My fourth point, and this is very much to the
7 business representatives here, is that even companies that
8 want to do the right thing, that have good privacy policies,
9 and that intend to respect to the consumer's privacy will
10 not be able to succeed in the absence of legal rights which
11 establish a level playing field.

12 And the reason for this is very simple. This is a
13 very competitive market, and it will grow more competitive.
14 And the companies that try to enforce good privacy policies
15 will run up against companies that are cutting corners, and
16 they will be at a market disadvantage.

17 America Online made this point last year when they
18 said that one of the reasons they were selling their
19 membership list is simply because their competitors did it.
20 They could not afford to give up an important income stream.
21 This is a very important point in the policy-making realm.
22 It is not just in the interest of consumers. It is in the
23 interest of business that wants to protect privacy, to
24 ensure that a legal framework with a level playing field
25 makes clear privacy rights and responsibilities.

1 And my final point is simply this. Smart
2 companies in smart countries know this. This is why you see
3 the rapid march in Europe, in Canada, and in Japan, for
4 technological and regulatory solutions that establish strong
5 privacy safeguards, because every country wants to ensure
6 the privacy of its information economy in the twenty-first
7 century. And absent strong privacy safeguards consumers
8 will be reluctant to participate in the network environment,
9 and businesses will constantly run the risk of
10 misunderstanding or not responding to consumer privacy
11 concerns.

12 That is everything you want to know about privacy
13 in America but were afraid to hear.

14 MR. MEDINE: Thank you very much, Marc, for
15 helping to crystallize some of the issues that we are going
16 to be wrestling with today.

17 As our third and final crystallizer for the first
18 session, I would like to call on Bob Sherman. Bob is a
19 partner at the New York Office of Paul, Hastings, Janofsky &
20 Walker, and is also general counsel to the Direct Marketing
21 Association.

22 MR. SHERMAN: Thank you, David, Ms. Commissioner,
23 Mr. Chairman, and members of the staff.

24 I was asked to help try to focus the discussion
25 with suggestions that would help stimulate dialogue with the

1 issues here today, and I guess what I would like to do first
2 is to try to put us in step and say that no one in this room
3 comes from a heavy technological background. This is such a
4 deep-rooted concept that actually defines itself as one
5 where we are encouraged to promote the progress of the laws
6 of science. But we can't lose sight of the fact that what
7 we are really talking about today is a vehicle for
8 communication, the means not an end. We must be respectful
9 of the underlying feat that is involved on the Internet.

10 Now again, and this is not new, we find ourselves
11 in the inherent pinch of the First Amendment right to
12 transmit these communications and the right to privacy. It
13 is one that has been faced in all media, and today's medium
14 as well. The Internet is just another way to enhance our
15 society, based on the flow of information. Different from
16 other societies, we have grown up differently. Indeed, the
17 reason we are here in this country stems from that very
18 right. And so it is not necessarily a fair comparison to
19 look at what other countries are doing, although it is
20 sometimes very illustrative, very instructive.

21 The Internet it is different things to different
22 people, for some it's just a means of entertainment.
23 Others, for education. Some just pure communication. And
24 now developing is a commercial industry, involving commerce
25 on the Internet. Industry, and specifically direct

1 marketers have experienced growing pains of other media. We
2 have learned from that experience. It has been successful
3 not only for themselves but also in the world of
4 communication. With the development of a new vehicle of
5 communication comes new opportunities and new
6 responsibilities.

7 But if we depend on technology to create the
8 opportunity, we should also allow technology to help us,
9 assist us in carrying out the responsibility as well. Other
10 panels will address technological means that will help us in
11 that regard.

12 Now, before directly addressing some of the
13 policies that are involved in private, Bill will be
14 providing you in just a moment with some basic general
15 principles that have been developed for you on the Internet.
16 I would like to just make a comment about self-regulation,
17 and why it does work, why it is burdensome in monitoring and
18 regulating. No method is perfect. Law enforcement is not
19 perfect. There will always be bad apples.

20 Self-regulation is a different process from law
21 enforcement. Self-regulation, when successful, in my view,
22 is defined as getting voluntary cooperation by members and
23 sound business practices and consumer information. It is
24 not law enforcement.

1 We don't have a nice law enforcement act. You go
2 at it a different way. We try to obtain the same ends
3 through education, peer pressure, and a self-imposed process
4 that we believe the system works, and will continue to be
5 successful if allowed the opportunity. But underlying self-
6 regulation is allowing good, sound, basic business
7 principles to evolve. Once they evolve, then self-
8 regulation can work, but it does take some time. None of us
9 would benefit from a ready/fire/aim form of regulation.

10 To that end, and now I would like to get into some
11 recommended principles. The Direct Marketing Association,
12 in conjunction with the Interactive Service Association, has
13 come up with general principles for use on the Internet
14 touched by three different areas.

15 The first, notice and choice; second, is a set of
16 principles for unsolicited advertising, e-mail; and the
17 third is marketing for children on the Internet, which will
18 be discussed in tomorrow's session.

19 First, and I would like and encourage all
20 panelists to participate, with comments and suggestions
21 because these are basic principles that have not yet evolved
22 into industry guidelines because we want to see how the
23 actual operation of marketing takes place. First is the
24 element of notice and choice.

1 We believe that all marketers operating on an
2 online site, whether or not they collect personal
3 information online from individuals, should make available
4 their information practices listed in a prominent place.
5 The notice should be easy to find, easy to read and easy to
6 understand.

7 It should identify the marketer, both an e-mail
8 and postal address at which they can be contacted, and state
9 whether the marketer collects personal information online.
10 It should disclose the nature of personal information
11 collected, such as the sex of the individual consumers, the
12 nature of the uses of the information, the nature and
13 purpose of the disclosures of such information, and the
14 types of persons to whom the disclosures will be made, and
15 the mechanism by which the individual may limit disclosure
16 of such information.

17 Every consumer should be furnished with the
18 opportunity to request that their e-mail address not be
19 rented, sold, or exchanged for online solicitation purposes.
20 The marketer should suppress in a timely fashion e-mail
21 addresses of individuals who have made such requests. The
22 system that has worked in other media, I believe, given the
23 opportunity to follow and with the interactive nature of
24 online marketing, should be no problem, and no reason why it
25 shouldn't work there as well.

1 With respect to unsolicited advertising by e-mail,
2 we have developed a set of general principles to follow.
3 Online solicitation should be posted through bulletin boards
4 and chat rooms, only when existence of the forum is a stated
5 policy. I think each of them should state their own
6 policies, and anyone who wants to solicit those who browse
7 must follow those policies.

8 Online e-mail solicitation should be clearly
9 identified as solicitation, and should disclose the
10 marketer's identity. That would avoid what I am told is a
11 burdensome need to go through every single e-mail in one's
12 mail box. It takes up time and some nominal, but admitted
13 expense to go through it. There is an indicia of some kind
14 to let the recipient know that if there has been unsolicited
15 advertising mail, so that the recipient can choose to read
16 it or not read it at his or her pleasure. We think that
17 would be a fair practice.

18 Marketers using e-mail furnished by customers with
19 whom they do not have an established business relationship
20 should give notice of the mechanism through which they could
21 notify the marketer that they do not wish to receive future
22 online solicitations. The marketer should also furnish
23 consumers with whom they do have established business
24 relationships with notice and a mechanism by which they can

1 request that their name not be transferred to other
2 entities.

3 Any person who uses for online solicitation e-mail
4 address that have been collected from online activities of
5 individuals in public or private spaces should see to it
6 that those individuals have been offered an opportunity to
7 have this information suppressed. Those who operate chat
8 rooms, news groups and other public forums, can inform
9 individuals in those places that information they
10 voluntarily disclose to those areas may result in
11 unsolicited messages to those individuals by others.

12 I think by following general principles we'll be
13 off to a good start in helping people who want to use the
14 Internet for a variety of purposes to enjoy it without
15 concern, without fear that their privacy will be violated.

16 MR. MEDINE: Thank you, Bob, very much.

17 Obviously, the Internet provides a unique
18 opportunity to generate, capture, store and reuse
19 information and I think one question that we can start off
20 with is what is the responsibility for how that information
21 should be handled and if there is a responsibility, how
22 should that be carried out. I suspect there are also panel
23 members who want to respond to some of the presentations as
24 well.

1 So does anyone want to volunteer to pick up the
2 discussion? Evan, do you want to respond?

3 MR. HENDRICKS: Well, I would first like to start
4 by --

5 MR. MEDINE: Why don't you introduce yourself?

6 MR. HENDRICKS: I am Evan Hendricks. I am the
7 editor and publisher of Privacy Times. I have been
8 reporting on privacy in Washington since 1977, and it puts
9 gray in your beard, I promise you.

10 I wanted to echo the presentation of my colleague
11 Marc Rotenberg, and I wanted to congratulate the FTC for
12 getting these three fine presentations, which really frame
13 the issue to where we are going on this.

14 I have said it before and I will say it again in a
15 way that hopefully people will remember. You can't protect
16 privacy in the way that you just after you get your meal
17 served you sprinkle parmesan cheese on spaghetti. You have
18 to protect privacy by cooking it into the sauce from the
19 very beginning. It sets the ground rules from the beginning
20 and it reduces the back-end cost.

21 Now, when I listen to Mr. Sherman's presentation,
22 I found it very complicated by all the different rules and
23 parameters in setting up, if this, then this. And the more
24 simple way, and the way that I would be advocating through
25 the next two days, is the method adopted by other countries,

1 that you require people's consent before their personal
2 information is used for commercial purposes.

3 And our legal system is based on informed consent
4 in virtually every other context, and it seems to me
5 consistent that we would move to a situation where we have
6 informed consent for use of our personal information given
7 that we are moving into the information age big time.

8 And so also the question as we come into this
9 hearing is what is the role of the Federal Trade Commission
10 in all this. Now, the Chairman said that this is a fact-
11 finding mission, hearing, and Commissioner Varney has said
12 in other interviews that she basically wants to go with the
13 voluntary approach, that it would be premature to do
14 anything else.

15 My hope here in this fact-finding hearing is that
16 as we go through the next two days, as the evidence is
17 presented, that the FTC will see that they have a larger
18 responsibility and a tremendous opportunity at this point in
19 history to take leadership on this issue and recommend and
20 take action to secure the kind of protections that we need
21 now to catch up to where the rest of the world is going.

22 MR. MEDINE: Ron?

23 MR. PLESSER: Thank you. I am Ron Plessner. I am a
24 piper -- I am a partner at Piper & Marbury.

1 I just wanted to add one thing because I think
2 this discussion about the privacy system that we have in
3 this country and information about privacy, we have
4 legislated in this area, and probably one of the few cases
5 where law has preceded technology. In 1988, I think it was
6 in 1986, I guess, the Congress enacted The Electronic
7 Communications Privacy Act, and ECPA really was enacted
8 almost at the front-end of a lot of these concerns.

9 And what ECPA does is some very critical important
10 things. It doesn't do everything, and certainly subjects
11 that have been discussed today are very important in terms
12 of how individual companies use and disclose information.
13 But it is important, I think, to have an extra backdrop
14 because not only is it 10 years later still a good law, it
15 also is a law that I think leads Europe and Canada and many
16 other places in terms of protected privacy. What it does is
17 protect e-mail privacy from government access. It protects
18 e-mail from at least public systems who provide e-mail from
19 disclosing the contents of the information.

20 And in an amendment that was passed, in fact just
21 two years ago, the Digital bill, ECPA controls government
22 access not only for the content of the information, but the
23 descriptive information in the header of the e-mail. It has
24 created a great deal of confidence in the American public, I
25 believe, in the ability to communicate electronically,

1 knowing that the privacy in e-mail and the privacy of other
2 communications from interception or from retrieval and
3 stored data is protected.

4 So I think those, as I will discuss in the
5 European section, but even in this context, it is important
6 to know that we do have at least this one very important
7 privacy law that is very much aimed at digital electronic
8 communications, and I think it does a fairly good job of
9 protecting at least that side of privacy on the Internet.

10 MR. JAFFE: Hi. I am Dan Jaffe of the Association
11 of National Advertisers, and our members do the majority of
12 all national and regional advertising in this country.

13 I think what is interesting about this whole new
14 medium is that probably at the earliest point in the history
15 of any medium business has stepped forward to come up with
16 voluntary approaches to give consumers protection in this
17 area.

18 I think that this is evidence of two things: that
19 business understands the strong privacy concerns in this
20 area, but just for the self-interest of the business
21 community we understand that if people do not feel secure on
22 the Net, they are not going to use it. And it will
23 marginalize this medium as to a very insignificant problem.
24 Unlike what Mr. Rotenberg was saying earlier --

25 MR. ROTENBERG: That's Rotenberg.

1 MR. JAFFE: I'm sorry, excuse me.

2 Mr. Rotenberg.

3 MR. ROTENBERG: You don't know me well enough yet
4 to miscall me.

5 (Laughter.)

6 MR. JAFFE: There were no implications as to your
7 statement and your name.

8 The situation is that the great competitive forces
9 are out there for businesses to be protected, because if
10 they are not protected then you are going to find that the
11 consumers are not going to go on the Net. Nothing forces
12 them onto the Net.

13 In fact, that's one of the interesting factors of
14 the Net, is that there is more control by consumers. This
15 is not a broadcast medium. This is not something that
16 invades your home. This is something that you go out and
17 make decisions as to where you are going to go on the Net.

18 One other thing that hasn't been discussed yet,
19 but I think is important, is that we have to understand that
20 the Internet is a global marketplace. This is why this
21 conference has been called, is to talk about the global
22 information network. And therefore even if the United
23 States were to decide that they were going to try and create
24 a wall around this country, and to try to set up rules,

1 comprehensive rules just for this country, it would miss a
2 tremendous amount of the information that's out there.

3 I have been told, I have not been able to verify
4 this, but I have been told by people that I believe are
5 quite knowledgeable, that more than a third of all of the
6 Worldwide Web is of foreign origin or are foreign based, and
7 that it's even more than that when you talk about all the
8 computers that are connected.

9 Therefore, if we set rules in the United States,
10 that does not in any way assure the control over the network
11 for consumers, and therefore we believe that it's only
12 through self-impoundment of consumers that you are going to
13 get real protections.

14 So we think that is something that has to be
15 factored in. We can't just wave a magic wand, if we can't
16 and nobody else in the Congress can, and suddenly force all
17 sorts of empowerment tools into the consumer's hands. And I
18 think that as we go through this discussion, and I will stop
19 in a second, there are so many others that have important
20 things to say, but we are going to find that in this area we
21 have more control, that technology will give us more power
22 over where we go and what we are going to see. And if we
23 don't see what we want, then we don't have to go into it.

24 In other words, if we don't find that some group
25 has a privacy policy that we want, we don't have to go

1 there, and we are going to very soon, and what is happening
2 now is that consumers are not that knowledgeable, but very
3 quickly they are going to become knowledgeable. People like
4 yourself and others are going to educate them so that they
5 will be knowledgeable, and then they are going to be able,
6 to really be able to develop their own protections whether
7 the companies want to give it to them or not, because if
8 they don't see a privacy flag that means their goals, they
9 just said, "I'm not flying in this area. I am not going to
10 go into this company's network at all because they don't
11 provide me with the protection I want."

12 If they feel secure or they don't care, then they
13 can go where they want, but they will be able to not go
14 where they don't want to. And that's really not true for
15 any other media.

16 MR. MEDINE: Jack.

17 MR. KRUMHOLTZ: I am Jack Krumholtz with Microsoft
18 here on behalf of the Interactive Services Association. The
19 Interactive Services Association is the leading trade
20 association for many of the online service providers,
21 including the Microsoft network.

22 I really want to echo Mr. Jaffe's comment. We
23 believe at the ISA that the keys to privacy are what we
24 refer to as the Two E's, education and empowerment.
25 Education is absolutely critical, and I am pleased that the

1 ISA joined in partnership actually with the National
2 Consumers League earlier this year in an effort to help
3 Project Open, which is a public education effort, and part
4 of that effort is to help consumers understand how to
5 protect their privacy online.

6 And empowerment, to me there are really two key
7 components to that. One is choice, making sure that the
8 consumers have a choice on how the information is used. And
9 I think that the ISA/DMA discussion draft of guidelines were
10 principles that Mr. Sherman referred to earlier, really the
11 fundamental underlying principle of that draft is consumer
12 choice. And, again, just echoing what Mr. Sherman said, we
13 really see this as a first step in this process, and really
14 welcome everyone here to provide comments, because we want
15 this dialogue to continue and to really hear what people
16 think about what our work product is to date.

17 The second component of empowerment I see is
18 technology, and I know we are going to hear more about
19 technology in the next panel. But, again, technology is
20 not, there is no fail safe answer to this. I think we just
21 need to be realistic in that regard.

22 Finally, in approaching -- in approaching privacy
23 we believe we need to balance two things. One, clearly
24 consumer privacy and the need to protect consumer privacy is
25 absolutely critical, and it's critical from a business

1 perspective as well. The point was made earlier that if
2 consumers don't have confidence in how their personal
3 information is being used, they are going to walk away from
4 the Internet, and that is not -- certainly not in my
5 company's best interest or the other members of the ISA.

6 So we need to balance that with commerce, because
7 commerce really is coming to the Net. And if we are too
8 restrictive, marketers and commercial operations are going
9 to leave the Net, and that's going to make the Net more
10 expensive, and less -- and less attractive, and we'll lose
11 the benefits of the great equalizing potential that we
12 believe that the Net has.

13 MR. MEDINE: Thanks.

14 Alan?

15 MR. WESTIN: I am Alan Westin, I am a professor at
16 Columbia University in public law and government, and the
17 publisher of "Privacy & American Business," a newsletter
18 that covers the business privacy issues.

19 In a sense we are all trying to cooperate in
20 painting a canvas and each one is coming up and putting a
21 few more brush strokes on and putting some more detail on in
22 the hope that in the end there is a Rembrandt for both
23 society and regulators and others to look at. So let me try
24 and add my brush strokes and see where they fit in.

1 The first thing, it seems to me, is that we have
2 to understand that people differ in the way they want to
3 balance their disclosure and their claim to privacy. We are
4 not all the same, and the steady stream of the survey
5 research shows that the American public divides up into
6 about a quarter who are intensely concerned with their
7 privacy, roughly the same number who couldn't care less, and
8 about half the population that say it depends on what you
9 are offering me and what benefits I get, or what society
10 gets by way of important values and protection, and also
11 whether the information you are collecting is relevant and
12 socially acceptable; and, finally, whether there are
13 adequate fair information practices, safeguards or other
14 privacy protection safeguards that make sure that the
15 information we give for those purposes is adequately
16 protected.

17 And we really are not all the same in the way in
18 which we want to strike those balances. I think the online,
19 given that that world is challenging and exciting, because
20 it really does offer the first opportunity in the world of
21 information and collection in the consumer area for people
22 to make their own choices about privacy. And it seems to me
23 a healthy thing that neither Jesse Helms nor the ACLU should
24 make the privacy rules for everybody, but that we all will
25 be able to make the choices in a properly structured system.

1 I think it's very authentic in terms of the
2 American social and political and legal culture that we do
3 first look to the voluntary approach because it is, first of
4 all, more efficient if it works. It doesn't require vast
5 policy practices to enforce, and the use of coercive
6 mechanisms, but it has to work.

7 And I think I differ with Marc in the sense that
8 when I use the term "market forces," I see a healthy
9 competition in offering different privacy choices to people
10 in the Internet and online environments as well as
11 elsewhere. And I should think that if we structure it
12 properly, we want a healthy competition in which AT&T and
13 MCI battle over who protects our privacy information better,
14 and that the online services make a similar competition.

15 And that if we see how that shakes out, there may
16 be a point at which the FTC or legislation would come in to
17 incorporate what has developed as an effective means, but we
18 shouldn't rush to write the rules before we really know what
19 the mix of policy and technology and market privacy choices
20 is going to be.

21 One thing that we can offer is that privacy in
22 American business will be conducting the first national
23 survey of how online and Internet users are currently using
24 information, and how they see the world of privacy choices,
25 and we will be releasing the results of this at our national

1 conference on October 9th, and we will be trying to present
2 in the survey the kind of choices about how people opt in or
3 out, or front-end options, and what it is that the American
4 online and Internet users really feel about these issues.

5 MR. MEDINE: Thank you, Bob.

6 MR. SMITH: I am Robert Ellis Smith. I publish
7 Privacy Journal Newsletter.

8 I think it's been a rather healthy discussion so
9 far. I don't accept the Direct Marketing Association's view
10 of the world or the view of the Internet. I think people
11 started maybe a year ago trying to view the Internet as
12 predominantly a commercial medium. It began as
13 predominantly an educational communications medium.

14 If it remains predominantly that with
15 possibilities for advertising only incidentally, then I
16 think we will be safe. But if the becomes predominantly a
17 commercial medium, as the new spin appears to be, then all
18 the safeguards in the world perhaps won't help us.

19 For instance, there are now credit reports being
20 bought and sold anonymously on the Internet. Mr. Jaffe
21 would say I can choose not to deal with that company if I
22 wish not to. My colleague here would say I can choose not
23 to participate in the Internet. I happen to want to take
24 advantage of the communications and educational
25 possibilities of the Internet. Because there are some bad

1 actors there on the Internet who are invading my privacy
2 does not mean that I want to opt out totally from the
3 system.

4 There are currently entrepreneurs selling social
5 security numbers, arrest records, credit reports, other
6 information about people, phone numbers, unlisted phone
7 numbers as well.

8 I think Janlori's solution would say I have some
9 sort of a point and a click option there, that somehow I
10 would have had a relationship with these companies, I could
11 have opted out at some point. I have no idea who they are.
12 They are not even obligated to identify themselves over the
13 Internet. But even if they are, they are certainly not
14 obligated to give me any possibility or voice at the time.

15 I certainly have to agree that the possibilities
16 for voluntary compliance have to be measured up to the Metro
17 Mail experience here. A large company has, I think, four
18 very clear violations of its own trade association's code of
19 ethics, and not a thing has happened. It's still operating.
20 I'm not sure whether the current law would reach some of the
21 activities that Metro Mail had been involved with. But
22 clearly no trade association has come forward to put an end
23 to those egregious invasions of privacy.

24 I think the pattern here is that, and I have seen
25 it in higher education, that business will come here and say

1 we opt for voluntary compliance, we want no cumbersome
2 statutes, and parenthetically I might say that the Telephone
3 Solicitation Act requires no vast police force to enforce
4 it. People have a right to go to Small Claims Court. They
5 have been doing so. It's a rather modest law that seems to
6 be working without any huge federal bureaucracy necessary to
7 enforce it. People are enforcing it themselves by filing
8 claims in Small Claims Court.

9 But the phenomenon that you see is that business
10 argues against any regulation and for self-regulation,
11 voluntary compliance. And then they discover that there are
12 a lot of bad guys in the business. There are people selling
13 credit reports out there anonymously. There are people
14 dealing in social security numbers. And they have an unfair
15 advantage because there is no regulation, and they will be
16 in the same room five years from now begging for regulation,
17 the more reputable larger companies in the business will be
18 begging for regulations five years from now.

19 Why not do it now? Let's anticipate that we are
20 going to have these problems.

21 MR. MEDINE: Thanks.

22 Kathy?

23 MS. KRAUSE: I am Katherine Krause with US West,
24 here today representing the Information Industry
25 Association. That association is comprised of over 500

1 companies that operate nationally and internationally,
2 ranging from large multinationals to small entrepreneurs.

3 And to maybe step a little bit out of the
4 association model here for a minute, I would say I suspect
5 that many of those businesses would feel more comfortable if
6 they were asking for regulation than having someone else
7 suggest that regulation is in their best interest.

8 I think most of those businesses don't believe
9 that regulation is in their best interest. They are
10 tremendously diverse in terms of the information products
11 and services that they offer. They use sometimes personally
12 identifiable information, other times, transactional
13 information that maybe is not personally identifiable.

14 And I believe that in an information society where
15 you have an information economy, information is the fuel
16 that drives that economy in that age.

17 One of the things that I think is a little bit
18 disturbing about the discussion is that Janlori talks about
19 the architecture right now being designed to collect
20 information, almost regardless of whether it's needed, maybe
21 without a level of purpose or with it's very good
22 intentions. I think there is a good deal of truth to that,
23 and I wish I could remember the gentleman from England whose
24 article I read once, who suggested that there is a
25 tremendous difference between data and information; that

1 data is something that simply flows around, and that
2 information is that thing that is brought to the data
3 through intelligence, through creativity, through
4 innovation. That is what we have in this country.

5 We have the strongest and the best information
6 market and information economy in the world, and it did not
7 get there by stifling the free flow of information or by
8 cutting off data at its source. It allows information to
9 flow freely and fully. It provides individuals who have
10 concerns, as Dr. Westin said, with the ability to say that
11 they would prefer that their information not be used. It
12 did not get to be that kind of a burgeoning economy through
13 warnings that look like cigarette warnings.

14 So from the point of view of the Information
15 Industry Association, which has companies ranging from legal
16 research companies, to credit bureaus, to database
17 companies, to telephone companies, to interactive services,
18 to computer manufacturers and software developers, a one
19 size fits all notion either about self-regulation or about
20 government regulation is tremendously disturbing.

21 We would prefer for the market to be able to
22 evolve. Certainly, as I think a number of people have said
23 on this panel, no market can evolve by ignoring a realized
24 consumer concern about privacy. In many sectors of the
25 information industry, in particular, there simply is not a

1 privacy expectation out there that is demanding attention.
2 When it does, it is being attended to in a way that I think
3 is appropriate for the relationship of the business to the
4 consumer, and for the consumer to the commercial
5 environment.

6 Thank you.

7 MR. MEDINE: Thank you. We have about 10 or 15
8 minutes left on this panel. A couple of people have asked
9 to speak. It would be helpful if, in at least part of the
10 focus of your comment if you could address, there seems to
11 be consensus here that privacy should be protected to a
12 degree, and across the board. I have heard every panel
13 member so far say there ought to be some form of privacy
14 protection. It might be helpful if other members in the
15 course of their comments would discuss ways in which that
16 could be accomplished as a transition into our next session,
17 which will talk about technological solutions. But the
18 mechanism, the burdens of who should bear the choice
19 elements would be helpful as part of your discussion.

20 So, first Janlori and then Ron.

21 MS. GOLDMAN: I think it's helpful in this context
22 when we are talking about how to protect privacy on the
23 Internet to remember that the existing privacy laws that we
24 have at the federal level and possibly at the local level do
25 apply to the Internet. Now, most of us that have worked to

1 either fill those gaps or at the federal level or to
2 increase protection and strengthen existing laws recognize
3 that those areas of privacy protection are few and far
4 between.

5 But as Bob Smith mentioned, where credit reports
6 are being sold obviously on the Internet, that is probably
7 against the law, and those certainly give the FTC
8 intersection of interest to come in and say, "What's going
9 on here?" We should be looking at this. There is a law
10 that regulates how credit reports are handled in this
11 country. There are laws that regulate how cable
12 subscription records and video rental lists, and financial
13 records.

14 I would be the first one to say that many of those
15 laws are not strong enough and they need to be strengthened,
16 and we have been working for many years to do that. In
17 addition to existing laws, there are gaps, and we have been
18 working to fill some of those gaps, most notably in the
19 medical records area. But we do not see in the near term
20 any comprehensive legislation protecting that information.

21 There has been, again as David says, lots of
22 consensus around basic principles. Of course, everybody
23 says it's important to protect personal health data. But
24 when it comes down to drafting a law that everyone will

1 support and move it through the Congress, that's another
2 story.

3 So our solution, and, again, it is probably an
4 interim solution but it also recognizes the long-term
5 benefits, is to give people the control over the information
6 at the front-end; have that opportunity in an interactive
7 environment, and not only fill the gaps, but to let people
8 make those decisions and not continue to wait and allow the
9 information to be unprotected in a nonregulatory
10 environment.

11 MR. MEDINE: Ron.

12 MR. PLESSER: I have got three points responding
13 to Bob and David, and hopefully including yours, Bob Smith
14 worrying about the larger issue I think is an excellent one,
15 about what is the purpose of the Internet and this kind of
16 commercialization, and how do we make that choice and
17 decision. And I think that, Bob, I would point you to the,
18 and I, of course, work with DMA and ISA in developing the
19 unsolicited marketing things, and the first one is online
20 solicitations should be posted to newsroom bulletin board
21 and chat rooms, and services or whatever, only when
22 consistent with the forums they follow.

23 So I think there is a great deal of sensitivity
24 from industry's respect that whoever runs the forum, runs
25 the communication, those rules should govern. And if

1 someone wants to set up a space that is only to be limited
2 to education and research that should be respected. MCI has
3 a no spamming rule; that you can't use their system to send
4 unsolicited e-mails to more than 25 people. That would be
5 respected.

6 I think that that issue has been thought through
7 by industry and I think rather than saying it all should be
8 this way or all should be that way, because I think we think
9 it's too large, our number one principle is that people who
10 are setting up these forums and spaces as part of the
11 Internet should be able to control that.

12 So that's also, David, responsive to your point as
13 to who should be doing it. I think the forum operator at
14 whatever level should be able to assert.

15 The second point, nothing we say about self-
16 regulation or guidelines or rules is in any way -- or the
17 importance of regulation -- is meant in any way to limit
18 prosecution for fraud or deception or unfairness. Those
19 things are not media specific. If somebody is going to make
20 a fraud in a telephone call, or in a letter, or in e-mail,
21 or in an electronic -- or in a web page, fraud is fraud,
22 deception is deception. I don't think any of us is talking
23 about how -- what rules should apply, would never mean to
24 suggest that the FTC and other enforcement authorities

1 wouldn't have that continued authority, and I think that is
2 another important rule. There still is a role for that.

3 And the third point I think is an interesting one
4 in terms of why are we doing this and why is it -- why are
5 the Direct Marketing Association and ISA sensitive to
6 unsolicited e-mail. There is a simple reason, which is
7 there is a cost to the consumer as well. It's a little bit
8 like the old fax machine controversy that led to legislation
9 a couple of years ago. There should be consumer interest
10 and consumer ability to limit those things because there is
11 a cost involved. There is space taken up on the e-mail
12 services and stuff like that.

13 And I think that's why you see industry
14 responding, and that's where the interests should be
15 protected.

16 MR. MEDINE: Bob.

17 MR. SHERMAN: Yes, just three very brief points as
18 well. We also encourage law enforcement against fraud and
19 deception. Where the deception also impacts on privacy, we
20 agree, it is legally actionable. I don't think anything
21 prevents the Federal Trade Commission or any other law
22 enforcement authority, to prohibit deceptive action and
23 practices. And if they also impact on privacy, so be it.

24 We are also talking about the same consumers who
25 have become accustomed to notice and choice in traditional

1 media, and who have enjoyed the many benefits of those other
2 media. And we suggest that let's allow them to do the same
3 over the Internet.

4 Finally, although I believe it's inappropriate to
5 discuss any single company in a meeting like this, I would
6 like to point out, however, when through self-regulation a
7 company meets with its trade association and peer group and
8 changes its practices and adopts responsible practices, then
9 self-regulation has worked.

10 MR. HENDRICKS: Well, I wanted to agree with Jack
11 Krumholtz's statement that empowerment is the key -- a key
12 goal here. And what better way to empower individuals than
13 to give them a right where organizations are required to
14 respect their choices.

15 You know, it's like Bob Smith said, and, by the
16 way, Bob has been writing privacy newsletters longer than I
17 have, and look how much gray is in his beard, that
18 organizations -- until we put the requirement that
19 organizations respect people's choices, I am afraid those
20 choices aren't going to be respected.

21 I mean, as I listened to US West's representative
22 speak, I think of the caller ID debate. Well, in
23 California, for instance, the Public Service Commission put
24 a requirement that there had to be a choice between online
25 block, per line blocking, per call blocking, gave people the

1 full range of choices. And sure enough in California a lot
2 of people are exercising that choice. But if it was
3 voluntary they would not have had the opportunity.

4 Now, once people have that choice it comes into
5 question whether caller ID in California, a state that has
6 50 percent unlisted phone numbers, is going to be a viable
7 service, but at least it's based on the choice and people
8 were given that choice.

9 And I too have been -- I have been very
10 disappointed in some of the voluntary policies as they
11 developed, not in the policies themselves, but in the lack
12 of enforcement of it. And that's why, if anyone is not
13 familiar with the Metromail case, I think they should
14 familiarize themselves with it because it really shines a
15 spotlight on the problems with voluntary compliance.

16 And I think, though business representatives don't
17 want to hear people like me say it, that it is in the
18 business community's interest to have a level playing field
19 with good rules. Let me just quickly say this one quote I
20 thought was very revealing, this May 30th issue. It says,
21 "Consumer confidence is essential to the success of Canadian
22 business." That's why we see this legislation very much in
23 everyone's interest. They are talking about the new
24 Canadian movement for a national privacy law for the
25 Information Superhighway. "As one of the most rapidly

1 growing industries in this country, with sales over \$10
2 billion, the direct response marketers understand that
3 consumer confidence must be maintained throughout the
4 economy." That was by John Gustafson, the CEO of the
5 Canadian Direct Marketing Association.

6 And I think that's the kind of leadership, I would
7 like to enforce that, that I would like to see coming out of
8 our business community, because otherwise I am afraid that
9 the abuses of personal information will start being abuses
10 of individuals, and I think we really have an opportunity to
11 get out in front and prevent it at this time.

12 MR. MEDINE: Ariel.

13 MR. POLER: I am Ariel Poler from I/PRO. I will
14 be talking a little bit about I/PRO in the next panel, but I
15 just wanted to point out that regardless of the concept of
16 regulation or self-regulation one thing to keep in mind is
17 that where I/PRO is a company that has been on the Internet
18 for over two years, most of the leading Internet companies
19 are customers or partners, so we are very close in the
20 medium, and two things that somebody has pointed out is most
21 companies needing this, companies like Microsoft, do not
22 know what's going on and what's going to happen in the
23 future. Nobody does. I mean, things are very unpredictable
24 and we are all making things up as we go along.

1 So we don't want to regulate -- I mean, it seems
2 to me that through good regulations, the regulations are not
3 going to be obsolete, they might need to know better what
4 all of the industry, which I must say that it just seems
5 unlikely, and at the same time things are happening at a
6 pace, the change of pace is unprecedented in terms of how
7 fast things are changing and so on.

8 So if you say, well, they won't know the future,
9 but they will adapt to it. But then they would have to
10 start doing regulation 10 or 100 times faster than they have
11 in the past.

12 So I just want to point out that as we try to put
13 an infrastructure around it, and you say, well, it would be
14 better to do it before we cook it, or rather than after it's
15 cooked, number one, we don't know how it's going to look in
16 the future; and, number two, it's being cooked so quickly
17 that we better run very fast. I just wanted to point that
18 out.

19 MR. MEDINE: Thank you.

20 We have time, I think, for three more brief
21 comments. Shirley, then Marc and then Linda.

22 MS. SARNA: I am Shirley Sarna from the New York
23 State Attorney General's Office.

24 I am not an advocate of regulation, but I just
25 want to raise a couple of points to throw out for the folks.

1 We have been talking in fairly theoretical terms. I want to
2 just come back down to earth for a moment and share with you
3 an anecdote, and this relates to the opportunity for
4 technology to solve our problem, and this is shared by a
5 colleague whose family has three VCRs at home. And when he
6 goes home each of them blinks 12, 12, 12.

7 It really raises the larger picture of whose
8 responsibility is this. Is it the job of the consumer, and
9 now I am talking about cyberspace's marketplace because that
10 is where this conversation really sits. It has less to do
11 with what has come before, and it has more to do with the
12 potential of the Net to offer us an array of business
13 services that maybe we have only begun to dream about.

14 But I think there is a very real danger that if
15 this market starts with a taint, that that potential is
16 never going to be reached. And I think that one of the
17 telling things statistically is to know the difference
18 between those who have computers, which are now bought and
19 sold like refrigerators, or the VCR that goes 12, 12, 12.
20 The access which is tremendous, and the actual number of
21 sales on the Internet, which is a fraction of what that
22 potential could be.

23 Now, for sure part of that has to do with the fact
24 that there is not a universally recognized secure system for
25 payment. But nevertheless, I wonder how much of it also has

1 to do with the generalized sense of insecurity. When we
2 talk about consumer choice, we assume that that choice has
3 to be based on full information.

4 Do consumers really understand the potential for
5 the data- or information-gathering capabilities of this
6 medium?

7 When I got my wake up call this morning at the
8 hotel, I heard "Good morning, Ms. Sarna." I would not have
9 liked to hear, "Good morning, Ms. Sarna, I heard you had to
10 change your carrier last night. You left at 7:00. You had
11 trouble with your taxi. You got to the hotel at 10:30, but
12 welcome."

13 So would I understand at the front-end of that
14 conversation what it is that I am giving up?

15 So because I understand that time is short, I
16 guess the points that I am making are, number one, when we
17 look to technology, we really have to understand who our
18 user population is going to be. If you don't get my
19 colleague's mother and father whose VCR goes 12, 12, 12, you
20 all have eliminated a tremendous segment of the population.

21 And number two, whose job is this anyway? Who
22 owns this data in a very real down to earth sense? Is it my
23 job to say before I get on this, it's yours, and I will tell
24 you which piece of it I want to take back, or is this start
25 of the conversation it's out there, and I will -- and you

1 tell me that it's out there, and I will just give the
2 permission on certain segments?

3 And I think those are in the mix important
4 questions to keep in mind.

5 MR. MEDINE: Thanks again.

6 I will just as the Chair ask for some very brief
7 comments from Marc, and then Linda, and then we will break.

8 MR. ROTENBERG: Okay, I will make just two very
9 brief points. Unfortunately, my battery has just kicked
10 out. So much for the technology.

11 MS. SARNA: It's another problem.

12 MR. ROTENBERG: This is the first panel. We are
13 trying to set a framework for the day, and there is a
14 critical concept that I think we leave this first panel
15 with. And that is the notion of a code of fair information
16 practices. That is the cornerstone of privacy policy. It
17 is the building block of privacy law. It means simply that
18 when you collect personally identifiable information you
19 have some responsibility to the people to whom the
20 information refers. And it is those codes of fair
21 information practice that develop as industry codes and
22 professional codes that are translated into law, into
23 technical standards, and they are very much a "Made in
24 America" policy approach. This is not anything that is
25 profound. This is how we regulate the credit reporting

1 industry. These are privacy responsibilities that are
2 placed on cable companies, e-mail companies, video sales
3 companies. This is the way we have to proceed if we are
4 going to get privacy on the Internet.

5 The second point is that there is a fantastic
6 opportunity to do this right. The Internet and the
7 information society is too malleable to suggest that we
8 can't find one out of this limitless slew of options that
9 both protects consumer privacy and allows business to
10 prosper I think is a type of denial that does not help the
11 policy process.

12 But at the same time it should be clear that
13 that's our goal, to protect consumer privacy and allow
14 business to prosper.

15 And the third point is that everyone will say that
16 privacy is important. Everyone will say it. The question
17 always is what will they do, and what would they do in their
18 own business, in their own industry, in their own agency to
19 make real that promise that privacy should be important. If
20 we just talk about privacy being important, we don't go
21 anywhere. We need to see what will change.

22 MR. MEDINE: Actually, the next session will be
23 devoted to some options for businesses to follow and Linda
24 will have the last work in this session.

1 MS. GOLODNER: Linda Golodner with the National
2 Consumers League.

3 There are some consumer rights that we always use
4 whenever we are talking about any business, any product, any
5 service, and I think we have to be reminded of those.

6 We have been talking an awful lot about
7 information, information on disclosure that is given, that
8 there will be information given by Direct Marketing
9 Association members that maybe have had a previous
10 relationship.

11 But another important right is the right to
12 education, and that is different from information.
13 Education means educating people about understanding what
14 privacy is, understanding what they are giving up when they
15 are giving information over the Internet.

16 So those are two separate things that I think we
17 have to keep separate. And I think that consumers must be
18 able to have control of that information that they give out,
19 and that every business should be required to have some sort
20 of privacy principles that are put up front so that people
21 understand what they are before they are going to engage
22 business with them on the Internet or online.

23 We are putting an awful heavy burden on the
24 Federal Trade Commission to look at everything out there.
25 And so I think that very, very strong guidelines have to be

1 put in place. Everyone doesn't want fraud. We certainly
2 are, I think, in agreement on that. But then there are
3 those that are in sort of the shady area that might not be
4 fraudulent, and might be sort of legal. Those are the ones
5 that I think we all have to have tough regulations for.

6 The National Consumers League, as part of our
7 National Fraud Information Center, has put up the Internet
8 fraud watch, and I think it's just a tip of the iceberg, and
9 that we have been sharing the information with the National
10 Association of Attorneys General and the FTC. And I think
11 there is going to be a lot more fraud out there, but there
12 are also going to be those shady characters that don't have
13 any regulation for them.

14 MR. MEDINE: Thank you, Linda. Thank you to all
15 the panel members for helping set an excellent framework for
16 the discussions for the rest of the day.

17 For those who are standing, I just want to remind
18 you that there is an overflow room in 332, if you would like
19 to be more relaxed.

20 We will take a 10-minute break and reset the panel
21 and be back.

22 (Whereupon, a recess was taken.)

23 MR. MEDINE: Thank you. Let's get started with
24 the session on electronic regimes for protecting consumer
25 privacy. If you want to talk, please go outside. We would

1 like to get started. We have a lot to cover this morning.
2 Thank you.

3 Before we get started with our first
4 demonstration, John Kamp didn't get called on at the last
5 session and would like a chance to make some comments. If
6 you want to identify yourself.

7 MR. KAMP: I am John Kamp. I am with the American
8 Association of Advertising Agencies. I was thinking as this
9 panel was concluded that an operational principal that we
10 might take forward through today and tomorrow would be that
11 we are exactly where we want to be on this issue; that
12 virtually all of the forces that need to be focusing on this
13 and paying attention are doing exactly that.

14 It may be that my operational principle is one
15 that is guaranteed not to have the full assent of anyone on
16 this panel, because all of us are at least somewhat uneasy
17 about where we are right now. But it appears to me that if
18 we look at the panel and we think about the kinds of things
19 that are going on, exactly the right things are going on.

20 I will pick up, in effect, as we watch this issue,
21 one of the seminal documents on this came from the Office of
22 Management and Budget last year which did, in effect, a kind
23 of rule-making without having done rules, deciding very much
24 that principles were in order as opposed to laws. But
25 essentially focusing on the fact that there are really three

1 major institutions, groups that need to focus on education,
2 enforcement, careful protection of privacy, and that we
3 must, particularly with this medium, be very careful not to
4 regulate too soon.

5 So I only start with that because I think that
6 many of the forces are here. I see Dan Jaffe and myself
7 representing CASIE, an organization that has developed a set
8 of goals on privacy for advertising in the advertising
9 community, the Interactive Services Association, DMA and
10 others, the organizations that need to focus on it, because
11 their numbers are likely to become major players on the
12 commercial use of this medium, are doing so.

13 The FTC is here in full force, and if anyone
14 thinks that the cop is not on the beat, both they and the
15 Attorney Generals are here; consumer groups, the National
16 Consumers League, and others are here, other institutions.
17 We will also be hearing from the Better Business Bureau,
18 CARU and others that are part of the Better Business Bureau,
19 developing another kind of shadow law enforcement agency.

20 If any of us think that if we sleep, it will be
21 forgotten, clearly those privacy advocates from the academic
22 institutions and the journals and others are here to make
23 sure that all of our consciences are tickled.

1 So I would like to try that as a thought, that
2 maybe we are exactly where we want to be, and the goal is
3 where would we want to be at this time next year.

4 Thank you.

5 MR. MEDINE: Okay, thank you.

6 As with the last session, we are going to start
7 with a couple of crystallizers. As we move forward in the
8 morning, I would like to shift from general statements about
9 the problem and general statements about solutions to being
10 very specific. We are going to see some demonstrations of
11 some specific approaches, but it would also be useful when
12 panel members speak to talk about the specific kinds of
13 information that can be collected or is being collected
14 today, and what could be done about it.

15 The first demonstration, first crystallizer in the
16 session will be Ariel Poler. Ariel, as we heard in the last
17 panel, is founder and Chairman of I/PRO, which is Internet
18 Profiles Corporation.

19 MR. POLER: For those of you who are not familiar
20 with I/PRO, what we try to do is help organizations on the
21 Web make the most of their Web efforts by understanding
22 better the consumers, and helping consumers get the most out
23 of the Web without compromising their privacy.

24 Now, we are better known as a market research
25 company, but privacy is not something that was an

1 afterthought. Actually, the first two names that I thought
2 for I/PRO were Privacy in Cyberspace, Private Internet
3 Domain. I couldn't trademark either of them as PIC or PID,
4 so I kept changing until I got to I/PRO.

5 So trying to do all of this and collect this
6 information with the privacy of the consumers in mind is
7 what I/PRO was about from the beginning.

8 I am going to give you a quick showing of the way
9 our system works, and I will start by just telling you what
10 the principles that we have are.

11 They start by saying let's put the consumer in the
12 driver's seat, meaning that they get to control who gets the
13 information and who doesn't on a site-by-site basis, and we
14 are very Internet-centric, by the way. They get to control
15 what level of information each of these sites gets. Some
16 sites might get all the information that consumer wants but
17 some might get none, or some might get anonymous
18 information, et cetera. They get to control who can send
19 them information and who cannot.

20 Again, we are not saying nobody should be able to
21 send them. We are saying the consumer is the one who needs
22 to decide, and the consumers should also be able to decide
23 what kind of information each particular site can send them.

24 We allow consumers to update and modify the
25 information. It shouldn't be the case that they provide it

1 and then it's gone. They should be able to control their
2 information. We believe that all of our customers and
3 partners need to recognize the value of information. It can
4 never be the case that someone collects consumers'
5 information and then just says, help me out, give me
6 information. Thank you very much. There needs to be
7 something in it for the consumer at all times because their
8 time and information are valuable. It's more of a market
9 thing rather than a privacy thing, but still important.

10 Finally, we think that we cannot damage the
11 experience, and a lot of the things added to collect a lot
12 of the information or to protect the privacy from the forms
13 and disclaimers and so on can end up really disrupting the
14 whole interactive process which we are very much against, no
15 matter if you are doing it to collect more information, as I
16 said, or to protect consumers.

17 We have a system that we launched, where, for
18 every site that can today control zero, anonymous
19 demographics or identity. And we know you will be able to
20 do more finer grain of disclosure. Again, the consumer can
21 say I have these interests, and I want you to send me
22 information about these things, and they can say here is my
23 name, put me on your mailing list if the consumer wants, or
24 they can say send me information, but I don't want the

1 advertisers to know where I am. I am just interested in a
2 particular area.

3 The moment they change the profile and say I'm not
4 interested in this anymore, then they don't get any more
5 information about that, to get the benefit of customized
6 information without getting junk mail that people get.

7 Currently, the system that we have in place and
8 you can go out on the Web if you go through our demo, we
9 just launched it commercially, by the way, two and a half
10 months ago, we have had 450,000 consumers join in these two
11 and a half months, all of their own free will, and decided
12 and said, yes, this type of thing is worthwhile for me, I
13 will do it. These things could make sense, and we have
14 somewhere on the order of 30 or 40,000 people signing up
15 every week, and some 25 or 35.

16 We are also making it more seamless, and I will
17 give you a free sample of that, so let me then click to that
18 one very quickly. I apologize for rambling.

19 So this it. The Sharper Image, which is a
20 retailer, and they are using our system. If the consumer
21 clicks here, I want a complementary catalogue. I just
22 downloaded this a few minutes ago and I will just take you
23 through it.

24 Then this is the prototype that goes into a local
25 data outfit. Basically that piece of information that says

1 the icon for Ariel is in my hard disk, then I have the
2 option of saying send my anonymous information, send some
3 demographics about me without sending e-mail or anything
4 like that, or I can say send complete information. Again,
5 it's a free market and it's up to the consumer and they
6 decide to say what am I going to give you, what are you
7 willing to give me in exchange, and it is sent.

8 So if the consumers say, well, if I were to send a
9 complete set of information, obviously I would get a
10 customized page that says the material, and they can know
11 about what my interests are and so on. And because I am
12 sending this information to Sharper Image doesn't mean that
13 it will go to other -- I don't know, to Microsoft or to
14 Netscape or to any other site out there, USA Today, and they
15 say go ahead and give it to them. They get to choose at
16 every site.

17 The way it works today, and I just pulled this up
18 from the Web. This is the real page from The Sharper Image
19 today. What I showed you before is a prototype. The way it
20 works today is you have to provide an I/code, which you type
21 there, it's a code, and the I/code alone is anonymous. If
22 you are willing to disclose all the information, you provide
23 your e-mail. So a combination of I/code and e-mail then
24 provides the information.

1 So, since I want to keep it short, I will leave it
2 at that and then we can open it. We believe that we are
3 helping bring out all the value that the Web can provide to
4 the consumers in a way that really protects the privacy.

5 So thank you.

6 MR. MEDINE: The next speaker is Peter Harter, who
7 is public policy counselor for Netscape Communications
8 Corporation, and he is responsible for Internet law, policy
9 issues and strategies.

10 MR. HARTER: Thank you and good morning.

11 It's good to be back here at the FTC for another
12 workshop. I attended a workshop back here a year and a
13 month ago, in April of '95. I was not at Netscape then. I
14 was on the other side of the fence working for a nonprofit,
15 but equally concerned with privacy and related issues on the
16 Internet. And back then few people knew what Netscape was,
17 but then new things happened in August and September, and
18 we've kind of been very busy since then.

19 It's very interesting to work in an industry
20 where, as some have already identified this morning, where
21 you don't know where the future is. Small and large
22 companies, companies that are just beginning to come into
23 existence now, here and elsewhere, we have to bear in mind
24 that the software industry, or the high tech industry is not
25 just a U.S. phenomenon. There are software industries in

1 the U.K. Germany, South Africa, Australia, India, Japan,
2 just to name a few of them, and they are rapidly ramping up,
3 and competing with us right now on a variety of issues.

4 And privacy, it seems to me, in a general sense is
5 somewhat of a snake. But when you see a snake, it's an
6 opportunity. I think if you can determine ways to add value
7 to your products, whether you are a small software
8 manufacturer or a very large one, with many different
9 integrated products for an online service provider or an
10 Internet service provider, or an Orbach or Telco, or whoever
11 you are, if you can offer privacy as part of your services,
12 and add value, if you build up a relationship of trust with
13 your customer, I think you'll have a very loyal customer,
14 and you will benefit in the long run.

15 Having said that as background, the main thing I
16 want to talk about, the most about during my comments this
17 morning, and I am sure I will get asked a few questions. I
18 have been warned already, about cookies.

19 The basic recipe for cookies is that's it's a
20 solution for a technology that was built to defend this
21 country against an atomic attack. The Internet or Arpanet,
22 is a decentralized network of computer networks running
23 different hardware, different software, connected by
24 different telecommunications means: radio, satellite,
25 fiber, cable, copper, what have you. And the theory was if

1 one of these networks or nodes was taken out by a hit, the
2 rest of the defense group could inter-communicate because
3 the other computer networks could route the information
4 around it. That was 25 years ago.

5 And although the same protocols that enable all
6 these different computer networks no matter where they are
7 located, no matter what their hardware or software systems
8 are to inter-communicate, the language of TCP/IP is 25 years
9 old, and the engineers tell me it is going to be changing
10 rapidly in the next few years to scale up to the
11 commercialization of the medium. There are some interim
12 stop gap measures, and one of them is cookies.

13 The problem with the particular protocol the Web
14 relies upon is HTTP, or hyper text transfer protocol, is
15 that HTTP is a stateless medium, meaning that when your
16 desktop computer, or what we call technically a client,
17 wants to interact with information on the Web, from a site
18 or technically a server, the client server technology that's
19 been around almost as long as the Internet, you know, just
20 transfers itself on top of the client server architecture.

21 When you go to a server, and I use L.L. Bean
22 frequently, I don't have any L.L. Bean clothes, I don't own
23 any stock in L.L. Bean, but you go to L.L. Bean, and you go
24 to the Web site, and theoretically you go from one page to
25 another. When you are surfing their site, moving from one

1 page to another from the men's clothes to the tents to the
2 women's clothes, you are Christmas shopping, the server
3 won't know it's the same person, the same client, just
4 because you connect and reconnect, connect and reconnect.
5 You have to download each page. It's a stateless medium.

6 In order to overcome this in that transactional
7 scenario, a device called cookies, or magic cookies, were
8 created to put information on the client side of the
9 transaction. So when you are engaging in a transaction with
10 the server, such as L.L. Bean, you submit information to
11 them. I want to buy this red shirt, this size at this
12 price. You point and click, fill in the blanks to buy that
13 item on their site. And the server will put that
14 information on your machine in a cookie text file. That
15 file is unique to that server. Only that server can read
16 it.

17 The J. Crew server, if you go shopping there,
18 can't read your magic cookie from L.L. Bean.

19 Now, there is not just a need for cookies in the
20 transactional scenario for merchants. Say you subscribe to
21 a newspaper online, but you speak Spanish. The Internet is
22 not just an English-only world. It's multilingual, and
23 increasingly so. And the fact of the matter is software and
24 service providers can create the text in one language and it
25 can appear on your computer in a different language.

1 So if you subscribe to this magazine, and most
2 magazines online have a free area, but if you subscribe, you
3 have to have a password or some other way to enter in to get
4 all the content. In order to get access, maybe a cookie
5 file could be used by that magazine, not only to indicate to
6 the server when you come back to it that it is indeed you
7 again, and that you are a subscriber as it reads this cookie
8 file, but that cookie file can also have other persistent
9 information, such as how long does your subscription last in
10 terms of the expiration date, which is a feature of a cookie
11 file.

12 But if the expiration date is not set by the
13 server, and you disconnect from the server, the cookie file
14 goes away because there is nothing in it telling it to
15 persist. So the expiration is an optional feature of the
16 cookie files, it's an important technical detail.

17 Because people have asked me why do cookie files
18 keep growing on my hard drive, and they have a hard time
19 understanding that, unless all the sites they go to have
20 long-term expiration dates in the cookie files.

21 But getting back to the point about the magazine.
22 The cookie file can contain your subscription period, what
23 language you are so when the page comes up it comes up in
24 the language you want to see, so you don't have to go to the

1 main page and then look for the Spanish hyperlink, and then
2 wait some more for that Spanish front page to come down.

3 Also, for those of you who access the Internet
4 over low speed connections, waiting for the main home page
5 to download and then find that little link at the bottom of
6 the page, "click here for the plain text version." Imagine
7 if the file indicated to the server that you only wanted
8 the plain text version so you wouldn't have to suffer with
9 excessive download times if your connection is not that
10 wide.

11 And there are many other ways to use cookie files
12 in this manner. So if you go to a site, and the site has
13 preferences or options for your privacy concerns, your first
14 connection time with that server you can tell the server how
15 you want it to use your personally identifiable information.
16 You fill out a form, and they know what they can and cannot
17 do with your personally identifiable information, which you
18 over the course of a transaction, or subsequent transactions
19 with that server, what you will send to it, by filling out
20 forms, or what have you, they'll have that preference
21 indicated in the cookie file.

22 And one last thing, people are concerned and ask
23 me, why is it not more possible and more conspicuous to the
24 user to see these cookie files. And in version 3.0 of the
25 Navigator, in the preferences files you can click on an

1 alert option, and so when a cookie file -- before a cookie
2 file is put on your client by the server, an alarm will go
3 off.

4 A few other points about cookies, and in the
5 general context of the Internet, there are two kinds of
6 cookies: plain old cookies, and then secure cookies. Plain
7 old cookies use hyper text transfer protocol, and then there
8 is another protocol called SHTTP, or secure hyper text
9 transfer protocol. The encryption is used. And some of you
10 may be aware of this other debate swirling in this town, of
11 encryption and export controls.

12 Well, if privacy is really to be maintained, I
13 would say that encryption is a great killer app for privacy
14 concerns and products. However, because of export controls
15 in the U.S., we can't use encryption that works. We can't
16 sell strong encryptor products outside the U.S., so the
17 whole idea of protecting privacy in this global medium is at
18 odds with the needs of encryption.

19 And while coming from California to Washington
20 this weekend I read through the EU Directive on privacy
21 again, and noticed an inconsistency, and I would like to
22 hear comments to see if I am on the right spot or not.

23 In Section 6, Article 13, paragraph one, it
24 roughly states that member states may restrict the scope of
25 obligations and rights of the Directive when such a

1 restriction constitutes a necessary measure to safeguard
2 national security or public safety.

3 And one of the areas of the Directive they may
4 restrict for these reasons is Article 6, Section 1 --
5 Section 1, Article 6, paragraph one, pardon me. Generally
6 the principles related to data quality: accuracy, the date,
7 the integrity. These are very important qualities to secure
8 that kind of commerce. When you have a transaction from a
9 client to a server, you want to make sure that information
10 you send is not read by someone else in transit; that it
11 arrives in the form in which you sent it, so the receiver
12 gets the accurate message; and that they indeed know it was
13 you who sent it at that accurate time.

14 Unfortunately, if member states of EU can opt out
15 of the privacy Directive under the provisions of national
16 security, public security, then I propose that French
17 legislation, which is going to implement a trusted third
18 party regime, escrowing the keys to encryption, is at odds
19 with privacy in Europe?

20 So the conclusion is that the privacy Directive
21 looming in Europe now is somewhat, from an encryption point
22 of view, on shaky ground. So I hope these are ideas for
23 thought this morning.

24 Thank you.

1 MR. MEDINE: Thank you. I believe you are set for
2 this afternoon's session a host of possibilities.

3 I will ask for crystallizing this morning, I will
4 call Paul Resnick, who is a founding member of the Public
5 Policy and Research Department at AT&T, and co-chair of the
6 Technical Committee for PICS. He will speak along with
7 Albert Vezza, who is Associate Director of the Laboratory
8 for Computer Science at MIT. He is also chairman of the
9 Worldwide Web Consortium.

10 MR. VEZZA: I think I will go first to set the
11 stage. I want to tell you a little bit about the Worldwide
12 Web Consortium. It's a consortium, it's a worldwide
13 consortium of over 140 companies. There are over 50 in
14 Europe and 15 in Asia and over 65 in the United States. And
15 I say "over," because if you add those up they only add up
16 to 130. I don't know the breakdown of the other 10 or 12.

17 The Worldwide Web Consortium does have a host
18 partner in Europe, INRIA, which is another computer science
19 lab in France. They are responsible for the European
20 theater. I am hoping that by the end of the month or early
21 July we will have a partner in Japan, a host partner in
22 Japan. And the whole goal of this is to develop a single
23 Worldwide Web standard, a set of standards.

24 Under the auspices of the Worldwide Web
25 Consortium, the PICS protocol was developed, and I want to

1 say that this was done -- our first meeting with our
2 members, which included some 22 or 23 member companies, or
3 other companies, was held on August 15, 1995. Since then we
4 have specs out and I understand that several of our
5 companies are announcing product this month that will have
6 both browsers and rating services using the PICS standard.

7 I want to say a little bit about PICS itself. At
8 that very first meeting we recognized that the United States
9 was a diverse society, and if I look real wide, we are even
10 more diverse, and the mores of countries or even cities in
11 the United States are different from one to another.

12 So therefore we decided that we would develop what
13 we called a viewpoint-neutral technology for labeling
14 content. That would allow many rating services to co-exist,
15 so that a parent, an individual or a teacher could choose
16 whatever rating services, whatever rating service they wish
17 to subscribe to in order to control the filtering of the
18 content that came into their home or classroom, or office,
19 for that matter.

20 I would like to -- Paul is going to give a demo
21 and is going to talk mainly about the technology, but what I
22 would like to do is answer one question that I get asked all
23 the time. And, in fact, I was asked this on the stand in
24 Philadelphia, and that is, is the technology foolproof?

1 The answer to that is no. Children can and will
2 get around it. But the answer to give is the technology is
3 not a substitute for good parenting.

4 Now, is PICS useful in the privacy domain? We
5 believe so. That's why we are here. It's a labeling
6 technology. You have to extend it somewhat in order to use
7 it in the privacy domain. However, just as in the rating
8 domain, technology is not foolproof, and a bad actor can in
9 fact violate privacy even if the communication between a
10 server and a client states how my private information should
11 be used.

12 However, given that, I don't think that we should
13 not use the technology, and I don't think that we should
14 ignore it.

15 MR. RESNICK: Like Ariel, I am going to just relax
16 here. I am going to -- my name is Paul Resnick, and I am
17 going to show you some technologies that will really help in
18 that notice and choice process, the informed consent part.

19 Before I do that, I want to just explain my role
20 in this. I am the co-chair of the PICS, PICS Technical
21 Committee, which is a project of MIT's Worldwide Web
22 Consortium. I work for AT&T, AT&T Research, which is the
23 portion of the old Bell Labs that stayed with AT&T in the
24 recent breakup.

1 I joined AT&T about a year ago to start a new
2 public policy research department. It will be forward-
3 looking, trying to identify important public policy goals
4 and thinking about ways that we can address those goals
5 through new communication technologies.

6 We want to make an online environment where it's
7 safe, fun and profitable to interact with people you don't
8 know very well. So we are very interested in these privacy
9 applications, and I think PICS can be an important component
10 in doing that.

11 I am going to start by giving a demo of PICS for
12 its original purpose so that you can understand what the
13 technology really is. That original purpose was to allow
14 parents to block children's access to materials that the
15 parents think are inappropriate for kids; typically,
16 pornography, things like that.

17 Then I go into a demo of how we might apply this
18 technology for controlling access or blocking access to
19 sites whose information practices you don't like. And then
20 I will go beyond that and say that maybe blocking access
21 isn't the thing we really want. What we really want is to
22 support the notice and choice process, and maybe even go
23 beyond that and have some kind of automated negotiation.
24 And finally, I will discuss some implementation issues like

1 who is going to provide the notice, who is going to certify
2 that the notice is accurate.

3 I can describe the PICS technology with one
4 diagram. In between the child and the material that's out
5 there on the Internet, there is going to be some stuff that
6 intervenes. In particular, some label reading software,
7 blocking software that will allow you to access some things
8 but not everything.

9 And the way it's going to decide which things to
10 permit and which to prohibit is based upon these rating
11 labels. So a single document might have several rating
12 labels associated with it. One of them might come from the
13 publisher, much as manufacturers attach labels to their
14 consumable goods, but these labels might also come from
15 third parties who would have well-known places that you go
16 to check with these labels; not just people going back into
17 the Consumer Reports magazine to check for their reviews of
18 products.

19 The parent is going to choose which labels to pay
20 attention to and which ones to ignore. And even within --
21 once they have decided that, decide which labels indicate
22 things that are appropriate and which things indicate that
23 they are not appropriate.

24 What PICS has added to this mixture is a format
25 for the rating labels, which allows the software and the

1 labels to be developed independently. So a big company that
2 wants to remain value neutral, a software company can
3 provide just the software, not get into the rating business.
4 A values-oriented organization, like a church or teachers or
5 a magazine, can provide the rating labels without having to
6 provide the software. So PICS is neither the software that
7 I am going to show you nor the labels that it's using. It's
8 the glue that makes them work together, even though they are
9 developed independently.

10 I have set up a little demo page. By the way, the
11 software that I am going to show you, it's not PICS. It's
12 just the software from Microsoft. It's their next version
13 of Internet Explorer or their web browser, and they have
14 built in the ability to read these PICS labels.

15 So I have set up a little demo page. There are
16 some things that are on the web that are uncontroversial.
17 Everybody should be able to get access to, like the PICS
18 demo -- like the PICS home page. Then there are things that
19 some people might want to have their kids access that others
20 would prefer not to, like Michelangelo's David, or pictures
21 of Hiroshima burn victims. I know we are going to have
22 lunch soon, so I won't subject you to that one. And then,
23 of course, there is Playboy's home page. In this case, I
24 can't get to it. The software is blocking my access because

1 I told it to look at the labels and block access to things
2 that have too much nudity in them.

3 Now, there is an option to override this. The
4 child that has been blocked, they can go to their parents
5 and say, "I really need this for my important science
6 project."

7 (Laughter.)

8 The parent says, "Sure."

9 Now, I have actually edited this down a little.
10 Now I didn't take out any nude pictures. There are no nude
11 pictures on their first page. They do have some
12 advertisements and a few more options. I edited it down so
13 that you could see what's at the bottom. It says, "We rated
14 with RSAC i." Now, some of you can't see that, even though
15 it's there. So that's as high as I can get it right now.

16 But what Playboy has done is they have voluntarily
17 chosen to label their site using a rating system set up by
18 the Recreational Software Advisory Council. It's an
19 organization that originally set up a rating system for
20 computer games. It was in response to concerns about
21 violence.

22 So about a month ago they set up an Internet
23 rating service. Playboy voluntarily chose to connect to the
24 RSAC site, fill out a detailed questionnaire, and they ended
25 up rating themselves on four separate dimensions: how

1 extreme the language is, the nudity, the amount of nudity,
2 sex and violence. They get four separate ratings, each on a
3 scale from zero to four.

4 Then they chose to put that label -- they got a
5 label back from RSAC and they stuck it into their site.
6 It's actually in the background. It's not displayed here,
7 but it's in the background and the software is able to look
8 at it and decide to block or access based on that.

9 So this is all sort of stuff that's real. It's
10 out there on the Internet today. Playboy really did do that
11 labeling.

12 I am now going to talk about a more hypothetical
13 application where we could use this technology but it isn't
14 yet being used. And PIC allows anybody to create a new
15 labeling vocabulary, and then go out and start labeling
16 things. And actually, Joel Reidenberg a couple of weeks
17 ago, who is up there spending some time with us at AT&T this
18 summer, took the Canadian Standards Association's fair
19 information practices guidelines and turned that into a
20 PICS-compatible labeling vocabulary.

21 They have done that and I have made a fictitious
22 telemarketer's web site here which unlike any real
23 telemarketer this one has -- this one has terrible privacy
24 practices. They don't conform to any of the Canadian
25 Standards Associations guidelines, and they will do anything

1 with your data. They won't tell you about it. They will
2 sell it, whatever. The only thing great is that they are
3 really up-front about this. They do tell you that that's
4 what they do. And not only that, they have put in a label
5 to that effect in this PICS-compatible format.

6 So I am now going to go -- right now I have the
7 software with the volume turned all the way up, basically
8 saying I don't care about privacy at all. I'm going to go
9 in and change the volume to say that I do care about some of
10 those Canadian Standards Association guidelines. Then we
11 will see that this site also gets blocked.

12 So on these browsers you typically get a bunch of
13 options for things that you can configure. The new one with
14 PICS is this ability to set ratings. And again, I have to
15 enter the password, we don't want the kids to be changing
16 the rules. Now you can see that I have this Canadian
17 Standards Association labeling system. There are a bunch of
18 dimensions in the Canadian Standards guidelines:
19 accountability, accuracy, consent and so on.

20 If I go down to accountability, you see I have the
21 volume turned all the way up. I will connect to this site
22 even if they take no responsibility for their information
23 practices, and there is no designated person responsible.

24 But let's say I did care a little bit about this
25 dimension. I can turn the volume down and say that, well, I

1 want the organization to take responsibility, but it's okay
2 if they don't have a designated person. Or I could say that
3 they have really got to follow the Canadian Standards
4 guidelines, which is the organization responsible and there
5 is a designated person.

6 So I could similarly go through some of the other
7 dimensions, but I won't do that now. Of course, I have
8 already got it loaded here, so I am going to have to clearly
9 come back to it, and then you will see that I won't be able
10 to get back to it anymore.

11 Again, we have the similar screen that we had with
12 the Playboy.

13 So, now, this gets us part of the way to where we
14 want to go, but you can see some of the legacy of what this
15 technology was originally designed for. And with the
16 privacy application, you probably don't want to block access
17 to things where your preferences don't match the site's
18 practices. Instead, you want something to be more in the
19 spirit of notice and choice. So I mocked up what that might
20 look like. Instead of getting that thing we saw, instead we
21 get something like this that gives you some information.

22 Your preferences don't match this site's practices
23 on the following dimension: accountability. And not only
24 that, the site has sent you back a little textual
25 information of why they don't match. In this case it's

1 because they believe everyone in the company is responsible,
2 and they haven't designated just one person to do the
3 enforcement.

4 You now have the choice. You can -- if this
5 really bothers you, you can back out and not deal with this
6 web site. If you don't mind, you can just close the window
7 and go on. I mean, you might even think about doing better
8 than just this notice. There might be some choices. The
9 site would say, well, if we offer you a \$5.00 discount,
10 would you accept -- would you accept our information
11 practices, and there would be a little check box.

12 Or even better, you might have some automated
13 negotiation. The sites says, oh, your preferences are that
14 you don't want me to collect data, that's fine. I am going
15 to give you a more limited version of my service. You won't
16 get all the customization features that I offer, but you can
17 still interact. And again, that's all in the background so
18 that users aren't constantly having to look at all the fine
19 print.

20 So this is a, I think, promising technology. It
21 is certainly worth exploring. The big idea here is that if
22 we put the notice into some standard format, and allow
23 people to express their preferences, the software can
24 automatically do the comparison, and at least sometimes the

1 notice and choice will be happening in the background,
2 rather than always being a burden.

3 What would it take to get this going? I think
4 there are three issues.

5 The first is the labeling vocabulary. If we are
6 going to rely on sites to label themselves, to disclose what
7 their information practices are, we are really going to need
8 to do that in a common vocabulary that all the sites use the
9 same vocabulary. They don't need the same information
10 practices. There is room for lots of variation there. They
11 need to use the same vocabulary for describing them.

12 And that vocabulary might be based on the Canadian
13 Standards Association, or OECD, or European Directive, or it
14 might be something new that we make up.

15 The second issue is who is going to actually
16 create the labels. In the indecency realm, the Simon
17 Weisenthal Center can go out and find neo-nazi material and
18 label it, even without the cooperation of the neo-nazi
19 group, because they can look at the pages and tell whether
20 it's hate speech or not.

21 The privacy and information practices might not be
22 so apparent, but I think it's going to be harder for EPIC to
23 go out and create a service, although it's possible that
24 they might be able to.

1 Another model is that we would have self-
2 disclosure, self-labeling, but sites might voluntarily
3 submit to some auditing group that would certify that the
4 labels are accurate. And I hope that some time either in
5 this panel or when you talk about the European stuff,
6 someone will ask Joel about the advantages of the certifying
7 authority notion for complying with the European regulations
8 on transported data points.

9 And the third issue, I think, is a start-up one.
10 It would be real nice if when 20 sites label themselves,
11 there would be some benefit for consumers. And as more
12 sites label, you would get even more benefit. I am afraid
13 that we might be in a critical mass situation instead. But
14 unless a large percentage of sites get on board, the
15 consumers aren't going to bother to set their preferences.
16 So that's perhaps an unfortunate situation, but we might
17 really need to get critical mass at the beginning.

18 In closing, I just want to say that if we all work
19 together, the marketing and advertisement community, the
20 privacy advocates, and the technologists, that I think we
21 have a chance to make technologies that will enhance the
22 notice and choice process. We can make an online
23 environment where people feel safe, connecting to sites that
24 they are not familiar with, or they feel safe revealing
25 private information when it's to their advantage to do so.

1 I hope this dialogue continues and I am pretty
2 optimistic about where it's heading. Thanks.

3 MR. MEDINE: Thank you, Paul, and thank you for a
4 very exciting demonstration of the possibilities for
5 consumers in the area of notice and choice and controlling
6 their privacy.

7 A question I would like to pose to the panel very
8 pointedly is have we just seen a solution to the problem?
9 Is this a solution that's cost-effective? Is this a
10 solution that marketers would like to adopt? Is this a
11 solution that privacy advocates think solve the problem?

12 I will start with Pierce Reid.

13 MR. REID: Thank you very much for the
14 crystallization and I think they are starting to really put
15 these issues in focus.

16 Now, as I started to look at where to take a
17 discussion today, looked back and looked at a piece from the
18 Direct Marketing Association that says that the survival of
19 direct marketing, and I will also add the Information Agency
20 to that, has always been based on consumer confidence. Now,
21 we have to work to maintain that consumer confidence through
22 the combined efforts of industry, of industry advocacy
23 groups like the DMA and the ISA, of consumers as laid out by
24 customers and as represented by the consumer advocacy groups
25 we see represented today, by Internet groups shepherding the

1 future of these technologies, such as the W3C, and of
2 government.

3 Now, I breakdown the issue today in several
4 directions. The first, we touched on a little bit in the
5 beginning, and that is self-regulatory efforts. That should
6 be back stops, and that should be combined with
7 technological solutions that we are focusing on in this
8 panel. And there is also the issue of outside regulation
9 if, and hopefully if, all of the other methods start to
10 breakdown or fail.

11 Now, these sorts of things to maintain consumer
12 confidence, as I said, are a cooperative effort. When I
13 look to make an analogy to bring technology solutions into
14 these areas, I make an analogy between that age-old race of
15 armor versus warhead. It's probably more familiar to the
16 people at the pentagon across the river, but this is the
17 fact that armor will get thicker, the warheads will get
18 larger; therefore, the armor will get thicker. And it's a
19 constant, constant cycle.

20 The efforts we make today to protect consumer
21 privacy and to address consumer confidence has to follow
22 much the same -- much the same precept for technological
23 solutions are very, very important, but there should also be
24 back stops to that, and those involve the self-regulatory
25 efforts of the industry.

1 To touch quickly on some of the self-regulatory
2 solutions that we see as the first step to address some of
3 things, are industry guidelines, and I will mention
4 something Marc Rotenberg said in the first panel about
5 creating information practices that were fair to consumers.

6 The Direct Marketing Association has for many
7 years had their fair information practices manual that is
8 intended to do just that, and in fact they are working and I
9 am working on a committee to expand that into the new media
10 as defined by everything from the Internet to CD ROMs and
11 other interactive, media.

12 There is also the element of education of
13 consumers and users of these technologies, and that's a
14 wonderful place for cooperation between government, between
15 industry and addressing its customers with the media who are
16 represented today, and, again, the consumer advocacy groups
17 that want to be a voice for their consumers.

18 That should be backed up by the technology. We
19 have seen today, for example, some blocking tools, things
20 that are client-based that people can put on their computers
21 that will block out access to certain sites. That carried
22 on will work under certain situations. That can be combined
23 with targeting tools, things that consumers can sign up for
24 and say, I would like information on this subject but

1 nothing else, and thus give marketers a pathway to provide
2 that kind of information to people.

3 It includes opt out lists, which have been a
4 cornerstone of the Direct Marketing Association's efforts to
5 protect consumers with the telephone opt out list and the
6 mail list. I believe it's the Telephone Preference Service
7 and the Mail Preference Service. Those can be expanded into
8 the online interactive world.

9 It can include identifiers that identify
10 solicitations such as X-headers, so that people can again
11 block out information they don't want to receive. And it
12 will involve things that we haven't even dreamed of. I am
13 fairly new to cookies and crypto, and that's one of many
14 things that will evolve, along with the Internet and the new
15 media.

16 Now, self-regulation is about effective change. I
17 think it would be quite successful in doing that. And I
18 would also say that the response of the consumer
19 organizations and industry organizations are not out about
20 protecting the companies who want to make inappropriate use
21 of this.

22 Now, self-regulation has worked in the past. It
23 still applies to the new media. It's faster. It's more
24 market-driven, and though we should look at what kind of
25 regulatory solutions there are, we have got to avoid a

1 shoot-then-point approach, and that's one of the reasons we
2 have got to apply the effort today of government and other
3 groups to educate themselves on this issue, and we are
4 starting to take an approach that educates people here.

5 I would like to make one last point. It's been
6 touched on here today, and that's that the Internet is
7 evolving. We have barely begun to imagine its potential and
8 it has barely begun to scratch the surface of the potential
9 market that these technologies can reach out to.

10 But before it can achieve its potential, it's
11 going to require investment, and a lot of that investment is
12 going to come from the private sector, from groups, from
13 companies, from industries that are looking for some element
14 of return on their investment.

15 Now, this investment is what's going to move the
16 technology from the lab into the living room. It is what's
17 going to take the Internet from the few informed haves who
18 have got it today, and make it available to the general
19 population.

20 The evolution we have got to work on has got to
21 make sure that we strike a balance between the need for
22 privacy and between the needs of those people who will
23 invest in the futures of these technologies and bring these
24 fabulous new worlds to our population and every American.

1 I state again as a conclusion that this evolution
2 is going to be reached with a cooperative effort. We have
3 seen that today, and I hope this is the first of many steps
4 and not the last step or the beginning of an end solution.

5 Again, I complement the FTC and thank you for
6 having us.

7 MR. MEDINE: Thank you.

8 I am going to encourage you to give briefer
9 remarks because we have a lot of panel members, and I would
10 like to also hear more specific comments. I will turn to
11 others, but I would like to hear people say specifically,
12 for instance, should fair information practices incorporate
13 this technology as part of -- as opposed to general
14 statements about what ought to be done; either it can be a
15 commitment to specific solutions or an opinion.

16 Dan.

17 MR. WEITZNER: Thank you, David.

18 I am Dan Weitzner for the Center for Democracy and
19 Technology, and you can see what happened to me. I have
20 been working on first amendments issues for the last year
21 and I got past the gray stage.

22 (Laughter.)

23 I want to try to answer your question, David, that
24 is this the solution. And I guess I want to make more of a

1 process comment than anything else, and get back where Al
2 Veza left off.

3 That less than a year ago the technology that Paul
4 Resnick showed was even before vapor-ware. It didn't exist.
5 It wasn't even a thought in anyone's mind. No one even had
6 thought of it enough to announce it as vapor-ware. That
7 happened along the way. But I think that it is important
8 that when faced with a real hard issue the Internet
9 community, and by that I include all the technology
10 companies, the content companies, and users, got together to
11 figure out how to address the problem.

12 And I think, with Al's disclaimer that nothing is
13 perfect, we have a real concrete way to address the issue of
14 what to do about inappropriate material for kids.

15 I think that we are in a similar position today on
16 the privacy area. I saw some of Senator Exon's staff, I
17 don't think that they are here anymore. I always thought we
18 should put them as, you know, chair for PICS or something.
19 But I think that we do have an extraordinary opportunity
20 because as everyone has said, if there is one thing that
21 everyone on this panel has in common, this is a new medium,
22 it's an evolving medium, and it's an incredibly flexible
23 medium. And the way in which it evolves is not just a
24 matter of speculation or a matter of hoping it comes out

1 right. It's a matter of people who were involved in getting
2 together and decide what to do.

3 Marc Rotenberg said this, a number of other people
4 said this; that we are at the very beginning of this
5 process, and we should decide how we want it to come out and
6 make it happen. I think we saw with the PICS experience
7 that we have some model for doing that. And I would say
8 that for the rather large amount of collection of personal
9 information that goes on in people's daily browsing
10 activities, we have got the seeds of a real tool to address
11 the problem, and we should all be working together and make
12 this happen, so that we can come back in a year and see
13 something up on the screen that's not just a laid out mock-
14 up from Mr. Resnick.

15 Thank you

16 MR. EK: My name is Brian Ek, and I am Vice
17 President of Government Affairs for Prodigy. I am also here
18 representing the ISA, and I am policy co-chair of the PICS
19 effort, so I am shameless PICS-rooter.

20 I would just like to crystallize some of the real
21 tangible benefits that this option offers. David, you
22 mentioned before whether this would work for direct
23 marketers, whether this would work for privacy groups. And
24 the bottom line is, because of how PICS is constructed, the
25 beauty of it is it works for everyone, because PICS is not

1 reliant upon self-rating by web sites. It can be -- it is
2 very simply what PICS is, is it allows the creation of
3 identifying labels.

4 Now, those labels could specify the amount of
5 nudity on a page. They could specify the privacy practices
6 that a particular web site operations under. Those labels
7 can be created voluntarily by the web site operator. They
8 could also be created by a third party, whether it's the
9 Privacy Journal or someone else. Those labels could be
10 distributed in a variety of ways. Could be CD ROM, could be
11 on a server, could be on floppy disks.

12 So consequently what would happen is when a
13 consumer asks to see a web site, if the web site operator
14 has not identified the site according to its privacy
15 practices as that site comes down into the computer,
16 whatever rating system the consumer uses could then
17 superimpose that system or that label and attach it to the
18 site, and then the label reading software could determine
19 whether or not to allow it.

20 Another benefit is that PICS is global in reach,
21 and I think that one of the things we need to consider very
22 carefully when we look at rulemaking in this country is that
23 we may be looking at adapting a national solution to an
24 global issue. And PICS has the capability of addressing
25 this on a global scale.

1 Another benefit is ultimately it's customizable in
2 various number of forums. I am struck by the fact that the
3 current privacy practices that are in use on the Web right
4 now by the commercial online services are far more
5 restrictive than what PICS offers.

6 The fact of the matter is approximately 50 percent
7 of all Web access is coming out through the Internet through
8 commercial online services. What a lot of people don't know
9 is that when you go out into the Internet through a
10 commercial service, you go through a proxy server which
11 strips out almost all personally identifiable information
12 about you.

13 That is something that worked for us at the time
14 when we first began offering Internet access. It may be an
15 overly restricted measure and often things like PICS may be
16 more friendly both to the consumer and to direct marketers.

17 Also, I think it's clear the technology can always
18 move faster than government. This group, the PICS group,
19 was convened in August of 1995. The standards were up on
20 the Web for all to see last month. By the end of the
21 summer, early fall, you will have the label reading
22 capacity, the label reading piece of the PICS software in
23 place on all of the major online services, all of the major
24 web browsers, and you will have at least four rating
25 services. Now, these are all focused on indecent content,

1 but you will have at least four available to the general
2 public and two of them are free.

3 So the point here is that technology can move much
4 faster than government. It is ultimately very, very
5 flexible on how it gets implemented. It is truly a global
6 solution, and I think that as we look forward in terms of
7 what to do a technology solution like PICS is something that
8 we need to look at very carefully.

9 Thanks.

10 MR. MEDINE: Marc.

11 MR. ROTENBERG: Well, let me say, first of all, we
12 have no financial relationship or otherwise with PICS. I
13 think it's a neat technology, and clearly it provides some
14 tools to users of the Internet to allow them to in some
15 setting customize the type of information they receive and
16 to receive more information about the practices of
17 organizations that offer services on Internet. I think, you
18 know, this is a wonderful development and certainly should
19 be encouraged.

20 But, and there really is a but here, because
21 Shirley Sarna, who was sitting next to me on the last panel,
22 reminded us of those blinking 12s on the VCR players. And I
23 have to ask myself with a VCR, with a simple function of
24 setting a time so the people in the house can see what time
25 is on the VCR, and people don't make that literal adjustment

1 to the technology, I wonder can we base a privacy policy on
2 a technology that requires consumers to take additional
3 steps.

4 And this is one of the big issues in privacy
5 policy, on who does the burden fall.

6 Now, if your understanding of a privacy policy is
7 simply notice and consent, which is largely how the PICS
8 analysis proceeds, these are great tools because they give
9 you information about practices and they give you the
10 opportunity to enter into an arrangement regarding those
11 practices, great tools.

12 But if your concept of privacy policy is much
13 broader and includes how organizations, who you may have no
14 relationship with, as Bob Smith reminded us, and where the
15 action is today on the Internet, companies that you never
16 interact with that have your personal information and are
17 always selling it, that they exist outside of this
18 technology, then you have no safeguard whatsoever.

19 So I think, you know, what I would say here is we
20 have the beginning of a good partial solution, but the short
21 answer to David's question is no. I mean, this doesn't
22 solve the problem. It gives us a flavor for the type of
23 solutions that might come about.

24 MR. MEDINE: Commissioner Varney.

1 COMMISSIONER VARNEY: Yes, I have a question to
2 ask to Marc and Bill, I think, really, when you were talking
3 about -- it seems to me there are two, at least two
4 different settings that we are talking about here, and you
5 have really clarified it.

6 When an individual is out on the Net either
7 browsing or engaging in a transaction, information about
8 them can be gleaned from wherever they are selling or doing
9 business, and maybe perhaps, and I think this is what we are
10 going to hear more about, maybe PICS works in that setting.

11 From our friends who are the privacy experts here,
12 if we pulled out that other side of the issue, those
13 merchants that are engaged in the collection and resale of
14 your personal data without your knowledge or consent from
15 this discussion, does that make a difference? If we were to
16 approach that problem differently than this problem, if we
17 acknowledge the dichotomy that we have just outlined, does
18 that -- what does that do to PICS or other technologies
19 being a possible solution for the individual who is actively
20 and affirmatively cruising to transact business on the
21 Internet?

22 MR. MEDINE: Do you want to give Marc a chance to
23 respond to that?

24 COMMISSIONER VARNEY: One or the other.

1 MR. MEDINE: Yes, why don't we gave Marc a chance
2 to respond to that. Then we will turn to Dan.

3 MR. ROTENBERG: I think that's a very important
4 point, Commissioner. I mean, I think, in fact, you have
5 taken my point and made it much clearer.

6 In those interactions online where there really is
7 an opportunity for the consumer to make an informed
8 decision, then technologies that support good information
9 and a better informed decision clearly should be supported.

10 Now, we would have questions, of course, about
11 enforcement. I mean, are people going to do what they say
12 they are doing? And we would have questions about whether
13 voluntary guidance in that area worked.

14 But I agree with you. I think on that point on
15 that interaction we are truly making some progress. And if
16 we can also hear from the government that in the area where
17 the consumer really isn't a player, but is nevertheless
18 affected by industry practice, that there is a role there,
19 you know, the pieces begin to tick.

20 MR. MEDINE: Dan.

21 MR. JAFFE: Let me say a couple of things to
22 create a background. Then try to also react to your very
23 good question.

24 I think that maybe what is not clear to everybody
25 is that there have been historic conversions in the business

1 community on this issue. That generally in the past the
2 advertising community, the agency community, the direct
3 marketing community were very separate communities. What
4 has happened here is that the whole business community has
5 come to say that privacy is a very important issue, and that
6 everyone of us has come forward with guidelines, goals,
7 statements as to the protection of privacy. In other words,
8 there is a convergence between the whole advertising
9 community and the direct marketing community because on the
10 Internet every advertiser basically becomes a direct
11 marketer in some sense. And so that's a very unusual
12 situation.

13 Right up front the whole community has said, yes,
14 there is a great concern for consumers, and, yes, they need
15 to be protected. I don't believe this is something you have
16 to have your own experience with; that we are talking about
17 something that is so technologically difficult that people
18 who can point and click will not be able to be able to
19 handle it easily. It is not going to be a situation in the
20 world where all the clocks are going 12, 12, 12.

21 This is actually going to make it a lot easier
22 than in most other areas. That you have got to go read
23 through things and then sign things, and initial things that
24 in any other area you think about that you state your
25 privacy goals.

1 What our policy statement, goal statement, which
2 is both the American Association of Advertising Agencies and
3 our statement, says that we believe that if the marketer
4 receives personal information by interactive electronic
5 communications, they ought to inform the consumer whether
6 the information will be shared with others. In other words,
7 potential list brokers.

8 We also believe that before a marketer shares this
9 personal information with others the consumer ought to be
10 offered an option to request that personal information not
11 be shared; that he will have or she will have the
12 opportunity to decide whether this information would be
13 given to third parties. Upon receiving such a request, the
14 marketer keeps his personal information confidential, and
15 does not share it.

16 And as was mentioned in the last panel, and I
17 think a very important point, is if these promises are being
18 made by a company, that's where the FTC does step in and
19 does have authority or other government agencies can step in
20 if these promises are not kept, because that's certain by a
21 false and deceptive claim if somebody is claiming that they
22 are going to be, you know, using your information one way or
23 another. So it's not a totally non-legal area.

24 So I think what we need is notice to consumers
25 that they be able to go on. We also go on and talk about

1 being able to look at what kind of information is kept and
2 whether it's accurate, to be able to change that
3 information.

4 So I think we are right at the outset, and we may
5 have to change our own policies as we become more
6 sophisticated, but we are trying to give consumers maximum
7 control over the flow of information, and at least be aware
8 of where that information is going.

9 And on the interaction you can ask, where are you
10 going to give it to, who are you going to give it to, and
11 someone at that point can say, yes or no. I mean, certainly
12 those systems can be set up.

13 COMMISSIONER VARNEY: So presumably PICS would
14 work.

15 MR. JAFFE: Presumably PICS can work. But what I
16 would say the commitment is to find systems that will work.
17 If it's not PICS, this community is committed to finding
18 systems that will empower consumers to be able to protect
19 their privacy interests. Because without this, as I said in
20 the first session, they are not going to come on to the Net.
21 It is not going to be an effective marketplace.

22 COMMISSIONER VARNEY: You said the business
23 community is committed to finding other vehicles?

24 MR. JAFFE: Our associations who --

1 COMMISSIONER VARNEY: When? When? What kind of
2 time frame? When can we come back and PICS won't be a
3 prototype? Or when is the next -- where are we in this
4 discussion?

5 MR. JAFFE: I don't think there is -- maybe there
6 is someone who will be willing to answer that question and
7 give you a deadline.

8 COMMISSIONER VARNEY: Is it six months?

9 MR. JAFFE: But we have had meetings just in the
10 last couple of weeks trying to talk about how quickly this
11 could be done, and the technologists can't tell us.

12 What we would want to be able to do is come back
13 as quickly as possible, and we don't know technologically
14 how quickly that is, but as quickly as possible. We would
15 love to be able to come back and say in three weeks we will
16 be back here to do that. I don't think that's realistic.
17 But certainly our horizons are within a year.

18 MR. MEDINE: Evan, and then Al, and then Joel.

19 MR. HENDRICKS: Well, I think Commissioner Varney
20 has asked several key questions there, and I want to answer
21 those. But first, you know, in terms that we have cited the
22 CASIE privacy -- they are called privacy goals. And I found
23 them disappointing because the first privacy goal addresses
24 educating consumers that sharing data about themselves will

1 help marketers service them more economically and
2 effectively.

3 I don't think that's a privacy goal. I think
4 that's a surveillance goal, and it doesn't comport with any
5 of the fair information practices that have evolved since
6 the early seventies when Alan Westin wrote "Privacy and
7 Freedom."

8 And the second goal states, as we heard, that
9 marketers ought to disclose their identity, but it doesn't
10 say they shall. It just says that they ought to do it. So
11 there is a lot of looseness.

12 And the third thing is they define personal
13 information as data not otherwise available via public
14 sources. And I think there is a lot of wiggle room in there
15 which doesn't provide much comfort.

16 To Commissioner Varney's question, I think that,
17 like Marc, I agree, these are very important technologies.
18 The I/PRO brings the person into the mix, PICS does, my
19 friend Ed Alburn from Colorado and Privacy, Inc., is working
20 on another sort of program. But none of these will kick in,
21 I don't think, unless we put the requirement that we have to
22 have information use based on informed consent.

23 And if you do that, establish that sort of a
24 guideline, and then these technologies will flourish because
25 we hear that Prodigy is responding very quickly to the CDA,

1 which is certainly a bad law in many ways, but now the law
2 is forcing them to respond, and to take care of this issue,
3 and I think that you will see these technologies flourish if
4 we put that simple requirement that informed consent ought
5 to be a factor here.

6 Now, the other thing here is, in terms of
7 maximizing choices, we should not forget that one of the
8 choices that has to be available is anonymity. And
9 anonymity requires the development of cryptography. And it
10 really burns me if someone who, you know, my lines go back
11 here on my mother's side, you're talking Daughters of
12 American Revolution, and on my father's side, you're talking
13 wagon train, 1843 to Oregon. I go way back in this country.
14 And I'm proud of it.

15 But we have seen our industrial policy fail, we
16 discussed yesterday, in the car industry, and in the steel
17 industry. And here we see in the New York Times Business
18 page today that now one of our leading developers of
19 cryptography is opening a subsidiary with the Japanese so
20 they can develop cryptography and then sell it back to us,
21 because of our export controls. It's ridiculous.

22 One of the most important things that come out of
23 this session and this report from the FTC is a very strong
24 recommendation that this administration has to get behind

1 cryptography and stop letting our law enforcement agencies
2 run our cryptography policy.

3 MR. MEDINE: Al.

4 MR. VEZZA: Yes. I want to set the VCR analogy
5 and put it in perspective because I think it's setting a
6 tone here that is not quite right.

7 I should mention that all four members of my
8 household know how to set the clock on the VCR. It still
9 blinks.

10 (Laughter.)

11 And the reason is, is very simple. I live in a
12 community where once a week the power fails intermittently
13 in the middle of the night for a few seconds, and we all got
14 tired of setting the clock.

15 Now, what does that say?

16 Well, I will put PICS aside. Any solution that
17 uses a computer where you build a profile, a profile will
18 stay in the computer, and you don't have to worry about it
19 again. The clock is not going to blink, and this is what my
20 point is all about. The fact of the matter is that it will
21 act in the background for you. You are not going to be
22 asked every time should I do this, should I do that.

23 It's similar to talking to a secretary or an
24 assistant and telling them what you want to be interrupted

1 for an what you don't want to be interrupted for. And I
2 think we have to put that in perspective.

3 The second thing I wanted to say about that is
4 that people say, well, the kids know a lot more than the
5 parents. My answer to that is very simple. It's a
6 generational start-up problem. It will go away, okay?

7 And, finally, I would like to answer Commissioner
8 Varney, I am not going to give you a precise answer, but I
9 will say the following. If industry gets behind something
10 like this or some other technology, and the right people are
11 involved, I think that within 10 months to a year you could
12 see the same activity in the privacy domain that we now see
13 in the rating domain.

14 MR. MEDINE: Let me call on Joel, but also pose a
15 question for future panelists. What is it going to take to
16 get industry to that point? And shouldn't industry be
17 there, and what is it going to take to get them there?

18 Joel.

19 MR. REIDENBERG: Thank you. I just wanted to come
20 to a couple of quick points. The first one is in part to
21 the question by Commissioner Varney.

22 I think PICS demonstrations with PICS is showing
23 that technical standards are policy rulemaking, and they are
24 rulemaking either by default or by design. PICS, this demo
25 was an attempt at looking at this tiny technological

1 rulemaking. And what I think is particular -- is especially
2 interesting about it is that it offers essentially a hybrid
3 kind of regulation where citizens are included directly in
4 making those policy choices.

5 In terms of some of the time table issues, as Al
6 said, the development of the technology itself, I don't
7 think is going to be the problem, the actual technology to
8 make that work. We saw how quickly the PICS concept came
9 from idea to fruition. I think it was spurred in large
10 measure by Communications Decency Act. That is sort of my
11 view as an outsider to it.

12 I think the real issues in PICS privacy will come
13 from a couple of places. One, there may be instances where
14 we decide that certain privacy interests or rights are
15 nonwaivable rights. And there we notice that the consent
16 may simply not be appropriate. We have that in instances,
17 we can see that in some cases on AIDS testing and polygraph
18 testing. We have identified particular areas where it's a
19 public policy decision.

20 The more critical problem, I think, for the time
21 table and how quickly this may get to market is going to be
22 the choice of vocabulary. PICS allows any one of an
23 infinite number of vocabularies. For the demo today we
24 chose the Canadian Standards Association for a couple of
25 reasons.

1 One, it is an existing, totally established by a
2 standards organization in Canada. It was adopted this past
3 spring. It happened to be pretty easy to instrumentalize in
4 terms of a simple rating system. The OECD code is a little
5 harder to turn into a rating system. The European Directive
6 is another step, with more difficulty.

7 There are all sorts of other kinds of codes that
8 you might want to turn into a rating system. So in getting
9 some sort of agreement like the important ones, and what the
10 exact vocabulary is is going to be one issue that's going to
11 take time to work out.

12 Getting the critical mass that Paul Resnick spoke
13 about, I think is also going to be the key to whether or not
14 this will function in the online work. Whether that
15 critical mass will arise in the absence of some form of
16 compulsion, legal compulsion, I think will be a question I
17 will defer to some of my other colleagues.

18 I think whether or not we see legal compulsion in
19 the United States, we will see it coming from abroad, and
20 the consequence for that is that we may see stimulated some
21 overseas PICS as a potential solution to problems in the
22 international context.

23 The third area that may be directly relevant for
24 you in sorting out the issues and why this affects the time
25 table is the certification process. In the demo we saw that

1 you may have self-reporting. A site may say these are -- I
2 conform to the CSA code, or I conform to another code, it's
3 self-reported. We may want a certification authority that
4 some sort of private sector entity says, yes, we have
5 audited, or, yes, we trust them and believe them.

6 In the context if it's a self-disclosure and the
7 software is configured to accept -- certain software, and it
8 turns out that's false, then you run into areas where we may
9 have powerful existing laws that can impose enforcement. It
10 can look at deceptive practices, fraud, all sorts of things
11 that the FTC is well acquainted with, as well as the State
12 Attorneys General.

13 And I guess I do want to conclude with I think
14 that there are some important opportunities, that this may
15 give rise to solving some of the global difficulties that we
16 will encounter, as I think Paul had indicated. Right now
17 this is very much in an infant stage. There are lots of
18 other issues that it won't work. But at least if this can
19 narrow down the places where we have to have it to make
20 concerns a lot more palatable.

21 MR. MEDINE: Thank you.

22 The issue of non-waivable rights or rights that
23 should be waived less easily will be the subject of our
24 discussion right after lunch.

25 Daniel?

1 MR. WEITZNER: Well, I want to say here that I
2 think that CDT is going to propose the No Blinking VCR Act
3 of 1996, because I actually think it was that very metaphor
4 that, if nothing else, led to the passage of the
5 Communications Decency Act; the sense that we have to take a
6 kind of policymaking view and presume that individuals who
7 use this medium are powerless and need protection by the
8 government.

9 I certainly do think that there are times when
10 individuals need protection by the government. And I think
11 that Commissioner Varney's delineation between the
12 interactions where there is direct contact between the
13 individual users and information collectors who run Web
14 sites on the one hand, and those who -- where there is not
15 contact is tremendously important.

16 I would suggest that today on the Internet and
17 the Worldwide Web the vast majority of practical actual
18 situations where people need privacy protection fall into
19 the first category. There may well be situations that also
20 fall into the second category and we should look at those.
21 But we shouldn't confuse those situations.

22 Marc has raised the question of burden. I think
23 that if you look at just the initial implementation of the
24 PICS specifications in the Microsoft browser, sure, that's a
25 burden and, sure, you have to go and you have to set your

1 rates and you have got to do things. But when you are using
2 the Internet you have got to do a lot of things.

3 And I think to set the standard that there should
4 be no burden on individuals really is going to lead us to
5 the wrong solution. And the reason I think it's the wrong
6 solution is because of a point that Professor Westin made:
7 that people have all kinds of different privacy preferences
8 and all kinds of different situations.

9 And we should make sure that people have the
10 ability to express those, and that people who run Worldwide
11 Web sites and do other kinds of information collection
12 activity on the Internet have easy ways to respect those
13 preferences.

14 If we get to a point where it seems that no one
15 who runs Worldwide Web sites wants to respect those
16 preferences of users, then I think we have a real issue.
17 But I don't think we are at that point. I know that in our
18 efforts to look at privacy on the Internet from a practical
19 perspective, from the perspective of someone surfing around
20 and what kind of information is collected about them, the
21 vast majority of Worldwide Web sites don't even have a
22 privacy policy. And the reason for that, I do not believe
23 it is either maliciousness or desire to collect information
24 and use it for nefarious purposes or to make a profit from
25 it.

1 It's because I don't think most people who run Web
2 sites even know that they should have a privacy policy.
3 They don't have lawyers on staff to tell them how to write
4 one. And what we should be about here is making that easy
5 to happen. I think that the Internet has been remarkably
6 good at working out ways that it can function well for
7 itself, as a community or as a set of communities. And I
8 think we should be about enabling that here, and recognizing
9 that there is going to be an enormous diversity of privacy
10 preferences and privacy desires.

11 MR. MEDINE: And the focus of our last session
12 today will be on how to get the word out to consumers and
13 businesses about these issues.

14 Bob Smith.

15 MR. SMITH: I think what we have seen PICS is a
16 form of call blocking, and it's great. It's one battle we
17 won't have to fight.

18 Does call blocking take care of all the issues,
19 dangers in the telephone system? No, not at all. It's a
20 tiny segment.

21 My fear about this discussion is that, and the
22 presentation, is that it leads us to believe that the
23 greatest danger to consumers on the Internet is getting
24 unwanted solicitation. And there are so many much greater
25 intensive problems that we have got to deal with.

1 We can't accept the direct marketing view of the
2 Internet to set our agenda. I think, for instance, of the
3 use of video on the Internet, doesn't that involve many more
4 intensive privacy concerns than the use of unwanted
5 solicitations?

6 If you view PICS as a form of call blocking,
7 that's very benign, but I just think sitting here thinking
8 it could also be viewed as a form of pre-screening, which
9 members of the FTC are very familiar with.

10 Why wouldn't a start-up company come here a year
11 from now with the Netscape cookie technology that we heard
12 about, with the PICS technology?

13 Wouldn't you then have a form of pre-screening
14 where marketers could choose not to do business with
15 companies that have -- excuse me -- with individuals who had
16 opted out of doing business with certain companies or had
17 opted out of receiving certain materials by the Internet.

18 Doesn't the very PICS selection tell something
19 about the family and its values, and the number of children
20 or the age of children in the family? And isn't this all
21 valuable information to those who would want to take the
22 technologies off of that and turn it into a pre-screening
23 device, as opposed to a call blocking device?

24 MR. WESTIN: I think Joel Reidenberg posed a very
25 important issue, which is since technology tools obviously

1 need to be informed first by policy choices, what are going
2 to be the units of analysis that we use?

3 I am troubled by quickly importing OECD standards,
4 European Union Directive standards, even Canadian Standards
5 Association's, when, as Marc Rotenberg pointed out, we have
6 a very distinctive U.S. approach, which is the fair
7 information practices approach.

8 Now, what is different?

9 Well, the OECD and the European models talk about
10 data subject that really have in mind registering big
11 mainframes, taxable slave terminals, and responsible keepers
12 as we had in the 1960s and '70s in computer technology. It
13 doesn't even begin to approximate the range of choice and
14 option and technology policy interventions that the Internet
15 makes possible.

16 I think it's much better to start off saying what
17 are the new and creating categories that we need to apply to
18 individuals on the Internet, and as Bob Smith says, not just
19 in the direct marketing area, but in all the areas in which
20 information and communication are going to flow; not just
21 for marketing but for communication, for education, for
22 citizen and government relationships that will take place on
23 the Internet.

24 I think we should be very careful not to start
25 with the European approach, and with anything which is so

1 badly out of keeping in terms of the technological realities
2 of the system. We need to rethink this, and you heard me
3 suggest I think we should start with ways of capturing
4 overall preferences that people have about how much they
5 want to reveal about themselves and not.

6 If we can think of some imaginative categories
7 that correspond to the way the survey research shows how
8 people want to reveal information, as a start. You want to
9 register yourself as an intense privacy concerned person,
10 and that will screen out perhaps technologically 90 percent
11 of what otherwise comes at you. And if you want to call
12 yourself an open American, give me everything, I'll take
13 everything you have got, then everything flows to you, and
14 in between you can set standards as to when you will reveal
15 and when you won't reveal.

16 But it just seems to me wrong to start, wrong
17 technologically to import the language that grew up in the
18 1960s and '70s in the European model as if that really helps
19 us with the new world.

20 MR. MEDINE: Just as a follow-up question on that,
21 Alan.

22 Do you see the technology that was demonstrated at
23 the beginning of the session as a model for effectuating the
24 kind of choice that you're talking about?

1 MR. WESTIN: I liked the technology. I want to
2 work hard on what the units of analysis are. For example,
3 if you say notice and consent, and if you take the European
4 model, it really drives you to an opt in model. An opt in
5 models does not comport necessarily with the click and open
6 and notice at the front end that you get in the Internet
7 world. So the medium itself is so different than the
8 database technology model of the computer of the mid-
9 computer age that it's importing one set of standards to the
10 wrong setup.

11 MS. GOLODNER: I agree with Alan.

12 MR. MEDINE: Use the microphone.

13 MS. GOLODNER: I mean, right now people do have
14 the choice of, you know, hanging up the phone or throwing
15 out the catalogues or walking out of the room when the ads
16 are on the TV, and I think they should have these same
17 options on this vehicle.

18 With regard to the option of PICS, I think, oh, we
19 must be very cautions. We have to make sure that we are not
20 relying on self-rating; that there in fact be a third party.
21 That third party has to be recognized by consumers, and
22 there has to be confidence in that third party by consumers.
23 And that that third party should not be working alone; all
24 stakeholders should be in the room, including government,

1 and not just industry. I think any third party should
2 include 50 percent consumers.

3 MR. MEDINE: Okay, thank you.

4 Marc. I'm sorry, Pierce first and then Marc.

5 MR. REID: Please, as I looked at PICS and how
6 that could be deployed into the industry and into the media,
7 I have got to look at it with a couple of different hats on.
8 One is as a representative from an online service, with a
9 large number of consumers and members who have privacy
10 concerns like any of us do. The other is, of course, as a
11 marketing professional and as someone looking for a market
12 opportunity.

13 What I see PICS doing is doing a very, very good
14 job when it comes to the issue of allowing consumers to
15 protect themselves or their children from content or from
16 information that they might either find objectionable or
17 that they don't want to visit or they don't want to have a
18 part in.

19 What I would also like to see a PICS evolving to
20 or a similar project evolving to is something that covers
21 the other side of that issue, and that is, how do we combine
22 the needs of consumers to protect their own information or
23 to release the information that they see fit out to those of
24 us in the marketing community who want to work with them.

1 At the very least, whether PICS addresses both of
2 those or just handles the consumer side, at the very least
3 what I see PICS as is an outstanding model for how these
4 sorts of things develop, and for how quickly industry and
5 companies are reacting in this environment to regulate
6 themselves and to bring solutions to consumers.

7 MR. ROTENBERG: Just a couple of quick points.
8 First of all, I think Bob Smith has possibly made the most
9 important point of the day, which is to remind us that
10 privacy issues, particularly on the Internet, are very
11 powerful consumer issues, and that the ability to find out
12 that information about individuals affects an individual's
13 ability to participate in the marketplace.

14 I am troubled, as Bob is, that a preference rating
15 service could be used to deny an individual consumer access
16 to a commercial opportunity, commercial opportunity now, not
17 everything on the Net, that another consumer might get
18 access to. I think that is a dangerous, perhaps vicious
19 spiral that could lead many people to losing privacy in the
20 commercial online world. I think we should really think
21 about what Bob said.

22 I think there is also an issue here about who is
23 being rated. I mean, it's one thing to rate a site for its
24 privacy policies and practices, and to give consumers
25 information so that they can act in a more responsible

1 fashion. It's another thing to rate the consumer. And I
2 think that would be sort of a curious reversal of how you
3 generally come to understand the use of rating systems to
4 rate and consumer choice.

5 And, finally, I would like to raise an issue about
6 the evolution of communication services, and just to pose
7 this as a question.

8 Imagine a telephone company that would say
9 tomorrow to consumers, "We're going to cut off that dime a
10 minute rate, and that lady who is always talking about dine
11 a minute phone service. We're going to give you a nickel a
12 minute phone service, and you can call anyone you want for
13 five cents a minute. We're going to keep a lot of
14 information, by the way, about your calls, and if there is
15 really good stuff on line, we might record it, but you can
16 have that phone service for a nickel. Now, if you want
17 fancy, super privacy enhanced phone service, the old
18 antiquated style where the only person who knew what you
19 were saying was the person you were talking to, that we're
20 going to charge you a quarter for."

21 Okay, now my question is, is that the direction we
22 want to be headed in, in the evolution of online services?
23 Do we want to force consumers to buy back a privacy interest
24 and a privacy expectation that we all currently today
25 understand? We get point to point telephone service with no

1 one knowing who we are talking to. We walk into a store
2 anonymously. We look at anything we want. No one finds who
3 we are. We ride the D.C. Metro service. We pay for that on
4 a cash basis. No user is identified. Obviously anonymity
5 is widespread in our society today.

6 The question is: are we going to lose this on the
7 Internet with some of these new commercial services?

8 MR. MEDINE: Your question is not hypothetical.
9 The Washington Post reported about a week ago that there is
10 an e-mail service that says if you gives us demographic
11 information, it will be free e-mail service. There are
12 trades offs.

13 Steve?

14 MR. KNIGHT: Yes, I just wanted to raise a couple
15 of questions where I see some disagreement on the panel
16 about how we could use a PICS type technology in the privacy
17 area.

18 The first of which is how are sites going to be
19 labeled in that when you are labeling content, I think as
20 Paul said in the introduction, you can look at a site and
21 for the most part be able to figure out what the content is
22 and you can have third-party labelers.

23 When you have -- when you are looking for a
24 privacy policy, that's not going to be obvious from opening
25 up a web page and looking at it.

1 So it seems that self-reporting is the more likely
2 option there, but there has been -- there has been some talk
3 on the panel about having third party raters, and I was -- I
4 just want to pose that question. Is that really a viable
5 option with this technology?

6 I'm sorry, the second related question is, if you
7 do have self-reporting, how is that -- how is the accuracy
8 of that going to be verified? And some people have talked
9 about could you audit the information that's self-reported?
10 Could you -- you know, obviously if you have a third party
11 doing it, they would be doing something to verify the
12 accuracy of it.

13 But, you know, with a million Web pages and the
14 thousands of service providers, is auditing really -- is
15 that something that speeds the process. It's going to have
16 to be more an enforcement model where you sort of spot check
17 and try to catch people and approach it that way.

18 MR. EK: I think, in response to that, that third
19 party rating is going to be essential to moving the process
20 forward in addition to self-rating.

21 Commissioner Varney raised the question earlier,
22 asking how soon could this process be put into place, and Al
23 mentioned that it could be put into place pretty quickly. I
24 think there is every incentive for the direct marketing
25 community to move forward, and that's because there is a

1 technology sitting on the Web right now which is the PICS
2 technology, which is available to anyone, including my
3 colleagues at the table, that if they so choose to create
4 their own system for rating Internet content according to
5 privacy they can do so.

6 I think that's a tremendous incentive for the
7 direct marketing community to move quickly to establish its
8 own system. But I also think that in a system of really
9 good checks and balances there should be third party systems
10 out there as well. And I think that's very, very important.

11 As far as how you would be able to determine
12 whether or not a site operator is in actuality abiding by
13 those practices, I think that there could be a combination
14 of things. I do think that there could be some kind of
15 policing activity to check. There would be Web-based
16 clearinghouses for consumers to report what they perceive as
17 violations to to look at. But I also think that as you get
18 a proliferation of rating or labeling systems out on the
19 Internet it is going to be in the marketer's best interest
20 to comply in an honest effort, because there will be a
21 variety of those rating systems out there that if you don't
22 comply and if you don't treat the consumer right, you will
23 find that those rating systems do not treat you very well
24 ultimately.

1 MR. MEDINE: Thank you. Janlori, I was going to
2 carry over right from the last panel, if you want to come to
3 a microphone so you can be heard.

4 MS. GOLDMAN: There were a couple of points that
5 were made here in the last hour that I think leave a
6 misimpression. I don't think anyone is suggesting that a
7 PICS-like solution is a total solution. But I think we are
8 in a circumstance right now where it doesn't offer an
9 additional burden on individuals. It's exactly the
10 opposite.

11 What it does is it offers individuals the
12 opportunity to be empowered through the technology, to set
13 at the user end their privacy preference maybe once. Maybe
14 the first time that they ever walk on they set their privacy
15 preference. You can set it high, you can set it low, or you
16 can set it in between, you can set it with variations. And
17 you never have to look at it again.

18 And then a decision is made before you log onto a
19 site as to whether your privacy preference is matched by
20 that site's information and practice.

21 So as Bob Smith was saying, it's exactly the
22 opposite of the site pre-screening the individual. The
23 individual is pre-screening the site. The site never
24 collects any information unless there is a match of those
25 preferences.

1 Now, again, we are talking theoretical here, but
2 the possibility of alleviating the burden that we currently
3 have in an information-based world, the burden is on
4 individuals to constantly make five or six choices on a
5 case-by-case basis, and often they are not even given the
6 opportunity to make those choices. In most instances, they
7 are not.

8 The other issue, I think it's really important
9 that we listen to what is being said here by the private
10 sector. People are saying that they want to have privacy
11 practices in place. They want to have privacy policies in
12 place, and that there is competition, a competitive
13 environment in the privacy area that we have never seen
14 anywhere before. And we should take advantage of it. We
15 should hold people to their word, and we should say you want
16 to set up a competition of who is going to have the
17 strongest privacy practice, and the strongest privacy policy
18 so people will come, so people will trust your service and
19 they will have confidence that their information is going to
20 be protected, let's do it, and let's let the FTC keep an eye
21 on it and drive that process forward, and make people hold
22 to their word.

23 MR. MEDINE: Peter.

24 MR. HARTER: I have a VCR, but it does not apply.

25 (Laughter.)

1 MR. MEDINE: It's got to be a very old one.

2 MR. HARTER: Maybe.

3 MR. MEDINE: He got rid of it because of the
4 blink.

5 (Laughter.)

6 MR. HARTER: My father is an engineer and he hates
7 the blinking. He puts tape over it. But bear in mind he's
8 a computer engineer, has been programming mainframes since
9 the late sixties and works for EDS. So he's very technical,
10 but you don't use a VCR to tell time. You have a watch, you
11 have a clock on the wall. The clock on the VCR is so far
12 away from where you are sitting on your couch, you are on
13 your bed or wherever you are watching TV, that you are
14 looking at the TV and not down behind the glass with all
15 your fingerprints on it, at this little blue LCD light. I
16 guess they could put a battery into the VCR to improve it so
17 it wouldn't lose time when you have those intermittent
18 outages.

19 But I think it's ridiculous to think, and it's a
20 horribly bad analogy, but an important one to poke fun at
21 it.

22 So if you are going to use technology to
23 communicate better, which I think we are doing, and you have
24 technologies that empower people, you have to give the
25 average user a chance to be literate. If they chose not to

1 set the clock on the VCR, that's a decision, because maybe
2 they are not going to set the time to record a program and
3 do time recording. They just want to put the tape in and
4 play. So the clock is not the most easy to use
5 functionality.

6 But if you look at the Microsoft browser, Netscape
7 browser, they have a stop button, a play button, a fast
8 backwards, a forwards. It's easy to use because the VCR was
9 easy to use in other respects besides the clock.

10 Cookies are both used by Netscape and Microsoft.
11 And Microsoft supports PICS. These are all open
12 technologies that will be implemented and applications
13 expanded and diversified as consumers demand an application
14 and customization of the applications which make the medium
15 easy to use because they can control it. The user can
16 manipulate it.

17 And going back to the encryption example. I have
18 to beat upon this because of the appearance next week.

19 MR. MEDINE: Okay, let's leave encryption to a
20 brief comment because that's not our main purpose.

21 MR. HARTER: Well, if we are worried about
22 aggregating preferences, as Mr. Smith identified, there are
23 certificate providers, they are in sunny California, GTE,
24 others elsewhere, and you get a certificate, only that
25 entity knows who I am, and they are bound by the contract

1 not to divulge or resell that information. So I have to
2 tell someone about who I am. But then I get that
3 identification and I transact with people, we have
4 magazines, we transact with L.L. Bean, and they don't see a
5 problem there. They can't sell that information. They can
6 see they are kind of buying boots and shirts and things like
7 that, but it's really useless because it doesn't apply to
8 any one person. It's just a number. So think if we can use
9 public cryptography worldwide, you are going to have an
10 ability to really made some progress.

11 Thank you.

12 MR. MEDINE: Al?

13 MR. VEZZA: Yes, I would like to comment on what
14 Bob Smith said. I never envisioned, I don't think Paul did
15 or anybody involved with the PICS as just another call
16 blocking mechanism. We think it can be more than that. We
17 don't know exactly what all -- we are not experts on privacy
18 necessarily, so therefore what I am going to do here is
19 invite Bob to come talk with us and tell us what all the
20 problems are in the privacy domain so we can understand
21 whether or not the technology will meet the requirements
22 that he has in his head, or other experts, for that matter.

23 I would also like to comment on what Alan Westin
24 said. In my opening comments I said that PICS was viewpoint
25 neutral. Moving along here, I can change that to say that

1 PICS technology is policy neutral. That is to say it is not
2 meant to implement any specific policy. One had to put the
3 policy on top of it, okay.

4 And so, for instance, in the U.S. you might use a
5 U.S. policy in terms of what servers and what users might
6 put on their computers to communicate with each other. In
7 Europe, you use an EU standard, and in Canada, you would use
8 the Canadian Standards.

9 Now I would like to throw a small curve ball. I
10 can sit in my home 15 miles west of Boston and with the push
11 of a finger I can be accessing a server in France or in
12 Germany. Which policy do I use? Which policy is in force?
13 That I think is what the Commission should be worried about.

14 MR. MEDINE: Joel.

15 MR. REIDENBERG: Yeah, this point is one that I
16 wanted to make. I think it's very critical to understand
17 that the way this would work, it can certainly allow
18 multiple ratings or vocabularies, so I don't think it is
19 appropriate to say, you know, import a single standard as
20 the one to measure all sites against. That is not the way
21 it would work.

22 A more complicated issue is what happens. The
23 fact that it can support a variety of ratings, it would be
24 something like the OECD, an OECD-based rating, a Council of
25 Europe-based rating, a European directed-based rating, the

1 Canadian Standards Association-based rating, or the old
2 1970s HEW-based rating system. In fact, all of those three,
3 and I don't agree with your categorization of each of these.
4 I think all of the three share the same basic set of
5 standards. There are differences in emphasis among them,
6 which is why operational-wise how you create the actual
7 category being used becomes difficult in the sense that you
8 may have the same principle but different ways of expressing
9 it, so your technical coding won't be the same.

10 The key then becomes, and this becomes part of a
11 technology issue or a Commission issue, how do you arbitrate
12 between them.

13 There may be -- there will be ways that a service
14 provider could set up its own arbitration, mixing and
15 matching. I mean, there are all sorts of opportunities that
16 may arise. How that becomes effective and how it becomes
17 meaningful is the policy question. How would it actually
18 get implemented, that becomes, I think, probably the most
19 critical side of it.

20 Which gets to the viability of the rating and the
21 third party rating question.

22 Labels, I think, is part of it. The labels may be
23 self-identified or they may be identified by third parties.
24 There is still another level. In other of those instances
25 you may have another third party that certifies the

1 labeling, and I will give a for-instance, what we are all
2 accustomed to.

3 Accountants, we all see corporate disclosure
4 statements that have been -- the internal accounting
5 department, the treasury department of the company will
6 prepare its books, and then you have a third party
7 accountant comes in and audits the books, and confirms that,
8 yes, the books conform to the generally accepted accounting
9 principles. In some ways that's the kind of model that you
10 might see in this area.

11 You can have self-identified labels, the EPIC
12 label attached to it, and you may have some third party
13 organization with -- in this instance the cooperation of
14 whoever the originator is, some sort of cooperation that
15 says we have looked, we think that they are conforming to
16 this particular standard. So it's a way of building trust
17 in the label, and that's something that again will have to -
18 - if it's going to work, that's going to have to evolve.

19 MR. MEDINE: Thanks.

20 Ariel is next up, and I thought he might also
21 comment on Peter's comment about encryption and maybe what
22 the relationship is between an I/PRO approach and an
23 encryption approach?

24 MR. POLER: Oh, actually our system works both
25 encrypted or non-encrypted, and we are not that far from the

1 main company doing the certificates, we meet with them quite
2 often. It's a matter of performance actually. Encryption
3 is expensive from the computer side, both take more time
4 than they used to, and again we are all about choice. What
5 we are saying is if you want your information to be brought
6 encrypted, we will be able to do it. If you are willing to
7 leave it open, you can do that as well. So our information,
8 and I believe the data that information goes back and forth
9 encrypted. And I strongly support encryption.

10 Two quick things. One is somebody suggested that
11 companies like I/PRO, that PICS would really thrive with the
12 privacy regulation. I believe we are thriving without it.
13 And there are all sorts of other companies and organizations
14 that are doing similar things, and all sorts of exciting
15 things, and what we need is an open dialogue. I mean, we
16 have been talking to all sorts of organizations throughout
17 to incorporate their things, and that, I think, has been
18 working quite well.

19 But I do want to make that point, that we are
20 already doing quite well, and that consumers are
21 participating in organizations, and have participated.
22 Playboy is another site that uses the I/code system, for
23 example. And again, they are very open about their privacy.
24 They would say, here, you know, you choose if you want to
25 give us information, and they can -- on the Playboy side, if

1 you go there, you will be able to do it in your name. So,
2 you know, it's up to the participant.

3 The final thing I want to say very quickly is that
4 it seems that some people are trying to present real world,
5 like the world that is perfect world where nobody knows what
6 you are doing and it's all very private, and the inference
7 is disaster. I just want to list this, you know, how many
8 people here don't use credit cards, don't subscribe to
9 magazines, don't -- you know, pay everything with cash.
10 First off, in the real world there is so much known about
11 us, and if we think we are going to make this perfect world
12 in the Internet, the Internet reflects the real world. And
13 I think we can make it much better if we can compensate with
14 information, we give them much more choice. But if we try
15 to make a perfect world on the Internet, we won't -- we will
16 end up with nothing, because that just doesn't exist. It's
17 all a matter of trade-offs.

18 When all this pornography debate was the biggest,
19 I was in New York City, and I stopped at a newsstand, and
20 like 80 percent of the material in the newsstand was
21 pornographic. And I thought, wait a minute, this just
22 reflects the society.

23 So, yes, we want to keep an eye on what's going
24 on, but we have to be willing to make compromises.

1 MR. MEDINE: Okay, we are almost out of time. We
2 have time for three more comments.

3 Daniel, Marc and then Paul.

4 MR. WEITZNER: Well, I am never going to think of
5 my VCR the same way after today. I do think that -- I won't
6 say anything more about that. I think enough has been said.

7 I just want to address the issue that was talked
8 about, pre-screening, and whether users are going to be
9 forced to identify to others their preferences in any way or
10 their identity or anything else. And I think Al touched on
11 this. I just really want to underscore that I think one of
12 the most important things about building in user preference
13 approaches is that it keeps the control with the user. You
14 don't have to have a big interaction with the web site
15 operator. You don't have to put yourself on some list
16 somewhere that says, "I don't want to be marketed to or this
17 is my kid, she is under 18, don't sell her anything,"
18 whatever it is.

19 So I think that the importance of the user
20 empowerment approach is that it does keep the choice with
21 the individual so that we don't have big collections of
22 information about people's preferences, which I think would
23 be a very serious problem.

24 MR. ROTENBERG: I will be brief. I mean, I don't
25 disagree with you, Ariel, and I don't mean to suggest this

1 black and white distinguishment between the real world and
2 the net world. But I think it's also important to
3 understand that PICS and I/code and other technologies which
4 will come down the line will be useful for privacy issues,
5 but they are not a substitute for an enforceable code of
6 fair information practices.

7 And this point is even more important because in
8 fact anonymity or psuedo-anonymity can be a substitute for
9 an enforceable code of fair information practices precisely
10 because no personally identifiable information is collected.
11 So when I sort of urge technologies of anonymity I am
12 actually trying to avoid these very thorny issues, which
13 exist with PICS, and not for any type of malicious intent in
14 answer to your point, Danny, but simply because there are
15 problems in negotiating the disclosure of personal
16 information that create new privacy issues.

17 And one of the benefits of anonymity is that it
18 avoids that set of problems.

19 Now, the second pointed I wanted to note, which
20 might pull some of this together, is a really interesting
21 application for PICS is not, you know, outside of Boston.
22 It's going to be in the European Union. It's going to be in
23 Canada, because what you have actually done, and it's very
24 interesting matter, is automated the judgments the
25 regulators within the European Commission and within

1 Industry Canada are going to make, in trying to assess U.S.
2 companies, and whether Canadian citizens, and European
3 citizens will have their privacy rights protected as they go
4 to our country for commercial activity. And I suspect you
5 are going to have a huge market in countries where their
6 privacy rights are enforced in law.

7 And I think there is an interesting message here
8 to the FTC. These types of mechanisms to promote privacy
9 choice and privacy screen and so forth will flourish
10 precisely in countries where there is a legal mandate to
11 protect consumer privacy. And I'm sorry to use the analogy,
12 but it will be like the blinking VCR. It just takes too
13 much time. There is better stuff to do on the Net that's
14 more fun. You know, you stay as far away from your
15 preference powers as you possibly can. This is going to be
16 another one of those situations. You want privacy law to
17 make your technology work.

18 MR. RESNICK: Okay, I am not going to agree with
19 everything Marc said, but I do want to agree with the point
20 that he is bringing up, that technologies that help with
21 notice of choice are all the things that I care about, and I
22 agree that the technology I was talking about was, you know,
23 would be for notice and choice.

24 I do think it goes beyond the line blocking
25 analogy, the call blocking analogy. I mean, I think, or at

1 least I should say the challenge is to make it go beyond
2 that, to make it support things like that you find out about
3 the mismatch and then you get a choice of how to proceed.
4 You get an explanation of what the mismatch is. So it's not
5 just going to be a straight block, and that maybe we even
6 have some automated negotiation where the site gives you a
7 different version of their service, depending on what your
8 privacy preferences are.

9 So I think we do have the challenge to go beyond
10 just the blocking notion to get to the true notice of
11 choice.

12 MR. MEDINE: Thank you.

13 Just a couple quick announcements. First of all,
14 I want to thank all the panel members for very helpful and
15 stimulating discussion.

16 Second, we are going to break for an hour, and we
17 will resume at about 1:30, and talk about medical and
18 financial information, and other sensitive information. And
19 for those who are leaving, we are leaving the record of this
20 proceeding open until June 19th, if you want to submit
21 information or materials. Thank you.

22 (Whereupon, at 12:37 p.m., the workshop was recessed,
23 to reconvene at 1:30 p.m., this same day, June 4, 1996.)

24 //

25 //

1 //
2 //
3 //
4 //
5 //
6 //
7 //
8 //
9 //
10 //
11 //
12 //
13 //
14 //
15 //
16 //
17 //
18 //

1 have enough to discuss in this limited time to focus on
2 online information.

3 What we are talking about, for example, would be
4 the use of medical information where you order a
5 prescription online, which might be very revealing of your
6 medical condition, and how is that information going to be
7 used, and what authorization should be given for the use of
8 that information, or not too far in the distant future, even
9 today that you can order credit cards, or a credit report,
10 or apply for a mortgage online and reveal a wealth of
11 financial information about yourself. And the question
12 again here is how is that information to be used other than
13 for the directly intended purpose.

14 Once again, we are going to start with
15 crystallizers to help focus the discussion, and our first
16 crystallizer will be Professor Alan Westin. He is a
17 Professor of Law and Public Government at Columbia
18 University. As we heard all morning, an expert in his field
19 and an author of many books on privacy, including "Privacy
20 and Freedom," and he is also the publisher of "Privacy and
21 American Business."

22 Professor Westin.

23 MR. WESTIN: Thank you, David.

24 It's kind of fortuitous that the FTC put these two
25 topics together in one session because all the survey

1 research that's been done shows that if you ask the American
2 public from a list of 15 or 20 types of records that are
3 kept about people, the two which are always rated the most
4 sensitive on the types of information that people would be
5 most upset about if it were revealed without their knowledge
6 and consent, the two winners are always financial
7 information and medical information. It says something
8 about our society, I suppose, that financial information
9 generally edges medical information in the United States
10 just a little bit.

11 I think that the backdrop we should understand is
12 that both the communities, the financial community and the
13 medical health community, themselves are in a state of great
14 transition and flux at the moment.

15 In the medical field it's obvious that we are
16 trying to sort out what kind of a health care system we
17 have, and who runs it. We have a move toward electronic
18 information exchange quickening; a drive toward
19 computerizing the patient record, and with the imperatives
20 to control cost to deal with fraud, waste and abuse; to try
21 to do research into exciting new areas in which kinetic
22 science offers important potential for improving part, if
23 the testing and the information used is appropriate. And
24 controlling fraud and crime in the system is another
25 imperative.

1 So at the base there are churning debates today
2 about what should be the role of medical record information
3 and health information processing in the way the system is
4 run.

5 And similarly at the base, the financial community
6 is undergoing great change. There are two cultures in a
7 sense within the financial community that are jockeying for
8 primacy. One, the traditional bankers who are thinking
9 about accounts and checking and savings, and investment
10 accounts and thinking about it in traditional
11 confidentiality norms.

12 And the direct marketing culture in the banking
13 world, target marketing, focused very heavily on affiliate
14 marketing and marketing each customer more deeply, and where
15 the same traditional notions of privacy are not first and
16 foremost in the minds of direct marketers for the financial
17 services community.

18 I find it troublesome, for example, that only a
19 handful of banks have enunciated privacy policies covering
20 all of these new activities in the financial community,
21 following the models that have been set by American Express
22 and Citicorp, and suggestions that have been well
23 constructed by Visa and Master Card.

24 I think that it's not auspicious that very many of
25 the 6,000 or so issuing institutions have not developed and

1 promulgated those policies as I think they really should,
2 and it's in their interest to do.

3 I mention this because in the online world, you
4 can ask what will be the reflection there of these
5 conditions of change and of rule rewriting and of conflict
6 that lie in the base communities.

7 First, it seems to me we can ask will we just be
8 transferring to the online world the financial transactions
9 and the medical transactions that narrowed them through
10 other means, and the key issue would be one of security.
11 That is, do we think of the Internet as a transmission
12 system, a communication system. In which case, the basic
13 rules of privacy and confidentiality will attempt to be
14 reproduced but we will have to worry about whether the
15 medium is secure, and whether we have the kind of controls
16 that will enable us to have confidence that if, for example,
17 a doctor wants to communicate on the Internet with a medical
18 record being transmitted from a patient to a specialist, we
19 can assume that that is going to have the required security
20 through any number of techniques such as encryption or other
21 secure identifier mechanisms and so forth that will enable
22 us to be competent with that.

23 And I think the same thing is true when financial
24 transactions are considered. That is, if we are going to be
25 using this for paying for goods and services by a payment

1 mechanism, whether it's a card or it's a number or some
2 other technique, will we have -- can we count on secure
3 transmission and receipt.

4 On the other hand, if we think about the online
5 and Internet world as one in which we are going to be
6 offering to give people information if they give sensitive
7 information about themselves in new ways, then I think we
8 have a different set of issues. For example, one could
9 imagine that there would be an opportunity for the
10 individual to use the Internet to get a credit report at a
11 time before the individual is going to engage in a major
12 financial transaction, and to be able to sit at home, to
13 sign on with a secure identification and to get an up-to-
14 date credit report, to check to see whether it's accurate
15 and to do anything that might be legally proper to do in
16 order to make sure that the credit report is in proper shape
17 for the transaction the individual wants to engage in. And
18 one could imagine that a credit reporting agency would be
19 able to certify this for purposes of certain kinds of
20 transaction around the world for which a credit rating would
21 be used.

22 So that there are opportunities in the financial
23 area, for example, to provide a direct to consumer service
24 as opposed to the tradition of getting a credit report as
25 the customer of a consumer reporting agency.

1 And I think that suggests the kind of new ways,
2 the term was used this morning "empowering," ways that the
3 Internet could allow individuals if there is proper security
4 and identification to get information about themselves in
5 ways that are not normally used today with high convenience,
6 low cost and so forth.

7 As far as the health information, to take another
8 example, a lot of people are revealing a great deal of
9 information about themselves today in forums, chat rooms and
10 other organizational settings where persons with muscular
11 dystrophy or persons with AIDS want to chat and talk and
12 communicate about themselves and their conditions. So that
13 we have all the problems, and we discussed this morning
14 about whether individuals' presences will be trapped as they
15 attempt to use the Internet for self-revelation and
16 community purposes, which are very important to people with
17 various kinds of either medical conditions or mental health
18 conditions and so on.

19 And the most menacing of course, would be if
20 people could track not only where they were or when they
21 were there, but also what they said, the content of what is
22 said in these places.

23 This raises the question of whether those are
24 public or private, and that will have to be wrestled with.
25 One could imagine either solution. That people get warned

1 at the beginning of entering a forum that everything they
2 say there is capable of being overtaken by others and
3 recorded by others. And it's like talking on the street
4 loudly with lots of people around. That would, it seem to
5 me, inhibit peoples' readiness and capability of using the
6 mechanism, and I wouldn't want to see that as the solution.

7 At the other end, I don't think we can quite say
8 that this is an absolutely privileged and private place, so
9 we probably have to struggle for something to define in
10 between that gives some protection, but people are warned
11 that what they said can be overheard by anybody who wants to
12 join that forum, or lurk there identified and so on.

13 I suppose that the way to end my comments is just
14 say that someone earlier remarked that when you are looking
15 at the debate over decency and pornography on the Internet,
16 you have to always understand that the Internet reflects the
17 larger society, and that we shouldn't expect too much to be
18 different in the online world than what we are used to when
19 we struggle over what is access and who has access to it,
20 and the special protection of children, in settings like
21 book publication, or movies, or video tapes, and other forms
22 of expression.

23 So too, it seems to me, with financial and medical
24 records. Look first to see the struggles that we are going
25 through in the manual and bulk-line automated systems,

1 whether we are going through how new information processors
2 in financial services and health that will have a kind of
3 trustee or steward role, that in order to do research or in
4 order to do cost controls or other things, they will become
5 trusted persons to process the information on behalf of both
6 patients and customers on the one hand, and the service
7 providers on the other.

8 Any of those issues, in other words, are going to
9 come and reflect themselves in the online and Internet
10 world. And while there will be some new technologies that
11 we can attempt to put into the protection of the policies
12 once we define them, I have always found that if you want to
13 decide where you are going, look where you have been, and
14 don't expect the world to be that radically different, that
15 the solutions that you attempt to come up with are greatly
16 aided by understanding the struggles you have been through,
17 and were useful solutions that you come with so far.

18 MR. MEDINE: Thank you. Our next speaker is
19 Trudie Bushey. She is Director of Legislative Affairs for
20 TRW Information Systems.

21 And I would just like to add that Marty Abrams,
22 from TRW, has provided very valuable assistance and service
23 throughout, and unfortunately had another commitment and
24 could be here today, but fortunately for us Trudie was able
25 to be here on behalf of TRW.

1 MS. BUSHEY: Thank you, David. Yes, Marty, for
2 those of you who know Marty very well, he's our director of
3 privacy and public policy, and he chose to go on vacation to
4 the Grand Canyon, and I don't know why he's missing all the
5 fun here.

6 On behalf of TRW, I would like to share three
7 points with you today on how TRW looks at the protection of
8 the information that we have in our database.

9 As with every information industry, TRW has been
10 thinking through the issue of data security on the Internet
11 since its inception. It's not an easy task. TRW maintains
12 five databases. Each of these databases has varying degrees
13 of privacy sensitivity.

14 From most to least sensitive, they are: the
15 consumer credit information, consumer demographic
16 information, business credit information, business marketing
17 information, and real estate information, that includes
18 property descriptions and title.

19 The products that we can make and provide from
20 each database alter the sensitivity of the database itself.
21 For example, information on a small business proprietorship
22 is closer to consumer credit information than it is on big
23 business credit information. A product offering relating to
24 small business is therefore potentially more sensitive than

1 a similar product about larger business from the same
2 database.

3 Online presentations of these products must
4 therefore provide adequate protections. Notably,
5 protections relating to privacy, data security, and
6 appropriate use. Technology and markets change, and I think
7 we have seen that, because a year ago I don't think we would
8 be sitting here today talking about the Internet.

9 Technology makes the applications of information
10 possible and at lower cost. And the market pull for more
11 precise marketing of offerings creates pressure for new
12 products, applications and delivery methods.

13 Over time sensitivity resulting from these changes
14 can be expected to lessen among those consumers. Witness
15 now the widespread acceptance of pre-screened offers, the
16 pre-approved credit offers that you receive in the mail, or
17 the banking industry puts up the convenience of electronic
18 funds transfers or ATM banking, and these weren't thinkable
19 a decade or two ago.

20 Online presentation and delivery of products
21 resulting from market pressures for change must therefore
22 provide adequate protections. Again, the protections
23 related to privacy, data security and appropriate use must
24 be considered. Protection mechanisms must have the capacity
25 for responsiveness to change.

1 As new products and delivery systems emerge and
2 proliferate, there must be mechanisms that continue to
3 permit appropriate protections.

4 At TRW we use a values approach rather than a
5 rules approach to providing these protections. Values can
6 be applied flexibly while maintaining appropriate rigor.
7 The three values that we apply in maintaining our data and
8 in providing products and services are partnership, fairness
9 and balance.

10 By partnership, we mean taking the consumer, the
11 data subject into account, when we consider whether and how
12 to meet a customer's request for consumer information. By
13 fairness, we mean primarily demonstrating openness and
14 allowing the consumer to know what we do and how we do it,
15 and ensuring that our methods do not entail practices, ours
16 or our customers, that might have the appearance of
17 deception or that might cause discomfort or embarrassment to
18 the consumer.

19 By balance, we mean making the determination that
20 the benefit to the consumer from the use of our information
21 and products benefits, such as credit and purchase
22 opportunities and choices, for example, is greater than the
23 potential for harm, and such, the intrusion on privacy. If
24 harm is balanced with the benefit, we can accomplish that.

1 We happen to apply two other values as well,
2 education, by which we proactively seek to help consumers
3 understand what we do and how it affects them; and dialogue,
4 by which we proactively meet with and listen to consumer
5 voices, both directly and through consumer interest groups.

6 We expect to continue to apply these values as
7 opportunities emerge for us to provide information services
8 by what we now envision as online media, and into the future
9 as those media and modes and others not yet envisioned
10 continue to emerge and develop.

11 Thank you for the opportunity and I look forward
12 to the comments from the rest of the panel.

13 MR. MEDINE: Thank you. Our third crystallizer is
14 Janet Koehler. She is Assistant Manager for Electronic
15 Commerce at AT&T Universal Card Services. She is here today
16 representing the Smart Card Forum, which is a cross-industry
17 effort focused on the need for inter-operability standards
18 for Smart Card infrastructure in the United States. Maybe
19 she will explain what that means.

20 MS. KOEHLER: Thank you.

21 Currently, the Forum, the Smart Card forum has
22 over 70 principal members from business, including banks,
23 telecommunication providers, software companies, equipment
24 providers, et cetera. Nineteen state and federal agencies
25 are members as well. Among the Forum objectives are to

1 promote inter-operability of smart card-based applications;
2 that is, that you can use different cards on the same
3 terminal and the like. Also, to promote standards for an
4 open and evolving market, and to serve as a resource to
5 policy-making bodies and to others dealing with legal and
6 regulatory issues impacting Smart Cards, especially in the
7 areas of social responsibility and privacy.

8 The Forum has established a privacy subcommittee
9 to articulate the issues and develop a consumer information
10 protection position or principles. And Peggy Haney of
11 American Express, who is here in the audience in the last
12 row, and Susan Murdy, of Visa Corp., are co-chairs of the
13 subcommittee.

14 A Smart Card is a credit card-shaped card with a
15 chip on it. The chip contains a microprocessor and
16 functions like a computer. Why is that relevant to our
17 discussion today? Because Smart Cards are currently being
18 used both for health care applications and for financial
19 applications.

20 What can a Smart Card do that a -- pardon the
21 expression "a dumb card" can't? That is not to say what
22 will it do, just what can it do.

23 It can do more than just store data in present
24 locations on the card. It can store lots of data for
25 selects in its memory, or provide access to multiple

1 databases. It can enable the consumer to download and store
2 value on the card to make purchases. However, unlike a
3 credit card it can authenticate the transactions without you
4 have to give your name, be an anonymous transaction.

5 The Smart Card can be locked to prevent access
6 unless and until the consumer unlocks the card. A Smart
7 Card can provide hardware based encryption to greatly
8 increase security and privacy over the Internet. The Smart
9 Card can authenticate that the hardware with which it is
10 communicating is valid as well.

11 How are Smart Cards being used? How can they be
12 used?

13 A Smart Card can be used both in the physical
14 world and the virtual world. It can be used online,
15 connected to a central database, or offline with no
16 possibility to collect information in the central data base.

17 A Smart Card can enable several providers to offer
18 a common application. Stored value cards enable consumers
19 to make purchases, promote to the merchants, more like
20 paying with cash than paying with a check or credit card.
21 Or a single provider can offer multiple applications on a
22 card. Colleges offer campus cards which students use for
23 access to buildings, to take books out of the library, to
24 purchase food in the cafeteria, and much more.

1 Different technologies can be resident on the same
2 card. I saw a campus card that had a UPC mark for using the
3 library, and a magnetic stripe, a digitized picture and a
4 chip. All this was needed to interface with existing
5 infrastructures on the campus in addition to the new Smart
6 Card applications.

7 Finally, multiple providers may offer separate
8 applications on the same chip, the same chip. In fact,
9 multiple providers may likely include a credit agency
10 sharing chip space with businesses. And, again, both
11 medical and financial applications could be co-resident on
12 the chip.

13 What are the issues? I will suggest a few.

14 Who will have access to information stored on the
15 card? Will or can access be protected by technology or by
16 contracts? For example, between service providers and
17 business. What data, and, in particular, what combinations
18 of data require greater levels of protection? What balance
19 will consumers choose between providing personal information
20 in return for being able to be reimbursed if they should
21 lose their stored value card? What trade-offs will
22 consumers choose to make in permitting some of their
23 transactions to be tracked to assist in preventing fraud?
24 What will the government require as they seek to prevent
25 money laundering? How will privacy disclosures be made to

1 consumers in a multi-application Smart Card system? Who
2 will be responsible for making the disclosure? Will the
3 disclosures be the same if there are less sensitive and more
4 sensitive applications on the same card?

5 The list goes on. And, again, the Smart Card
6 Forum welcomes your input and your guidance.

7 Thank you very much.

8 MR. MEDINE: Thank you.

9 Again, I would like to focus this afternoon on
10 really two questions. One is, do we agree that there are
11 certain kinds of sensitive information that are entitled to
12 special types of protection to proceed through online? And
13 if so, what should those procedures be.

14 Is there anyone who -- Marc?

15 MR. ROTENBERG: Let me try a couple of points
16 here. Also, I wanted to actually amplify on a point that
17 Janet just made, which I think is similar to a point made
18 earlier this morning, and that is that this a technology
19 which can be shaped. We can design Smart Cards in such a
20 way so that they are user identified. We can design Smart
21 Cards as a method of transmitting electronic cash. And this
22 is really -- these decisions are open. I mean, there is
23 nothing that's preset here.

24 Now, David's question, I think the title of the
25 panel invites one obvious answer, which is not necessarily

1 the correct answer. The obvious answer could be in this
2 area of particularly sensitive information a regulation may
3 well be justified, whereas in other areas where we may
4 choose not to regulate. And there is certainly some support
5 for this view.

6 I mean, depending on how you look at the patch-
7 work quilt of the federal privacy law, we have tried to
8 attempt in some sensitive areas to regulate. In other
9 areas, we have chosen not to regulate, and I think Alan's
10 point is important as well. Medical and financial
11 information remains critical for American consumers.

12 I would like to suggest to Alan that for his next
13 survey he put on his list the privacy of children's
14 information, because I would be willing to bet that it would
15 rank as high as medical information, financial information,
16 when that question was asked.

17 But this obvious answer is not necessarily the
18 correct answer. I would like to suggest a different answer.
19 That is, information becomes more sensitive as individuals
20 have a greater interest in being able to find out what
21 others know about them. That is to say that if there is an
22 organization that has medical information about you, or has
23 financial information about you, you have a heightened
24 interest in being able to see what that information is.

1 Let me give a commonplace example. Your monthly
2 bank statement, which allows you to make choices and
3 decisions in terms of the management of your checking
4 account, is critical for you to manage your financial life
5 in the real world, and to create a regime where the bank
6 would say, well, we have some financial information about
7 you, you have a certain balance with us, and we will let you
8 know if you overdraw. You know, we will get back to you
9 about that. The system would collapse you see.

10 So actually your ability to act rationally is
11 oftentimes dependent on having access to information about
12 you that is in the possession of others. I would like to
13 suggest also that in the medical world, I don't think this
14 is a 100 percent solution to the nation's health care
15 problem, but I don't think we are hurt by any means to give
16 individuals more information about what's in their own
17 medical files about the types of concerns and problems that
18 their caregivers have identified.

19 I think, as in the financial world, people would
20 be able to act rationally on this information.

21 Now, this leads then to another point, I think,
22 about this special significance of sensitive information.
23 It reminds us that notice and consent is not adequate for
24 privacy policy. We must also ensure access. We must give
25 individuals the ability to get information about themselves

1 held by others, and this principle in fact is in our oldest
2 federal privacy law in the modern era, and I think the
3 modern area began after the publication of Alan Westin's
4 book --

5 (Laughter.)

6 -- the Fair Credit Reporting Act of 1970. It said very
7 simply that the consumer should have the right to get a copy
8 of their credit report so that other people who are making
9 judgments about them, they will be able to see if that
10 information is accurate and the people are making
11 appropriate judgments.

12 So my answer, David, is there is a temptation, I
13 am not taking it off the table, to say that when you have
14 sensitive personal information we need higher laws, we need
15 more regulation, so on and so forth, there is another very
16 important principle today here. That's the ability to get
17 access to your own information. The more sensitive, the
18 more critical that point is.

19 MR. MEDINE: Bob.

20 MR. SHERMAN: Thank you. It's getting
21 frightening. Marc and I are starting to agree on some
22 things. But a good point, to the extent that information is
23 used for the purposes that are regulated by the Fair Credit
24 Reporting Act. Then it is already regulated. And all of
25 the requirements of that act obviously should be followed.

1 I will go out on a limb and try to be directly
2 responsive to your question, David. I believe that
3 information derived from the relationship between a medical
4 provider and a patient should never, never be disclosed or
5 used for marketing purposes. I think it's off limits.

6 Now, that is not to say that a consumer can't give
7 out information voluntarily through questionnaires, through
8 compiled lists, et cetera. And in those situations I
9 believe the appropriate process should be that at the point
10 that that sensitive medical information is voluntarily
11 given, at that point the consumer should be told about the
12 potential uses and either agree or disagree with it at that
13 time.

14 Security, particularly on the Internet, is a
15 critical issue. I think Professor Westin hit it right on
16 the head. That if we try to, and I suggest that we should,
17 try to translate some of these privacy principles to the
18 Internet. The overriding issue might be will it work based
19 on security and safeguards.

20 But that is where I think we come out on medical
21 data derived from the medical provider/patient relationship,
22 it's off limits. If voluntarily given by the consumer, then
23 the notice and understanding and opportunities should be
24 given right at the point where it is provided.

1 MR. MEDINE: Let me just ask, one question is what
2 does voluntarily mean? What kinds of disclosures have to be
3 made to a consumer when they are providing medical
4 information which could be highly sensitive that could
5 reveal a medical condition that could affect their
6 insurability, their employability? Should there be a
7 different kind of disclosure than the information that you
8 buy red shirts might be sold to another marketer?

9 MR. SHERMAN: In my view, not only should it be,
10 yes, disclosures should be very specific under those
11 circumstances. But, again, those are Fair Credit Reporting
12 Act uses; namely, whether it will adversely affect credit,
13 insurance, employment.

14 And in those three areas, I mean, the Congress has
15 already seen fit to regulate, and I think we have got to
16 comply with the requirements of that Act.

17 MR. MEDINE: Does it have maybe issues like
18 electability that go beyond Fair Credit Reporting Act
19 concerns?

20 And I will open it up to more people. But I would
21 like people to address what kinds of disclosures need to be
22 made when you are dealing with - should there be heightened
23 disclosures when dealing with this kind of sensitive
24 information?

25 Bob Smith?

1 MR. SMITH: I think that the poll results reflect
2 what people perceive is information that most likely is
3 disclosed and used in the marketplace about them. I can't
4 believe that people in answering that survey didn't think
5 about sexual orientation information, for instance. Would
6 people put that on a lower scale? Or child-bearing
7 information, or even the fact that they have children, or
8 smoking or alcohol consumption. The downloading of
9 pornography, most people would say that's very sensitive. I
10 don't want that booted about the Internet.

11 For me, social security number is key, because
12 it's the key to other information about me. So I would say
13 that's extremely sensitive to me. Many people feel their
14 home address is in that category, and I feel the same way.
15 What about my digital signature? That's not really --
16 that's not going to be an intrusion of my solitude, but it
17 certainly could be a security risk to me if my digital
18 signature is in cyberspace and falls into the wrong hands
19 and is affixed to a document without any evidence of cutting
20 and pasting at all.

21 As well, my digitized photo image. Think of the
22 ways that can be altered and cut and pasted without my
23 knowledge. I think many people would respond to the survey
24 saying that's a piece of information that I don't think
25 should be in cyberspace.

1 I agree with Marc that the identity of children is
2 particularly sensitive. It is to me anyway.

3 It's interesting too that the discussion hasn't
4 mentioned the word "accuracy." I think most people would
5 respond to a survey saying I don't want inaccurate
6 information about me booted about in the electronic world.
7 And I would think that this Commission already has authority
8 to have some sort of protocol screen that the industry
9 already regulates, may not transmit information
10 electronically without going through some screen for
11 accuracy. The accuracy rate in the credit business is
12 anywhere from 20 to 33 percent. That's just really not
13 adequate for transmitting information across national
14 borders and into cyberspace.

15 We have already heard that the Internet is an
16 insecure medium. It's a multinational medium, outside the
17 range of any one particular set of laws. It is a medium
18 that you can operate on anonymously.

19 Because of all those properties, I would offer a
20 modest proposal, and say that personal information of any
21 sort may not be offered for sale on the Internet. I am not
22 saying it can't be transmitted once there is a relationship
23 established, and obviously that's already happening. But I
24 don't think personal information of any sort should be
25 offered to strangers for sale on the Internet because of

1 these anonymous characteristics of dealings on the Internet
2 and because of its multinational character.

3 When you think about what we are considering, we
4 are considering transmitting information that we already
5 concede is less than 66 percent accurate into a medium that
6 we have admitted is insecure, and that can be used by people
7 anonymously, and we are also putting it into a culture that,
8 though we haven't said so, is really dominated by a kind of
9 mischievous devil-may-care culture at this particular point.

10 I think that would be unthinkable if we think of
11 it in the those terms.

12 MR. MEDINE: Okay, Kathleen, would you also give
13 your perspective on the use of medical records.

14 MS. FRAWLEY: Kathleen Frawley, American Health
15 Information Management Association.

16 When we look at health information, there are
17 really two different issues. One of the issues involving
18 the providers and the use of online Internet versus
19 consumers. And certainly for providers, as Alan Westin
20 pointed out, there is an enormous benefits to enhance the
21 quality of care and to facilitate communication and
22 collaboration among providers. And certainly even in
23 communicating with patients, the provider's use of e-mail
24 could be very helpful in terms of establishing appointments,
25 following up with patients, potentially transmitting lab

1 results or following up in terms of complaints with
2 medication.

3 The value also again, in terms of being able to
4 transfer information from one point to another to ensure
5 continuity of care, is invaluable.

6 The problem, of course, we know is that there is a
7 tremendous concern in the provider community regarding
8 breach of confidentiality, and the potential for misuse or
9 misappropriation of that information.

10 So certainly the provider community right now is
11 very troubled in terms of the fact that, you know, there is
12 a lack of security, and the fact that many organizations do
13 not have good information security policies in place, and
14 also the tremendous concern about the use of this
15 information for commercial interest.

16 So from a variety of perspectives, most certainly
17 the information technology could have enormous benefits to
18 health care delivery systems, and there are tremendous
19 concerns.

20 From the consumer perspective, the major concern
21 our association faces on a daily basis is the fact that
22 consumers are totally unaware of what health information is
23 collected about them. Most consumers have never seen their
24 medical record. Right now you only have 28 states that even
25 allow them to access their medical records.

1 So the problem that we have in this morning's
2 discussion talking about user preference or notice and
3 consent, I may be a healthy person. I may decide to go in
4 and research information on epilepsy, not even thinking of
5 the possibility that that information could work its way to
6 my insurance carrier, and then my rates to go up.

7 Or I might decide that I wanted to join a self-
8 help or support group because I am caring for an elderly
9 parent with Alzheimer's. Again, concern that that
10 information could work its way and have an impact on my
11 insurance benefits, or more importantly, my employment
12 situation. Tremendous concerns there.

13 The problem that we have is that, the case in fact
14 is that, consumers don't have access to their information,
15 they can't make informed decisions. And many times when
16 people enter the health care delivery system that is not the
17 time you want them to make a decision about whether or not
18 their information can even be used for certain purposes.
19 And so the real problem here is that this is not the time
20 when you would be wanting to be asking people to make
21 certain decisions or certain choices. So that's extremely
22 problematic.

23 This is the area where I think that voluntarily
24 compliance is not going to work. It's an area where we
25 really will have to probably need regulation. There has got

1 to be enforcement. I mean, this situation, the impact it
2 could have on, you know, basic necessities of life, that my
3 information could be used against me can cause such problems
4 to consumers.

5 MR. MEDINE: Thanks.

6 Robert.

7 MR. MEROLD: Hi, I am Bob Merold from IMS America,
8 which is not a household word. We are the largest health
9 care information company in the world. We collect
10 information in over 70 countries. Mostly on drugs, devices
11 used in medical practices, but also more recently on
12 diseases, treatment patterns, patient outcomes, and we do
13 that not only here in America but in seven European
14 countries as well where privacy is even more restrictive.

15 My comment broadly on this topic is first, yes,
16 there should be special protections for medical records to
17 answer the question. But I think we are starting to get
18 into a discussion here about the macro-issue about medical
19 records privacy, which is far bigger than the online topic.
20 And I am happy to comment on that, and as a policy IMS's
21 position is that any records we collect need to be
22 anonymized. We do not collect any personally identifiable
23 information. And that is perfectly possible to do. It's
24 technically feasible to do. We have been doing it for 10
25 years, and there are significant public policy values from

1 the data that's collected in terms of how do you treat
2 diseases, what are their outcomes, and are we going to
3 figure out how to do medicine well at a lower cost.

4 And every large federal agency, CDC, FDA, HHS, are
5 users of our services as well as for their own collection in
6 this area.

7 So there is a big medical records privacy issue of
8 keeping medical records private except for the provider, the
9 patient and the payor.

10 Then there is a separate issue of the online
11 environment. And I think here it's very clear that there
12 need to be special security precautions. To the issue of,
13 you know, if I order a prescription online, if another party
14 is able to detect that, chalk that, what have you, there is
15 an invasion that needs protection.

16 Once that prescription reaches the mail order
17 pharmacy or whatever, it's no different than a prescription
18 coming through any other medium, and there are issues with
19 that, privacy issues with that, but I think they should be
20 treated in a broader medical records context and not in the
21 context of an online environment issue.

22 MR. MEDINE: Bob.

23 MR. SHERMAN: Sure. Just to address the other
24 issue on the table, which is financial. The greatest
25 difficulty I am having is that it's an undefined term.

1 Certainly marketers need information to determine credit
2 worthiness. You would not have an economically viable
3 system if marketers could not use certain information to
4 determine whether or not to extend credit to a potential
5 customer. So I don't think we are talking about that when
6 we talk about financial information.

7 DMA has long had in its guidelines the proposition
8 that credit card numbers, account numbers, checking account
9 numbers, debit account numbers, et cetera, should not be
10 transferred without the consumer's knowledge of that. The
11 only reason that financial information, other than credit
12 worthiness, or an account number should be used is to
13 complete the transaction. We believe there is a reasonable
14 expectation, that that is what the information will be used
15 for really and nothing more.

16 And so unless there were circumstances that would
17 suggest that a reasonable expectation would be other uses of
18 that information, we think it should be so limited. But my
19 concern has -- I hope, I suggest to the other panelists that
20 if we're going to talk about financial information, that we
21 try to put some kind of a definition on it. It can't just
22 be anything that has remotely to do with money or credit.

23 MR. HENDRICKS: Well, I think that so far the
24 panel has been very excellent in being representative, but I
25 think we forgot one thing today, is that we should have had

1 a physician on this panel. And I went back to the list
2 ahead of time, and I didn't catch it either. But we're
3 talking about medical information online. And I think
4 medical information requires heightened protection, and
5 because the medical has its own tradition in this country,
6 partly because of the patient's right to privacy or
7 autonomy.

8 A patient can go into a doctor's office and the
9 doctor can recommend you need this to save your life, or you
10 need this to get better. And the patient has the right to
11 refuse treatment. That is part of our tradition, and it's
12 tied to one of the rights to privacy.

13 And I believe that same right translates into the
14 information age. That patients should have the right to
15 decide that it's not worth it for them to have this
16 information placed in insecure databases or in insecure
17 transmissions. Obviously, Kathleen has already outlined the
18 obvious benefits of being able to beam your medical
19 information in emergencies to speed treatment, et cetera.
20 Those are all situations where either the patient can
21 consent to it with informed consent, or it's an emergency
22 and the doctor says, "I have to do this to save a life," and
23 the patient is not capable of answering.

24 But this is one concept that needs to be factored
25 in to any decisions that are made about medical information.

1 MR. DAGUIO: I am Kawika Daguio. I am with the
2 American Bankers Association.

3 ABA doesn't have an industry consensus policy to
4 share with you. We are wading through the issues, and it's
5 very difficult to in fact represent an entire industry with
6 a bunch of different focuses and perspectives in one policy.
7 So we are hoping to develop some principles that might guide
8 policy development for the institutions that wish to pursue
9 that.

10 Yes, financial information especially deserves
11 special protection, but balancing the two issues and two
12 principles; protecting privacy and accountability.
13 Accountability is terribly important.

14 When people buy things online there are two
15 transactions that most people forget are occurring. One is
16 the transfer of goods and services and the other is the
17 transfer of value, the payment or payment order.

18 The account number, we would argue, belongs to a
19 financial institution, not the customer, because it's the
20 financial institution's risk that it might be used. As a
21 result of Reg E or Reg Z, where there is an unauthorized
22 transaction, the risk is on the side of the financial
23 institution.

24 There are two different levels of data or
25 information that should be addressed. One is the

1 transactional level information, personally identifiable
2 information relating to specific transactions. And no one
3 out there is selling copies of people's checks or register
4 receipts because the tradition in common law is protecting
5 customers' records through confidential treatment. The
6 information is recorded, it's there, it's available to risk
7 management, and other exercises within the financial
8 institution mode, the holding company. But it isn't
9 available to be transferred outside of that organization.

10 What we might be discussing is aggregated
11 information that might be transferrable, and other
12 information which might have to flow outside of the
13 institution, whether somebody has a tendency to bounce
14 checks, whether they have been involved in fraud in the
15 past, and whether the person, for example, is dead and their
16 account closed.

17 Management of this issue is terribly difficult
18 because no one, neither the consumer, the merchant, or the
19 financial institution has absolute rights, but the rights
20 vary according to their responsibility and the risks that
21 are presented to others.

22 MS. GOLDMAN: I know we're talking here a lot this
23 hour about theory and policy, and medical and financial data
24 travel over the Internet. But I just want to bring us one
25 moment to a little reality check in terms of the existing

1 legal regime, which is that currently there are no
2 enforceable protections on the use of medical information on
3 the federal level. And the private sector is not barred
4 anyway in terms of say personal financial data, even though
5 the government is restricted at getting access to financial
6 data.

7 There have been efforts in recent years to pass a
8 federal bill that would protect peoples' medical records
9 that incorporate a number of the principles that we are
10 talking about here at this table: access to records, a
11 consent provision that prohibits the information from being
12 disclosed without the person's permission; you know, rules
13 that would require researchers to have to go search through
14 certain procedures to use personal health information,
15 sanctions.

16 And while everyone at this table is, again, saying
17 the right thing and we are all shaking hands, there are a
18 number of private sector interests, particularly, that are
19 not interested in seeing a law or seeing a set of
20 regulations that governs medical records in this way. They
21 are not at all interested in that. In fact, they have been
22 very vociferous in their opposition to any enforceable rule,
23 because they want to use the personal medical information
24 for a variety of purposes. They want to get access and
25 believe that a consent provision or an authorization

1 provision is going to get in the way. But if people are
2 asked and have to give their permission to use the
3 information, than they won't.

4 And I think that that is a fundamental sticking
5 point. We have been at this for a couple of decades not,
6 not me personally, although it feels like it. But there are
7 people in this room who have been at it for a couple of
8 decades and it's been a very discouraging, and I think in
9 some ways a disgraceful process that we haven't been able to
10 do anything.

11 I think, you know, as Alan Westin said, to some
12 extent what happens in the offline world is a reflection of
13 what is happening on the Internet. I don't think in this
14 area that is at all an acceptable calculus. The Internet
15 should not be a medium over which personal health data
16 flows. It is not only an insecure medium, but I am not sure
17 that it is capable right now of providing appropriate
18 security. There are other mechanisms where the information
19 can flow electronically off the Internet in a closed system,
20 a system where there are fire walls and where there are
21 greater protections, but certainly not the Internet.

22 And I think any attempt to do that right now is a
23 huge mistake and we would oppose it very loudly.

24 The concern is not only that the medium is
25 insecure, but we are going to exacerbate and in some ways

1 perpetuate what are already serious vulnerabilities. The
2 information is not secure in paper form, and it can be
3 faxed. In fact, most of the horror stories that we have and
4 we rely on in terms of pushing for enforceable policy result
5 from paper records having personal information that are
6 misused. So that is where the bulk of our horror stories
7 are.

8 A number of years ago I met with some managed care
9 company who was looking at how they should put privacy rules
10 in place for how personal health information was handled,
11 and they said, well, we are sending the medical records
12 unencrypted over the Internet now, and I guess, you know,
13 you probably worry about that. And, you know, it's shocking
14 that that was happening. But there was nothing in place.
15 There was no kind of social constraint saying, well, here is
16 this story and here is why it shouldn't be happening again.
17 We tend to make public policy as a result of horror stories
18 and there hadn't been one in that instance yet.

19 MR. MEDINE: I just want to leave some time for
20 others.

21 MS. GOLDMAN: I am almost done. I am almost done.

22 MR. MEDINE: Good. Thanks.

23 MS. GOLDMAN: I think that the difference from the
24 medical area and the financial area is that in the medical
25 area the individual is not out of the equation. When it

1 comes to health, personal health information that is
2 collected or divulged, they are not part of it at all.

3 In the financial area we have seen a lot of
4 movement towards security and a lot of moving towards secure
5 systems and control because, again, the person is part of
6 that equation and they are not going to buy things if they
7 don't think that their financial data is secure. So, again,
8 I think it does involve very different equations.

9 MR. MEDINE: Thank you.

10 We have time for just a couple more speakers. We
11 have also a busy schedule this afternoon.

12 Andy Strenio?

13 MR. STRENIO: My name is Andy Strenio. I am with
14 Hunton & Williams, and I am definitely not speaking for
15 anyone with the possible exception of myself.

16 I think that the panel has done a very good job of
17 identifying a number of the very real concerns and costs
18 that could go along with improper use of medical or
19 financial information, and that's very important, and with
20 everyone else, I also am inclined to think that special
21 safeguards should be employed here. But I hope we don't
22 overlook the possible enormous benefits that can be used and
23 can be gained by the proper use of information using these
24 technologies.

1 For example, in the area of medication, and one of
2 the major problems encounter in actual practice, is the
3 number of patients who don't comply with the prescriptions
4 that they are supposed to have. You are supposed to take
5 your medication once a day, something of that sort. The use
6 of e-mails to -- as a daily reminder to a patient is
7 something that could be of great value in getting greater
8 compliance and it's something that would be in the patient's
9 interest as well as the medical community's interest in
10 security that.

11 Now, whether and how we take advantage of that
12 opportunity balancing a patient's privacy interest is the
13 question. In that particular setting, I think that we could
14 rely upon using doctors as gatekeepers of having the doctor
15 ask the patient whether she or he would be interested in
16 having the daily reminder sent electronically, and you have
17 a possibility of getting informed consent in that fashion.

18 But just as the costs are higher in this area, the
19 benefits are higher. It's a very complicated question. You
20 are going to get down the road to the question of if the
21 doctor can do this particular questioning, what about the
22 HMO if it comes from the HMO as opposed to the doctor, is
23 that all right? If the HMO is okay, what about the
24 pharmaceutical manufacturer who has an interest in the
25 efficacy of the particular prescription? And if that's all

1 right, what about having an interactive regime where the
2 patient punches a button to certify that the medication has
3 been taken, and there is some kind of reward for that, that
4 you get a dollar off on your next prescription?

5 And you can go down that road very far, and I will
6 not do that at this point. But I simply wanted to
7 complicate the discussion by saying that as we have these
8 extra safeguards, we should be very careful not to rule out
9 areas where it is clearly in the patient's interest to get
10 that information. And I have given the easy situation of
11 having a doctor as the gatekeeper where you can get informed
12 consent.

13 The question I will leave for the group is what
14 about other situations where it is either impractical or
15 impossible for the individual to have consented in advance
16 of receipt of information that he or she would consider to
17 be valuable, important, perhaps life saving. How do we
18 address that type of situation with the proper regard for
19 the patients, not only the privacy interest, but health
20 interest?

21 MR. MEDINE: Final word, Marc.

22 MR. ROTENBERG: Okay, I wanted to first make a
23 very quick comment on an interesting, what appears to be a
24 contrast in viewpoint between Mr. Merold and Kawika.

1 Mr. Merold in describing the activities of IMS
2 America underscored the importance of anonymity, and I think
3 it's fair to say that at least in part of your records
4 practices the anonymous nature of the records reduces the
5 risk of misuse of that personal information.

6 Now, Kawika has suggested in the financial world
7 there is a risk of anonymity, and that is that it reduces
8 accountability which, of course, banking and financial
9 institutions have a strong interest in.

10 And what I would like to suggest, one of the ways
11 that we create a dynamic in the private sector and this new
12 world is to encourage Kawika to look to the, you know, the
13 example from the health community and see if there is a way
14 to accomplish your goal of assuring that you receive, you
15 know, good value in exchange for service, and at the same
16 time preserve anonymity, because anonymity does serve a very
17 important role in information security and privacy.

18 And my second point, and it really should be Bob
19 Sherman's point, because I think Bob is the one who has
20 probably given the most thought to this issue, and I think
21 he suggested, David, in response to one of your questions,
22 consent plays a tricky role when you are talking about the
23 receipt of medical services in an emergency room, when you
24 are coming, you know, to a closing on a home mortgage, and
25 someone who has absolute control over your life, whether you

1 get that home, whether you get that operation, says to you
2 we need to know something about you. We need your tax
3 returns for the last three years. We need to know this and
4 that. That is not the point at which you are going to say,
5 yes, but does this follow the Canadian Standards Association
6 principles with regard to accountability. You really don't
7 have time for that judgment in these situations.

8 And there are good reasons in a lot of these cases
9 why that information should come out. There are also
10 situations perhaps when that information should not come
11 out. An employer, for example, who is about to hire you for
12 a job says, "By the way, have you ever received any
13 counseling? By the way, is there anything I need to know?"
14 With regard to, you know, fill in the bank.

15 And suddenly you begin to get a sense that there
16 are information transactions and they will occur online
17 where we may need to establish some baselines, where we may
18 need to say, as we have, as Joel pointed out earlier, it is
19 not appropriate to ask people about their HIV status. It is
20 not appropriate to require a polygraph test as a condition
21 of employment. And I think we really need to think about
22 some of those five questions, because they may be situations
23 where the consumer is most at risk. They need something.
24 They are in an unequal bargaining relationship, and there

1 will be no one there on their side to say you really
2 shouldn't have to give that information out.

3 MR. MEDINE: I want to thank the panel very much.
4 I think Marc left us on just the right note, which is we
5 have a lot to think about in this area, which we will
6 continue to do.

7 We are going to take a very quick five-minute
8 break to switch over the chairs for the European Union
9 session.

10 (Whereupon, a recess was taken.)

11 MS. SCHWARTZ: The topic of this session is the
12 impact of the European Union's Directive on the protection
13 of personal data. Now, this is a subject that has been
14 coming up off and on throughout the day, and David has told
15 you that we can talk about it later, so now is the
16 opportunity.

17 The format that we have used up till this time, we
18 are going to start off with some presenters, crystallizers.
19 The first crystallizer is Joel Reidenberg, Associate
20 Professor at Fordham University School of Law, where he
21 teaches a seminar on information technology law, and global
22 networks, and he has written widely on this field.

23 So I will turn it over to Joel who is going to
24 speak from the podium.

1 MR. REIDENBERG: I guess I would like to start by
2 commending the Commission for including this topic, which is
3 quite different from the United States. Here in the U.S. we
4 have heard already a discussion on some of our rights, self-
5 regulation, the importance of practices, what's happening in
6 the marketplace. -- what the regulate looks at a wide range
7 of confirmation practice activities. Thirteen of the 15
8 European Union countries -- some of the things we tend to
9 connotate with privacy in the United States, confidentiality
10 concept traditionally spoken for the U.S. -- because faced
11 with the situation -- the Directive went from draft --
12 changes were taken place in the union. The master came into
13 effect -- in the context of free flows and free movements of
14 information.

15 The Directive itself in its final form is designed
16 to elaborate principles, and not to be technology specific
17 or system specific. It was designed to set the framework,
18 referred to as the framework directive. There are separate
19 specific directives that are at least in the works. There
20 is one in ISDM that is still -- I understand it's supposed
21 to have a common position come out some time this month, So
22 it is expected that there will be more specific directives
23 targeted at particular applications.

24 The framework directive contains a set of
25 substantive rights. And most of these are -- the core is

1 contained in Article 6. They require that the member states
2 of the European Union enact national laws that include
3 principles of fair and lawful collection of personal
4 information, personal information which only should be
5 collected for specified purposes. It should only be used
6 for purposes -- for compatible uses to those specified
7 purposes. It requires limitations on the collection of
8 extraneous data, durational limits. You shouldn't keep data
9 longer than you need it for the specified purpose. There
10 are accuracy provisions in that individuals must be given
11 rights of access to personal information that's being given,
12 and rights to correct -- have that information corrected
13 when errors exist.

14 A critical element in the European Directive is
15 transparency. Citizens ought to be able to -- they should
16 be given notice, have a right to participate in decisions as
17 to when and how information will be used -- how information
18 about them will be used.

19 Sensitive data is to be treated with special
20 protections. Sensitive data being things like race,
21 religion, health, sexual preferences, that is to be given
22 special protection.

23 The Directive includes enforcement mechanisms.
24 Member states have to enact laws that provide remedies to
25 individuals. Member states need to have supervisory

1 authority, data protection agencies. And certain data
2 processing activities will have to be reported to the data
3 protection authority.

4 For perhaps our greatest concern today is the
5 Article 25 provisions, which mandate that European member
6 states prohibit transfers of personal information to
7 destinations that do not have adequate privacy protection.
8 If the destination has insufficient privacy protection, data
9 flows are supposed to be restricted.

10 Article 25 doesn't really establish very clear
11 methodology or answers to what constitutes adequate. That
12 is left vague for the moment, and we will be hearing a
13 little more about that later.

14 If the destination country does not have adequate
15 privacy so that it fails to satisfy Article 25, there is
16 another provision in the directive, Article 26, which allows
17 for the data flow anyway if additional measures are taken;
18 if there is a contractual measure, if the individual
19 concerned consents, if there is some other mechanism that
20 may take place. So that there is -- the general rule is
21 that if there is unsatisfactory privacy, the information
22 should be blocked subject to circumstances which can qualify
23 for one of the exceptions.

24 At the moment the directive also creates something
25 called the working party, which is a group of commissioners

1 from each of the supervisory authorities in the member
2 states, which are the data privacy commissioners. And they
3 are to assist the Commission in determining countries that
4 have inadequate protection or destinations or uses in
5 foreign sites that are inadequately protected, as well as
6 assist in developing some formal methodology for criteria
7 for adequacy, determining what adequacy was.

8 So this is the backdrop for what is happening in
9 Europe today. And these laws, the Directive is to be
10 implemented in the next three years in the member states.
11 But again, 12 of the 15 member states -- 13 of the member
12 states already have laws. The Directive will require in
13 some cases changes, in other cases, perhaps not. Certainly
14 the two member states will have to adopt laws sometime in
15 the next three years.

16 With that, I will turn it back.

17 MS. SCHWARTZ: Next, we will hear from Gary
18 Friend, who is Vice President of Government Relations and
19 Marketing at Dunn & Bradstreet. He is going to -- Gary,
20 okay, he has got a demonstration, as well as a talk about
21 the impacts of this Directive.

22 MR. FRIEND: Okay, can everybody hear me all
23 right?

24 You said liven it up, so we will bring a little
25 multimedia in to spark things up.

1 Thank you for the introduction, and as did Joel, I
2 commend the Federal Trade Commission for convening what I
3 understand is a sell out, sell out crowd, and I understand
4 the overflow room has overflowed, which -- the lady doth
5 protest -- I think it speaks to the importance of the topic
6 and the timeliness of it.

7 Joel provided some landscape of the European
8 Directive. What I am going to try to do in just a few
9 minutes is to present one company's perspective of how we
10 see it affecting what we do, and perhaps that will translate
11 into how you may see it affecting your businesses, how it
12 affects the role for government.

13 And let me try to -- I don't know if these are
14 controversial/noncontroversial, but make three opening
15 points.

16 One, an adequacy requirement is not new, and I
17 will explain in a little bit how, but it's an issue that is
18 probably over 20 years old, and so that's point one.

19 Point two is that we see this as a global issue.
20 It is not a European Union/United States issue, but data
21 protection is a global issue, and most important from our
22 standpoint data protection is good business practice. If
23 someone says to me is it good for your company, I would say
24 emphatically yes, and I will explain a little bit as to how.

1 I guess the question that keeps being asked is
2 when does the spigot get turned off. Is it going to go from
3 a solid line to just drips? Is it going to be a steady
4 dribble? In our perspective, perhaps the spigot won't be
5 turned off at all, and I will show you why.

6 Let's look at just one of our companies, Dun &
7 Bradstreet Information Services, who are in 39 countries
8 outside the United States, dating back as far as 1857. And
9 in those 39 countries 27 have some form of data protection
10 laws in place now; many of which have transported data flow
11 restrictions, requiring either equivalency, adequacy as in
12 contractual measures. So this is not a new issue.

13 In terms of what is the underlying issue in data
14 protection, Joel talked about the context of data protection
15 versus privacy. The underlying issue is balancing human
16 rights issues versus societal needs for really creating a
17 framework of protection for an information society.

18 The global information of Dun & Bradstreet, Bob
19 Merold talked about one of our current companies, IMS in the
20 health care area. I am just going to talk specifically
21 about one, and that's in the business information area.

22 We capture information on over 40 million business
23 establishments worldwide, and it includes everything from
24 corporations to sole proprietorships, information about who
25 the principals are from the directors, the owners, the

1 business characteristics and some information about the
2 business performance. But one important point, just so that
3 there is clarity, we are not in the business of capturing
4 consumer information or doing consumer credit reporting.
5 It's business information, and that's a very, very important
6 distinction.

7 In terms of what our practices are, what do we do
8 in our handling of information? Just as an opening point,
9 everything you see we do voluntarily. We don't do it
10 because the United States, that there are laws that say we
11 have to. We do everything that you are seeing voluntarily.

12 One is notification about a business report. We
13 tell the business principal when a report is created about
14 them, or when there is a full update to the report involving
15 information that the business provided to us.

16 Second is that there is an access and correction
17 procedure. Third, there is an ability to stop marketing
18 use. Where our information may be used, it's captured for
19 the purposes of business credit purposes. If a business
20 does not want their information also disclosed to a
21 marketing list, the business to business marketing list,
22 there is a very comprehensive process for taking their names
23 off.

24 And then, finally, in our environment we have a
25 contractual commitment with customers. The contractual

1 commitment limits uses, it limits who uses, but most
2 importantly, and this is something I would underscore, is
3 that in our agreement makes reference to obligations on the
4 user with respect to both U.S. and foreign laws, and that's
5 an important point, and I think Joel will cover some
6 additional aspects of this as far as U.S. practices in
7 compliance with third country laws.

8 Who gets trained? It's really everybody. There
9 is comprehensive training for the people who collect the
10 information. There is training for the people who handle it
11 and data entry. There is training for the people who sell
12 it, and then there is training for the people who actually
13 use it. And just as a prop, this is the documentation that
14 covers those four segments. This is not just blank paper.
15 I didn't grab a stack of -- but if somebody wants to look
16 through this, I can't let you have it because of its
17 sensitivity, but this is how comprehensive what you see is.

18 There is also one other constituent that we train
19 and that is our shareholders. In our annual report we have
20 a statement on our business ethics, but also at the bottom
21 on data privacy, and it specifically tells our shareholders
22 how we are spending their money on issues involving the use
23 of security and information accuracy.

24 So why do it? And I made the point if nobody is
25 telling us to do this. We do it because in our judgment

1 it's good business and it's a necessary business. We live
2 in an environment of a very voluntary system. The
3 information that is provided to us is provided voluntarily,
4 and it is dependent upon the confidence and trust of the
5 data providers.

6 Data quality, a point about getting it right
7 first, and why accuracy is important, and accuracy is best
8 measured in terms of the data collection.

9 And then finally, in our judgment, good practice
10 equals good continued cooperation. Somebody once said we
11 could probably increase our customer base by 50 percent and
12 reduce our information base by 66 percent, if we were
13 selling information to people that our data subjects didn't
14 want us to sell it to.

15 And also an important point is to anticipate what
16 is ahead, because ultimately with the EU Directive the laws
17 would be determined by the laws of what we call the
18 controller, meaning the German -- each country will
19 implement national laws, as Joel said, and therefore it will
20 ultimately be the German law that dictates transported data
21 flow issues between Germany and, for example, the United
22 States.

23 I guess the final point I would just make as a
24 parting thought is it's the right thing to do.

25 Thank you.

1 MS. SCHWARTZ: Thank you. We are going to invite
2 Joel back to the microphone.

3 MR. REIDENBERG: Okay, I think I will do it from
4 over here this time. It's a little easier.

5 MS. SCHWARTZ: Fine.

6 MR. REIDENBERG: What I am going to do now is
7 address more specifically the U.S./European Union
8 comparisons. I think Gary's presentation is a good
9 illustration, certain background of how we can look at
10 comparisons between what happens in the United States and
11 the European Directive, which is the mandate.

12 Whether we like it or not, the Directive and
13 existing member state law will force scrutiny and
14 comparison, scrutiny of what's happening in the United
15 States and comparisons with the European standards. I think
16 that the Commission is certainly actively engaged in making
17 and thinking about evaluations and anticipating making
18 evaluations in the future.

19 A colleague, Professor Paul Schwartz, and I did a
20 study over a period of several years for the European
21 Commission that we concluded last year, looking at the
22 comparison between European Union principles and data
23 protection, and United States law and practice. I should
24 say our study, fortunately, will be publicly available
25 starting I guess at the end of next month. The commission

1 has authorized the Michie Company to publish it in the
2 United States. So that will be out.

3 But that's not the only aspect. The Commission is
4 getting information about what will be happening, not just
5 in the U.S., but abroad. They have an ongoing study right
6 now looking at the methodology for determining adequacy.
7 It's expected to be completed, I think, some time in the
8 fall. They are about to start a study on interactive
9 services and online privacy. They just closed a bidding
10 process for that several days ago.

11 The working party of the member state
12 commissioners has now, they have now had two meetings, and
13 they too are preparing their thoughts on criteria for
14 evaluating foreign countries.

15 And I guess I should point out in terms of how the
16 U.S. fits into this, at their very first meeting back in
17 January, Professor Schwartz and I were asked to come and
18 discuss our study with them. So they were particularly
19 interested in information about what's happening in the
20 United States.

21 In looking at the U.S. particularly, I'll focus on
22 the private sector, which is the area that I worked on for
23 the study. One of the conclusions or arguments that we made
24 is that context is critical when you are trying to determine
25 whether or not you have adequate data protection in the U.S.

1 I think if you ask the question is there adequate
2 U.S. law under the European standards, the answer there is
3 no. Is there adequate data protection in the United States?
4 I think the answer there is maybe. And the reason that I
5 say that it's maybe is what we find is our targeted rights.
6 We have targeted rights. But implementation then becomes
7 critical to figuring out whether or not we match up. And we
8 find in the private sector cases where -- we saw some
9 examples of what one global company is doing. They are
10 operating with global privacy principles that conform to the
11 various laws in the countries in which they operate. And
12 you can find examples of companies with excellent practices,
13 and you can equally find examples of companies with the
14 poorest practices. So you have an inconsistency that is in
15 part generated from the fact that we have very targeted
16 narrow rights, and we have to rely on what companies are
17 actually doing.

18 I think that there are some particular problems
19 that this raises that I think will come to bear in the
20 international arena for U.S. companies; namely, transparency
21 is difficult in the United States. It's very hard for
22 citizens to find out and learn about what is happening to
23 their personal information. And this is especially true now
24 in the online world.

1 Secondary use of personal information, is the
2 information being used for purposes that are compatible with
3 those that caused the collection. And I think this has been
4 historically particularly problematic for marketing uses in
5 the U.S.

6 And then the third area that I think will come up
7 is the enforcement area. The European standards are very
8 keen on enforcement and supervision; that there be oversight
9 and independent supervision, and that's something that is
10 very hard to find and replicate generically in the United
11 States. We can always point to specific areas where we do
12 find it, we do see specific instances particular enforcement
13 powers. But overall we can also point to plenty of areas
14 where we don't.

15 I think that this suggests two global consequences
16 for us. One is in the absence of U.S. laws, and the second
17 area is in the absence of a data protection office in the
18 United States, in the U.S. Government.

19 In terms of law, the absence of a U.S. law, I
20 think, will mean that consumers will have higher levels of
21 data protection consistently abroad. So if an American is
22 surfing on the Web in a foreign site, in the U.K., in
23 Germany or in France, what happens to the click stream if it
24 is resident on the foreign site will be more consistently

1 matched with information practices than what would happen in
2 the United States.

3 There will be, I think, as a result of that,
4 transaction costs for dealing with privacy in the U.S.
5 Therefore, U.S. companies, there would be increasing
6 scrutiny of U.S. information processing, because in the
7 absence of a law, for a foreign regulatory body to determine
8 whether or not there was adequate data protection in the
9 United States they need to know what the specific company is
10 actually doing. It won't be sufficient to just have a code
11 of conduct or a trade association statement of policy. What
12 will be important is what is actually taking place.

13 And I think similarly, it will be harder to have
14 effective data protection enforcement. That is something
15 that will become increasingly important.

16 The global consequences for the absence of the
17 data protection office, in this sense I don't mean one
18 exactly like the European office, the European or British
19 Data Protection Registrar, or one of the counterparts in
20 Europe. I think there are some things we could learn from
21 that positively, and there are some things we could
22 certainly learn from those agencies negatively that we would
23 certainly not want to replicate here in the United States.

24 But the consequences of nothing at all, no
25 essential policy clearinghouse or policy-making apparatus

1 within the U.S. government places, I think, a very important
2 burden on U.S. businesses, and I can point to recent
3 examples of American companies doing business overseas where
4 they have found that they have had to go and persuade data
5 protection authorities that protections were fine,
6 enforcement was fine for the activities they were doing.
7 And they face skeptical regulators, because the regulators
8 have no U.S. government counterpart to point to.

9 The second consequence is that foreign data
10 protection agencies will be setting the global policy agenda
11 in the absence of a powerful U.S. voice. Presently, the
12 foreign data protection commissioners get together several
13 times a year. They have an annual conference where they all
14 get together. This coming year it's being hosted in Canada.
15 There are several subconferences. There is a conference of
16 the data protection commissioners looking at documentation
17 issues organized by the Berlin privacy commission. There is
18 a new subconference of data protection commissioners looking
19 at multimedia interactive services hosted by the French data
20 privacy commission. And there is no U.S. voice at any of
21 these conferences because there is no logical or depository
22 from the U.S. Government of a policymaker.

23 I think that is going to increasingly be a problem
24 for the U.S. Government, and I think similarly, as the
25 Commission focuses on adequacy and focuses on how to deal

1 with countries or sectors within countries as a whole, the
2 absence of any central office in the U.S. will pose a
3 practical negotiating problem for them.

4 Recently, European Union officials have come --
5 made visits here to the United States, and I would say
6 within say over the last year I have been asked at least a
7 half a dozen times by different foreign commissioners, when
8 they want to make a visit to the U.S., who should they talk
9 to, who is the right person in the U.S. Government to talk
10 to the commissioners. And whoever the right agency was
11 seven months ago is not the right agency -- not necessarily
12 the right agency today.

13 So we are seeing a constant shifting and changing
14 and sometimes it's the same agency just playing musical
15 chairs, but it's a real problem for the foreign agencies
16 when they are going to be looking at questions about
17 adequacy. And more importantly, one of the provisions in
18 the directive allows for bilateral negotiations. And it's
19 not at all clear who, if the Commission wanted to begin to
20 engage in bilateral negotiations, who would be the right
21 people from the U.S. Government to conduct those
22 negotiations, where would we have the right expertise, who
23 has the right jurisdiction.

24 To conclude, I guess I want to make three points.
25 One, I think for the transport of data flow we will see some

1 particular solutions. We will see -- there will have to be
2 practical solutions worked out.

3 I think the second point is that foreign pressures
4 will force fair information practices on the United States
5 through both legal and extra-legal means. And for the
6 moment I think that's going to be forced on foreign ties,
7 because that's where the more consistent, broader view,
8 comprehensive view of data privacy is being mandated.

9 And then I guess my third, I will come back, I
10 think we really need some sort of U.S. Government policy
11 center to be able to advance the sorts of discussions that
12 happened here today as well as the international dialogue.

13 MS. SCHWARTZ: Well, I have a very long list of
14 issues that your comments generate. I want to turn first to
15 Ron Plessner who I spoke with earlier about kind of reacting
16 to the presenters, and giving us his views either directly
17 addressed to Joel's comments, or otherwise.

18 MR. PLESSER: Well, let me very quickly say that
19 Gary's presentation was terrific and demonstrates, I think,
20 how self-regulation works, and how companies can respond to
21 both market and regulatory demands without being subject to
22 regulation or control, and I think that is a good example.

23 Turning to Joel, it was just so much and
24 excellent, although I finally found something that I really
25 very much disagree with Joel. We usually just -- we usually

1 just look at the picture, and I say it's half full and he
2 says it's half empty, and we are both right, but it's a
3 different perspective.

4 I actually pretty strongly disagree with him about
5 surfing and electronic access, and that it's stronger in
6 Europe than the United States. I actually do not think
7 that's true from what I said this morning. And I have been
8 asked both publicly and privately if I wanted to set up a
9 secure e-mail system, would I do it in the United States or
10 would I do it abroad.

11 But the answer is you would do it in the United
12 States, and the answer is the reason why is that the
13 Europeans have not -- really have very little equivalent to
14 the Electronic Communications Privacy Act. Peter Harter, I
15 think, very well today pointed out the problem that there is
16 a total derogation in the EC for government access and use.

17 Part of the cultural difference, and maybe this,
18 as Bob Sherman says, this goes all the way back to the boat
19 in the Boston Harbor and why we are a little bit different.
20 Our system has developed over the years, in fact, centuries
21 with the Fourth Amendment, on the basis of controlling
22 government access to private sector records. And those
23 rules are fairly refined by the Privacy Act of 1974, with
24 all of its problems is a comprehensive privacy federal
25 statute way before the Europeans did one, and I would

1 suspect that it compares favorably to what the Europeans are
2 now suggesting to do on a directive.

3 Secondly, we do have ECPA, we do have the Fourth
4 Amendment, we do have wire tap controls. We have controls
5 on how information is used in storage. These are not
6 academic questions. I counsel clients where European
7 authorities have tried to get access in e-mail storage, and,
8 frankly, if it's deposited in the United States, generally
9 they have gone away because the answer is that they have got
10 to go to the department, they have got to get a valid
11 subpoena from their country of origin. They have got to go
12 to the Justice Department. They then have to get a
13 corresponding subpoena, and then it has to be served -- or a
14 warrant, and then it has to be served in the United States,
15 where in France, as I understand it, the captain of police
16 can sign an administrative order, and all of your
17 information can be obtained.

18 There is a difference in focus, and I think we
19 really make a mistake if we get defensive about our laws or
20 be convinced that somehow we are inadequate or secondary to
21 the Europeans. We have focused historically on a different
22 issue.

23 In terms of the transport of data flow issue and
24 the impact in the United States, I think if what Joel says
25 is right, that would be fine, or at least that's a start.

1 The Europeans, as I understand it, are not satisfied with
2 just the point of presence for contact. The State
3 Department has done that. Now maybe the CIA will do that.
4 What adequacy is, at least as we hear it, or the question is
5 whether or not there really needs to be a U.S. data
6 protection commission with regulatory authority.

7 And I think today is a wonderful example of how we
8 have regulatory commissions who work on substantive issues
9 like unfairness and issues like that, will follow those
10 issues where they go, will create privacy guidelines and
11 debates, and really we don't need another agency, an
12 independent regulatory agency on privacy. The Federal Trade
13 Commission, the Trade Commission, the Securities and
14 Exchange Commission are looking at some of these issues.
15 This is really the way to go, and then perhaps the
16 government -- I do agree with Joel that there should be more
17 of a centralized policy within the government, but that's
18 not what the Europeans are looking for. The Europeans are
19 looking for enforcement.

20 The other issues, and let me just end with this,
21 is everybody talked about data commissioners, and, you know,
22 that that's necessary, or may be necessary for adequacy and
23 the other issues. One of the elements of the European
24 Commission -- two more points -- one of the elements of the
25 European Commission is data registration.

1 Well, when we talk to the European representatives
2 they all say, well, of course we don't mean that. We don't
3 want you to do data registration. Well, why not? I mean,
4 data registration is just as much an element of the European
5 Directive as the privacy commission is or the enforceability
6 rights. And so the question of this kind of picking and
7 choosing is somewhat confusing.

8 The other point that I do want to point out, and I
9 would like Mari Ann Blatch to talk about it, because she
10 worked very hard on it, that in terms of the Directive in
11 Europe and direct marketing there is a provision in there
12 that allows for what we would normally call notice and opt
13 out rather than affirmative consent for direct marketing
14 purposes.

15 So I think the European Directive has been
16 responsive to direct marketing activities, and we think on
17 that level, in terms of a European look governing what
18 Europeans are doing for themselves, it's fine. The question
19 is what can they tell us to do about how we run our system.

20 MS. SCHWARTZ: In some order of indications of
21 speaking, I am going to ask Barbara, Roger, Marc, and Mari
22 Ann, you have been volunteered, so I will put you there in
23 that order. That's a good way to proceed.

24 MS. WELLBERY: Thank you.

1 I am with the Department of Commerce, and chief
2 counsel of the NTIA, National Telecommunications and
3 Information Administration, a part of the Department of
4 Commerce.

5 And we are very involved in the issue of privacy
6 as are other parts of the executive branch, as is obviously
7 the FTC.

8 Last fall NTIA published a privacy report that
9 specifically focused on the telecommunications sector, and
10 recommended a voluntary framework that involved notice and
11 consent. Our report built on the principles that the IITF,
12 the working group, the Information Infrastructure Task
13 Force, Privacy Working Group, had developed earlier in the
14 year. So there is quite a bit going on in the executive
15 branch on the policy development side, and the working group
16 on privacy continues to work on policy development as does
17 NTIA.

18 We also, in case Joel needs to know, we will be
19 working at the State Department on the negotiations with the
20 EU. We met last week with the -- informally with the EU
21 representative, and we pulled together an interagency
22 government team that met with the EU representatives. So
23 there is an effort to focus on those issues. There is focus
24 on those issues in the executive branch.

1 At the risk of being told that I am straddling the
2 fence, I have to say that I agree to some extent with
3 everything everybody said, and disagreed to some extent. I
4 do agree that the U.S. has a very different tradition with
5 respect to privacy. We come at it very differently. We
6 have a sectoral approach as opposed to an omnibus approach.
7 We have, as a result, a much less centralized approach. As
8 Ron said, we tend to be much more distrustful of government
9 rather than the private sector. In Europe, it tends to be
10 the reverse.

11 When you hear about the kinds of registration that
12 Europeans go through in terms of where they live, and if
13 they move for more than two weeks at time, if they are on
14 vacation, they have to register with the police. It sounds
15 just flabbergasting to an American, and yet quite the norm
16 for a Frenchman, at least.

17 We agree that the private sector needs to do
18 something for a variety of reasons. It's the right thing to
19 do, first of all. Second of all, our concern is that the
20 Internet and its wonderful potential will never be realized
21 if people don't feel comfortable using it, and we feel that
22 they won't if their privacy is not protected.

23 We also think that it would be a mistake for the
24 U.S. Government to take action now in terms of regulation or
25 setting up any kind of central office for two reasons.

1 One, because we are concerned that any effort to
2 regulate the Internet right now might freeze the Internet or
3 in some way interfere with its ability to continue to
4 develop. It's an extremely fluid creative medium, and it
5 should be -- and it's done wonderfully without regulation.
6 And the trend in the U.S. right now, certainly in
7 telecommunications, is toward deregulation. And so we
8 shouldn't begin to regulate the Internet. Certainly not
9 now, as we are deregulating other parts of the
10 telecommunications market.

11 Second, we think it's premature to regulate in
12 response to the EU Directive at this point. We are still at
13 very early points in discussions with the EU. As Joel said,
14 the EU is still defining what it means by adequacy, and its
15 group is still working out what the various things mean.
16 It's not clear how different provisions of the EU Directive
17 will be implemented. I have heard the same thing that Ron
18 has heard, that registration -- that transparency is more
19 important than registration.

20 So I think we really need to be educating
21 ourselves right now about what's going on in Europe and what
22 the EU's view of the directive and how it needs to be
23 implemented is. I think the U.S. Government needs to be
24 educating itself about what the private sector is doing, and
25 encouraging the private sector to do everything it can on a

1 self-regulatory basis. But I don't think this is the time
2 to create any new bodies in the U.S. or to create any new
3 laws other than the medical privacy law that I am aware is
4 coming up now.

5 Thanks.

6 MS. SCHWARTZ: Thanks. Roger, will you introduce
7 yourself too.

8 MR. COCHETTI: Yes. I am Roger Cochetti with IBM
9 and here on behalf of Interactive Services Association.

10 For those of you who find the discussion about the
11 European Directive a little bit confusing, particularly in
12 light of the conversations that have taken place here
13 earlier today, that confusion is understandable, and it's
14 important to recognize that.

15 The European privacy directive is principally
16 aimed at managed centralized data networks that are subject
17 readily to the control of national jurisdictions. Most of
18 the discussion we have for the rest of day has been about
19 the Internet, which is an unmanaged, uncentralized network
20 of networks that is not subject to or readily controlled by
21 national jurisdictions. And thus the existence of the
22 privacy directive and the requirement of adequacy of third
23 world countries forces us to examine and will force us to
24 examine two very central questions, which I think are
25 central to the whole process of the FTC looking at this.

1 The first is the extent to which national
2 regulation can manage the protection or even contribute to
3 the protection of privacy in an Internet environment, in a
4 highly distributed Internet environment.

5 Others have mentioned earlier that the Internet is
6 a global environment, and as such I think nearly all of us
7 who have used it recognize that it is not difficult for a
8 service provider to move from one country to another, or to
9 relocate their service and facilities.

10 But by the same token, it's quite difficult for a
11 national authority, whether it's the European Commission or
12 a United States federal agency, to regulate the activities
13 of service providers who can move quickly between national
14 boundaries.

15 This, however, is not so much a problem, and not
16 so much the case with dedicated and centralized private
17 networks which are the main subject of European privacy
18 directive attention.

19 And by the way, before leaving that, it's probably
20 also worth pointing out that those highly centralized,
21 highly managed networks today carry an enormous quantity of
22 vitally important information. We haven't spent much time
23 today talking about them because we have been spending a lot
24 of the day talking about the Internet, but those private
25 networks which the European privacy directive seeks to

1 regulate are critical to commerce and business in our every-
2 day life.

3 The difficulty is that the regulatory framework
4 that's used by the privacy directive is aimed at those
5 networks, and not at the highly decentralized network or the
6 Internet.

7 The second question is, which we touched on
8 earlier, I think, in the discussion, about the role of
9 technology and technology solutions. I think if there was
10 ever a situation that will force an examination of how
11 adequate regulatory tools can be in dealing with protection
12 of privacy on the Internet, the effort by the 15 European
13 governments to devise national legislation that implements
14 this Directive as it relates to the Internet will be a
15 perfect test case, because the -- the regulatory tool, as
16 Brian Ek pointed out earlier today, is a relatively clumsy
17 tool. It's slow to develop and even slower to change, but a
18 detailed regulatory tool that's created under the
19 preexisting structure that's aimed at private data networks
20 is an even more difficult tool to use to regulate privacy on
21 the Internet.

22 So I think, in conclusion, what I would say is
23 that no one should miss the point that the European privacy
24 Directive is a very, very important initiative on the part
25 of the European Commission and the European governments, and

1 it will have an enormous impact on private data networks
2 which are a vital part of commerce and our every day life.
3 How it will relate to the Internet and the provision of
4 services on the Internet is beyond most people's
5 understanding, and certainly not an easy question for any
6 regulator in the United States or much less in Europe to
7 answer.

8 COMMISSIONER VARNEY: Teresa, before you move on,
9 I think there is an important point here that I would like
10 to get some clarity from the panel on. I have now heard
11 today two sides of one position.

12 There seems to be a group of people on the panel
13 who argue very vociferously that the EU Directive was
14 created for, aimed toward, means to deal with large highly
15 centralized databases.

16 There is another group on the panel that says no,
17 that is not so.

18 Have I got that right? Panelists, is there a big
19 debate in this community?

20 MS. SCHWARTZ: Let's ask Marc.

21 MR. ROTENBERG: I would be happy to defer on this
22 to Joel, because I think his presentation was quite expert.
23 But it's very important to understand how the EU directive
24 came about as opposed to the European convention or the OECD
25 guidelines.

1 The EU Directive came about because of the growing
2 harmonization of the European Economy and an attempt to
3 promote the free flow of information within the European
4 Community. At its heart, this is an effort to standardize
5 national, legal regimes.

6 Now, there are other interrelated directives, some
7 of which address ISDN and some of which address network
8 services, but I think that characterization would be
9 actually a little bit misleading. It is not so much the big
10 day-to-day 1960s model. It was, rather, to create an
11 environment, and this is critical to understand the purpose,
12 that reflects the commitment to human rights in this
13 emerging economy of Europe.

14 And if I could continue to answer your question?

15 COMMISSIONER VARNEY: And I would be interested in
16 testimony being submitted for the record on this point,
17 because it does seem to me there is a lot of disagreement
18 here about precisely what the EU directive is aimed toward
19 and why it may or may not be consistent with the U.S.

20 MR. ROTENBERG: If I could continue.

21 MS. GOLDMAN: There is just one line in the
22 Directive, I think part of the disagreement comes over what
23 the Directive actually says, which is that it is meant to
24 apply to the process of personal data that is automated or
25 contained in a filing system structured to permit easy

1 access to personal data. And so they are fairly clear that
2 they are looking at automated records and records that are
3 in a filing system that is organized by personal
4 information.

5 MR. REIDENBERG: You have to also look at the
6 definition of "filing system", which points out specifically
7 that it applies whether it's centralized, decentralized or
8 dispersed in a functional or geographic basis. And all of
9 the rights and responsibilities that the directive imposes
10 on what's defined as the controller of the data. And the
11 controller of the data is, and this is again from the
12 definitional article in the Directive, is the person who is
13 determining, either alone or jointly, who determines the
14 purpose and means of processing the personal data.

15 So it's really designed not at the collection of
16 data itself per se, but at who is pulling it together, who
17 is doing something to data.

18 COMMISSIONER VARNEY: Okay, Teresa, as we go
19 forward, I don't think we need to spend a lot of time here
20 on this, but I would again really urge you who have opinions
21 on this to submit them to us in writing, because this is an
22 issue we will be looking at as we go forward.

23 MR. ROTENBERG: If I could just continue. I
24 wanted, apart from Joel's excellent presentation, I wanted
25 to also note that I thought Gary's presentation was

1 excellent. But I don't think it's perhaps quite fair to
2 say, Gary, that part of the reason that Dun & Bradstreet has
3 the very good policies that it does isn't related to the
4 presence of privacy regulations in the different countries
5 that you do business in.

6 It is in interacting with these different
7 countries and addressing issues with regard to privacy and
8 security and so forth that you are able today to make this
9 presentation. I think it's -- you know, it's quite helpful
10 to us to understand how businesses respond.

11 But what I would really like to do is answer a
12 point that Ron Plesser made, and I have to say in some
13 respect I sort of wish what Ron said were true. I don't
14 mean to be unkind in that comment, because Ron and others
15 have made a great emphasis on the importance of the
16 Electronic Communications Privacy Act, which was the
17 amendment to our federal wire tap statute in 1986, continued
18 a tradition that goes back to a Brandeis dissent in a 1928
19 case and even our Fourth Amendment: put some constraints on
20 government, a very important principle, and I think in 1986
21 it was very timely, without question.

22 But I don't think in 1996 it would be fair to say
23 that it is the U.S.'s role, particularly on the
24 international front, to put constraints on government when
25 it comes to communications privacy. You would have to

1 conclude, if you even pick up this morning's paper and look
2 at the front of the New York Times Business Section, that it
3 is almost the opposite; that it is the United States due to
4 the clipper chip, due to the FBI wire tap bill, through
5 informal negotiations that are conducted not by our Commerce
6 Department, but by our Justice Department, to expand the
7 ability of foreign governments to surveil their own
8 citizens. That is the cold, hard reality of privacy in
9 1996.

10 And it comes about, in part, because we do not
11 have in place within the federal government an office that
12 has tried to advocate privacy interests, whether they be in
13 the private sector or the public sector.

14 So, I mean, my point is really not to so much
15 disagreement with Ron. I mean, in 1986, the ECPA was very
16 important for what it did. But what has happened since that
17 point has been to, you know, set in motion forces that have
18 served, you know, neither the private sector's interest or
19 the citizen's interest, particularly when we talk about the
20 development of international communication standards.

21 MR. PLESSER: Can I respond?

22 MS. SCHWARTZ: Very briefly. I have a line up
23 here, and I am going to say the order in which people are
24 going to speak. It's Mari Ann, Doug, Janlori and Evan.

25 So quickly.

1 MR. PLESSER: Thank God we have the ECPA.
2 Otherwise that chipping away would have occurred with
3 dispatch, and let us have the Europeans do something
4 equivalent so that when we send our data over to Europe we
5 know it's not open for government inspection.

6 MS. SCHWARTZ: Okay, Mari Ann. You should
7 introduce yourself, Mary Ann.

8 MS. BLATCH: I am Mari Ann Blatch. I have been
9 Chair of the U.S. Council for International Business Privacy
10 Committee since we set it up. And I say "we," it was
11 Reader's Digest, IBM, and American Express back in 1968,
12 that petitioned our parent, the International Chamber of
13 Commerce in Paris, to set up a committee on information
14 policy, and particularly data protection laws, because if
15 you are an international company you have to be involved in
16 both the original private mainframe and then eventually the
17 lease networks and now into the Internet, and we had an
18 exchange of information there. How did we deal with the
19 Swedish also? How did we get certified by the French law?
20 How did we set up information officers in our German
21 subsidiaries, et cetera?

22 That grew to a point where the business community
23 petitioned the U.S. Government, the U.S. Council and others
24 worked with the government back in the eighties and said,
25 please go to the OECD. Please work to get privacy fair

1 information practices. Those principles, as Marc has said
2 many times today, are well accepted worldwide. If you look
3 at national data laws, privacy laws, information policy
4 laws, many of them are still using those same principles.
5 We are still talking about those same principles.

6 We are talking today, I think, there isn't a
7 controversy, Commissioner Varney, I feel, because the
8 original effort of the EU was to create a market and try to
9 harmonize those laws which had to do with those situations
10 at that time.

11 The U.S. Council for International Business has
12 had many meetings with the EU since 1990, when the first
13 directive was prepared. And in all of those conversations,
14 with John Mold, the Director General of DG-15, he said we
15 will work with international business. We do not want to
16 cut off the free flow of information, but we would like to
17 see that there should be an assessment in the light of all
18 circumstances surrounding the data operation, the nature of
19 the data, the purpose, the duration of the processing,
20 internal laws, self-regulation laws. And we have had the,
21 ICC and the European Commission have had a series of annual
22 meetings. These were sponsored by the European Commission
23 and by the ICC in Brussels starting in '94.

24 And at that first meeting we talked about
25 alternative solutions, and that's where the idea of a

1 contractual possibility arose. But inside this private
2 lease network you could have a sort of contractual
3 protection and get security, your cryptograph. All the
4 people that have been talking today about those kinds of
5 protection, we're addressing those kinds of networks.

6 More recently, when John Mold was here a month
7 ago, and met with a group of private and government
8 agencies, and many of you were in that meeting, we talked
9 again about how does he see the methodology that will be
10 applied in the future, because in October 1998 they have to
11 decide how they are going to apply it, and they are looking
12 at that now.

13 And he told us that, number one, as Joel
14 mentioned, there is a study out, and they will be looking at
15 that in the working parties in September and December. But
16 in the meantime, he said very clearly, "I can imagine," and
17 he said this since 1990, the same thing, "I can imagine a
18 sort of cocktail that could be made up of internal policies,
19 rules, laws, regulations and a combination thereof."

20 What we are now talking about is when two
21 representatives, or one representative from DG-15 and one
22 representative of the Data Commissioners Working Party were
23 here last week, they announced that following the
24 Information Society paper, which is better known as the
25 Banglin paper, that now they have established an information

1 forum which is made up of business, government and data
2 registrars, and they are looking precisely at the whole
3 question of the Internet, and what regulatory regime you
4 might need, and in what way would that be the same, in what
5 way would that be different. And they foresee that the
6 mechanisms that they have established will be also examined
7 to see if that will carry them forward in this area.

8 So I don't see conflicts. I think we are on both
9 sides, the EU/U.S., have to remember, and that's my role as
10 the chairman of the U.S. Council for International Business,
11 to say what Gary Friend said a minute ago, we are global
12 companies. We are companies that have to build practices
13 not because there is OI Sweden, although of course you are
14 right, Marc, that helps, but because in order to do business
15 around the world you need to establish policies and then
16 work with their OECDS and then support the U.S. Government
17 as it tries to work.

18 So we think that back in the mid eighties when
19 U.S. business interests pleaded with the U.S. Government to
20 set up a point person with a phone number and a fax, and
21 they established in the State Department the Office of
22 Ambassador for Coordination of Information Policy, and Diana
23 Dugan was the first spokesperson. And then it did shift in
24 January, and Diana and I were on many OECD delegations when

1 sometimes the leadership was the Office of Consumer Affairs,
2 and sometimes it was another agency.

3 Not speaking on behalf of my committee but
4 speaking personally, I am delighted that NTIA is now
5 stepping up and leading our bilateral discussions, and I
6 think that the more we do together, and by the way, the
7 third annual meeting between the European Commission and the
8 ICC will take place this year, and Olf Bruhahn will be
9 speaking to us about methodology and how we can work
10 together in a nonconfrontational way.

11 I am a born optimist. I have been working at this
12 since 1970. I do not have gray hair. I still think it's
13 going to work out.

14 Thank you.

15 MS. SCHWARTZ: Thank you.

16 Doug, do you want to introduce yourself?

17 MR. BLANKE: I am Doug Blanke from the Attorney
18 General's Office in Minnesota.

19 I want to thank the Commission for the seat at the
20 table today, but to say that I still do aspire one day to
21 become a crystallizer.

22 (Laughter.)

23 And I am waiting for my aura to align with my
24 energy level, then I will be ready to crystallize.

1 I want to congratulate the Commission for
2 including this particular session, and for the workshop.
3 Unfortunately, those of us who work at the state and local
4 level in consumer affairs do so in almost total ignorance on
5 a day-to-day basis of the work of our counterparts in
6 Europe. And even our federal colleagues, I think it's fair
7 to say, don't always have a detailed familiarity with the
8 activities that are going on in the European community and
9 elsewhere around the world.

10 That kind of ignorance is unfortunate in any area
11 of consumer protection, but in this area it can really be
12 perilous, because the choices and policies that may be set
13 by someone in a distant jurisdiction can drive and even
14 determine the practices of an international business and may
15 apply to the consumers who reside in our jurisdictions,
16 whether the distant official is a Bavarian concern about
17 obscenity on the net or whether it's a Swedish data
18 practices commissioner.

19 So we need to study the European experience and
20 see what we can learn from it. I think a number of lessons
21 in the areas of harmonization and how we go about trying to
22 reconcile variations among multiple jurisdictions, that's
23 something we wrestled with very early in this country.
24 Although we don't always word it in terms of harmonization,

1 we are more like to speak about federalism and preemption
2 and uniformity and state's rights and so on.

3 But I think there are some lessons there in this
4 directive. Even more importantly though I think, and to me
5 perhaps the most foremost lesson, goes back to a question
6 that ran throughout this morning's sessions of this
7 workshop. And that was the question who should have the
8 burden, the person who is the subject of the personal
9 information or those who would commercialize that
10 information.

11 And I think the EU Directive, while it may be
12 fraught with ambiguity, it does seem to have answered that
13 question, at least as a starting principle. It proceeds
14 from the premise that privacy is a fundamental right, and
15 then the analysis proceeds from there. The design of the
16 Directive assumes that the burden resides with those who
17 would limit the right of the privacy, and it is their burden
18 to demonstrate some competing interest sufficient to
19 override the presumption of the protection of privacy.

20 At least with regard to certain types of sensitive
21 information, including the medical information that we
22 talked about in the preceding session, the EU has gone
23 farther, and has found its balance point by returning to the
24 premise that Evan Hendricks invoked several times this
25 morning. That's the notion that we take for granted in so

1 many other areas, the idea that the prerequisite for
2 compromising an individual's right is their informed consent
3 to taking that step.

4 And here the EU Directive applies that presumption
5 of informed consent, at least to the sensitive areas of
6 medical information, information about one's sexual
7 orientation or activity, racial and ethnic origin, beliefs
8 on politics, and religion.

9 And what I would like to see as we go forward from
10 this workshop today and tomorrow is some sustained effort to
11 see if there is any potential for achieving any consensus at
12 least about any of these types of sensitive categories of
13 information where informed consent might be an appropriate
14 prerequisite. The DMA earlier affirmed its view that at
15 least medical information is in that category.

16 And so I would be interested in hearing from those
17 from the business side of the discussion about what the
18 objections are to this sort of an approach, and to this sort
19 of European model, whether there are areas where it might
20 make sense, and whether it would work in this country either
21 in the context of self-regulation or something that might
22 come forward from either the national or the state level.

23 MS. SCHWARTZ: Okay, we don't have very much more
24 time for this session. I have three more speakers who have

1 indicated an interest, Janlori, Evan and Al. So just if we
2 can wrap it up in another five, six minutes.

3 MS. GOLDMAN: Thank you.

4 I think in the five years since the directive was
5 first proposed a number of us had hoped that we would be
6 able to use this as an opportunity in this country for the
7 passage of privacy laws.

8 As it applied to the Internet, though, I think
9 very different issues are raised, and much of our discussion
10 this morning, I think, could be instructive here. These
11 fair information practice principles incorporated in the
12 directive can be self-executing on the Internet in terms of
13 having people get access to their own information, having
14 people express their privacy preferences, and their
15 interests in detecting personal information, in terms of
16 unambiguous freely given consent, if that is something that
17 is stated at the outset. Again, the information isn't even
18 divulged in the first place.

19 A number of the concerns that were raised here
20 earlier, I want to echo in terms of concern about a
21 registration authority and how you would apply an omnibus
22 model to the Internet. But again, I think that some of the
23 practical solutions that we talked about this morning can be
24 very instructive here, particularly given that are not going
25 to see any legislation in the next couple of years, given

1 that we haven't seen any in the last five years to respond
2 to the Directive.

3 MR. HENDRICKS: Thanks. I would like to start by
4 answering Commissioner Varney's excellent question. And
5 it's too bad we don't have a European to speak for the
6 Europeans here, because I think it would be very instructive
7 and helpful.

8 But I think there is no question to me it's not to
9 regulate big information networks. The primary purpose is
10 to advance the human right of privacy, and that is by giving
11 people a legal interest in their own information.

12 Who owns your name? Do you own it or the people
13 who collected on it? Who owns your information? It all
14 says something about you. But it stems from the history out
15 of World War II, and the Nazi abuse of personal information.

16 And going to Ron's point, in the nineties now
17 there is a significant blurring of the line between the
18 public and private sector. We have a Census Bureau. They
19 are protected by statute. But a few weeks ago when Yahoo
20 and Data Base America put up 170 million Americans on the
21 Web, you could just dial in and find anyone's name and home
22 phone number, and address. We got Janet Reno's address
23 here. And as soon as she was writing her story, Yahoo
24 pulled out 70 million names of the unlisted phone numbers
25 out of that database.

1 If we had the kind of protection that I advocate,
2 and which I think is the core of the European Directive,
3 people would be able to consent, whether they wanted that to
4 happen in the first place.

5 A quick story. The United Kingdom did not have a
6 privacy law. A company there was going to get a contract to
7 process identification cards for a Swedish institution. The
8 Swedish institution was blocked by the Swedish authority
9 from transferring the data to the U.K., because they didn't
10 have a privacy law. The U.K. company lost the contract.
11 They took their case to the government. The U.K. passed a
12 privacy law. They have a privacy commissioner. They have a
13 ridiculous registration scheme that we would never have
14 allowed here. So I don't think that's even on the table.

15 But I think they did the right thing for
16 themselves and the right thing for international commerce.
17 But in the United States it just astounds me that we keep
18 seeing -- what is it about American industry that keeps
19 wanting to paint itself into a corner.

20 I mean, we talked earlier about the auto industry.
21 If they would have -- I think it would have been the right
22 thing to do to go to more fuel efficient cars, and they
23 wouldn't have lost so much market share if they would have
24 done that. But they made the wrong decision.

1 If they would have had leadership from regulators,
2 this terrible word "regulation," where they got out in front
3 of this issue and said, hey, let's talk about down the road
4 and standards, you know, maybe they would have helped our
5 industry.

6 And so I think it's the same way. The only
7 question to me is whether the Europeans are going to enforce
8 their own Directive, Internet or not. It's personal
9 information, it's your name. It doesn't matter what medium
10 it comes through. And if they do enforce their directive,
11 we are on a collision course that's going to have incredible
12 implications for international commerce in line with what
13 the New York Times said on the front page of the newspaper
14 today.

15 So I am optimist too. I think, because privacy is
16 such a fundamental value, people will never stop struggling
17 for it. But I want to see some enlightened leadership out
18 of our government agencies, and out of our industries, not
19 just because it's the right thing to do, but very soon our
20 economic viability is going to --

21 MS. SCHWARTZ: Al, you have the last word, at
22 least for this session.

23 MR. VEZZA: Well, I am not going to say much about
24 privacy, but I thought I would put some context in here.

1 The Worldwide Web was invented by a British
2 citizen working at CERN, which is part of a physics
3 laboratory in Geneva, Switzerland. Now, in 1994, I made a
4 trip there and I started negotiations with him, and I was
5 able to convince him to come to MIT to be director of the
6 Worldwide Web Consortium. I was able to do that for two
7 reasons, and I think we in this room have to understand why.

8 The first reason is, is that he viewed, and I
9 think he was right, that the U.S. was more entrepreneurial
10 than the Europeans. The second was that the Internet, which
11 is far larger than the Worldwide Web, it's far larger in the
12 United States. In fact, we probably at that time had 95
13 percent of all the Worldwide Web sites in the world here in
14 the United States.

15 So he decided to come, and we actually set up a
16 very interesting activity at MIT: 140 companies, as I said,
17 are members.

18 Now, having said that, I have spent a week once
19 every two months in Europe. I have talked to the European
20 Union. I have talked to my partners over there. And I will
21 say that I see a lot of change in the European Community.
22 Just this January the Internet was endorsed by France
23 Telecom. Now, France Telecom had an operation called
24 Minitel, and had actually blocked the Internet almost
25 exclusively in France. But because of this cooperation with

1 INRIA and because of pressure from the European Union they
2 embraced the Internet and have now opened up the Internet in
3 France.

4 I view that what is going to happen is that there
5 will be a dialogue between the United States and European
6 Union, and somewhere along the line we will come up with a
7 solution to all of this.

8 But what I want to leave you with is be very
9 careful about passing regulations at this point in time, or
10 passing laws at this point in time that are going to be
11 outdated in two, three, four, or five years. I think one
12 has to look very carefully about what one does in this
13 domain because the Internet is changing very rapidly. It's
14 changing the people's preference very rapidly.

15 MS. SCHWARTZ: Thank you very much.

16 This has been an excellent discussion, and I think
17 we all learned a great deal from it. And I thank all the
18 panelists for their participation.

19 We are going to take about a 10-minute break so be
20 back very quickly so we can go on to our next session.

21 (Whereupon, a recess was taken.)

22 MR. MEDINE: Thank you very much.

23 We would like to start our final session. Just a
24 couple quick housekeeping announcements. If anyone thinks
25 they might be getting messages or would like to check if

1 they have gotten messages, please check the message board
2 outside on your way out.

3 Second, I would like to thank -- I don't know if
4 he's in the room -- Randy Clark. I have never been to an
5 Internet program where things have gone so well as far as
6 demonstrations. And if Randy is here, I would like to thank
7 him for that effort. I appreciate it greatly.

8 I would like to get you mentally back into the
9 discussion, mostly of this morning, of what do we do to
10 protect consumers' privacy online generally, get yourself
11 out of the European framework, and get back into a domestic
12 mindset.

13 And two questions we want to consider in this
14 final session, I think, are critical questions. One is, how
15 do we educate consumers about how information is used
16 online, and how they can go about protecting that
17 information. And equally, if not more importantly, how do we
18 educate businesses along the lines of the presentation just
19 a moment ago that it's in the businesses' interest to have
20 some sort of privacy protection? And how can businesses go
21 about as a technical matter implementing privacy
22 protections?

23 We are going to again follow the crystallizer
24 format, and our first crystallizer, who has come in from the

1 west coast just to be here and crystallize for us, is Beth
2 Givens from the Privacy Rights Clearinghouse.

3 MS. GIVENS: Well, if I tell you I was in
4 California, you might think I am going to present you with
5 other ideas of what you can do with crystals and
6 crystallizing, but I won't do that.

7 I have been asked to describe what we do at the
8 Privacy Rights Clearinghouse, which is at the University of
9 San Diego, Center for Public Interest Law. So I will start
10 off with telling you about our center and then go into what
11 I see are some of the more important aspects of consumer
12 education that should be considered in the online world.

13 The Privacy Rights Clearinghouse is a consumer
14 education and research program, and we have been in
15 operation now for three and a half years. We are grant
16 funded from the California Public Utilities mostly, and we
17 operate a toll-free telephone hotline for California
18 consumers to call, ask questions, raise complaints, and get
19 information.

20 I think I am truthful in saying that we are the
21 only consumer education-focused privacy program in the
22 country. We do not have legal authority to take action, but
23 rather, we act as an information and referral service. We
24 give very practical kinds of street level information to
25 consumers on how they can take privacy protection into their

1 own hands. And we refer consumers to other sources of
2 information, whether that's government agencies, industry
3 representatives, other consumer groups and also the media.

4 Our arsenal of consumer information includes 19
5 publications which we call fact sheets. I have left one out
6 on the table earlier. Including privacy in cyberspace.
7 These publications are in paper form and also on the web
8 site. We get about 10,000 calls a year which is, I think,
9 considerable for a staff of three to handle.

10 Some of our part-timers are law students, and one
11 of the things I am proudest of is getting young lawyers to
12 be interested in privacy issues, consumer privacy issues in
13 particular. So we are turning out a few, I hope, privacy
14 advocates who are attorneys.

15 What have we learned in these past three and a
16 half years that can be applied to today's discussions? I
17 will make five points.

18 The first point has to do with visibility. One of
19 the best things that we can do as consumer educators is to
20 make the invisible visible. This is the first step toward
21 empowering consumers to take action on their own behalf.
22 One of the characteristics of the online world, and it's
23 been mentioned a few times here already today, is that
24 personal information can be gathered and compiled in ways
25 that are invisible to users.

1 Now, a major theme of this workshop, and I think
2 an action item that the workshop organizers probably want us
3 to take away with us, or would want the participants to
4 carry with them, is that online systems must be built with
5 information gathering mechanisms that are visible to the
6 user and which, of course, involve user's consent.

7 If the transparency is not built into online
8 systems, the results will be resistance to use, the
9 formation by consumers of conspiracy theories, and believe
10 me we have heard them all on the hotline. And as well as --
11 let's see, I'm sorry, I am reading from my notes here -- oh,
12 as well as finding ways to get around the information
13 gathering practices which would include sabotage and dirty
14 tricks. And I am working that up into another story.

15 We just learn tremendous amounts from consumers
16 who are so mad and frustrated about their lack of control
17 over personal information that they take great delight in
18 telling us how to screw up the system.

19 Okay, point number two, interactivity. At the
20 clearinghouse we have had the luxury, and it is a luxury, of
21 engaging in the good old-fashioned form of interactivity
22 called talking. We have real time dialogue with many of our
23 hotline callers. In fact, we talk with about two-thirds of
24 them personally. The other one-third is captured on our

1 voice mail system where they give us their name and address
2 and we send them publications.

3 We have learned something very interesting, I
4 think, from a couple of surveys that we have done with a
5 random sample of our users. Those who have talked with us
6 directly are more likely to take action to protect their
7 privacy than those who simply left their names and addresses
8 on the voice mail system.

9 Now, how does this finding relate to the online
10 world? Simply, when developing online forms of consumer
11 disclosure and consent, the more interactive such methods
12 the better. Consumers need to become actively involved in
13 the process of deciding the fate of their personal
14 information more than just reading a screen of text on log-
15 on.

16 My third point has to do with feedback. Many
17 consumer education initiatives do not involve feedback. A
18 lot of pamphlets are printed and distributed, or web sites
19 put together and that's it. But the learning loop is
20 missing. As I mentioned earlier, we at the clearinghouse do
21 have the luxury of talking to a lot of people, and I realize
22 that in the overall scheme of things 10,000 calls a year is
23 not that much, nor the few hundred web site visitors are all
24 that much, but what we can do with what we are learning from
25 these people is digest what we are learning, and then feed

1 it back to government agencies, legislators, industry
2 representatives, other consumer advocates and so on, much
3 like I am doing here today.

4 So when consumer education is built into online
5 systems, I strongly recommend that the architects of these
6 systems actually build in ways to learn from the myriads of
7 people who visit those sites. I think that taking tallies
8 of the number of consent boxes that are checked off will not
9 be sufficient. There is a great deal more that needs to be
10 learned in the consumer education process.

11 My fourth point has to do with the slogan "high
12 tech/high touch." If you remember back about a dozen years,
13 I think John Nesbitt, the futurist, coined that phrase. And
14 this point I am addressing to business and industry.

15 It is definitely in the best interests of business
16 to address consumer privacy at more than the lip service
17 level. Now, based on what we at the clearinghouse are
18 hearing from consumers, I would characterize industry's
19 efforts to date at addressing privacy issues as still at the
20 lip service stage for the most part.

21 Callers to the hotline are saying over and over,
22 and I can attest to this, I hear this every day when I
23 answer the hotline, they are saying over and over, "All I
24 ever get when I call the credit bureaus are those recorded
25 messages. I never can reach a real person." Or they will

1 say, "I signed up for that mail preference service, but I
2 don't know if it's doing any good, and besides how do I know
3 if my name is really on it?"

4 So what does this have to do with the slogan "high
5 tech/high touch"? That it's great to take advantage of the
6 power of technology to give consumers access to this huge
7 array of information and some services, but for those
8 service areas in which consumers might experience problems,
9 for example, privacy examples being credit fraud, unwanted
10 mail, phone solicitations, the human high touch element
11 cannot be ignored. There are times when consumers must get
12 in touch with real people to help them solve their problems
13 or answer questions that could not be conducive to online
14 communications. And unfortunately, consumers are
15 increasingly finding that the real time human interaction is
16 in scarce supply.

17 Now, my fifth and final point has to do with youth
18 or young people with a nod towards Sylvia Goodman of the
19 Illinois Privacy Council, who is making this one of her
20 focus points. One of the greatest challenges of consumer
21 awareness efforts is getting consumers to take notice of the
22 message that's being imparted and then to take some action
23 on it, to change their behavior.

24 For example, most adults today are not -- they are
25 not used to finding meaningful disclosure and consent

1 opportunities in the course of their every day transactions
2 where personal information about them is being given up.
3 They have virtually no expectation of being told that their
4 personal information is being gathered, and that they have
5 the opportunity to say yes or no about this.

6 Well, it's hard to teach old dogs new tricks, such
7 as looking for those disclosure notices when they are there
8 and then taking advantage of them by either giving or
9 withholding consent. That's why it's so terribly important
10 that youngsters learn about privacy when they are introduced
11 to technology in school. This includes looking for and
12 taking advantage of those disclosure and consent
13 opportunities, learning the consequences of revealing
14 personal information, and also being taught that when they
15 don't like the information gathering process that they are
16 seeing, they can and should take their business elsewhere.

17 Now, I must admit that I have had limited
18 experience interacting with young people in my consumer
19 education work, but in my few encounters I have been
20 horrified at the lack of privacy consciousness or even
21 interest in the topic. So I think there is a great deal of
22 work that can and should be done in this area of working
23 with youth, and raising their consciousness about privacy
24 issues.

1 That concludes my remarks and I thank you very
2 much.

3 MR. MEDINE: Thank you.

4 Our next crystallizer is a very familiar face here
5 at the Commission's public exercises in finding out what's
6 going on on the Internet. Bill Burrington is the assistant
7 general counsel and director of Public Policy at American
8 Online. He chairs the Online Public Education Network,
9 Project OPEN, which he will talk about, and Interactive
10 Services Association, and perhaps more importantly, Bill has
11 chosen to be with us here on his birthday. Happy birthday.

12 MR. BURRINGTON: Thank you very much.

13 VOICE: Twenty-nine today?

14 MR. BURRINGTON: I've actually aged since I have
15 been sitting here, so what a neat present this has been.

16 Thank you, David, and I want to thank the
17 commissioners and the Commission staff and all of you. This
18 is -- each time we have these, I think this is the third
19 public hearing that I have been to, they get bigger and
20 bigger, but we seem to be moving forward too and getting
21 more understanding, which is great. And I know the
22 logistics of putting this together have been a lot.

23 I want to just sort of put all of this in
24 perspective. You have heard today about the role of
25 government, the role of self-regulation. You have heard

1 about technology. And there is a third component that is, I
2 think, equally, if not sometimes, especially at this
3 critical stage as this medium is evolving as a global
4 medium, and that's education, the third component to this
5 whole thing.

6 And I want to say, to put some of this in
7 perspective and tell you a little bit about Project OPEN,
8 and then let Linda Golodner, the President of the National
9 Consumers League, provide her perspective as well on the
10 education front.

11 What I would like to -- as I listened to everybody
12 today, and I have been here all day, I would like to kind of
13 put this in perspective. I see here and hear here sort of a
14 couple of groups.

15 There are the pure privacy advocates who feel that
16 no matter what we do will never be enough, and that's fine
17 because that's their business, and that's their job as
18 advocates and it's an important role in this debate.

19 And I think there are some pure industry advocates
20 that absolutely at all cost would resist any kind or any
21 form of regulation, and say that self-regulation is the
22 answer. And I think neither of those viewpoints is entirely
23 correct.

1 And then there are sort of consumer advocates who
2 are here, like Linda and others, who fill a very important
3 role in this discussion.

4 But I think what has been missing, and what we
5 need to do, and in fact sort of for the record I would like
6 to suggest that this hearing record should not close until
7 the FTC does or engages in some serious empirical consumer
8 focus groups to take consumers who are actually using online
9 services on the Internet today and bring them in here and
10 ask them, to find out what they really think.

11 I mean, we all sit here in Washington, and many of
12 us either live here or come here to visit, and we are all
13 experts in this area. But it would really be nice to hear
14 directly from consumers when presented with choices. I am
15 sure we are going to hear that they care a lot about
16 privacy. Dr. Westin has done some great research in this
17 area. Of course, they care about privacy, but let's present
18 them with a series of options, and maybe explain to them
19 that, in addition to the power of this medium, it can
20 package material for you, it can make your life a little
21 easier so we don't have this constant flood of information,
22 and with that to become more offerors and customize
23 information that might be of interest.

24 And I would be interested to see the outcome of
25 that. I mean, it could be very, very revealing, because I

1 think we are all sitting here assuming that all consumers
2 are as interested in this issue as we are. We are very
3 interested, and I know the consumers are generally, but I
4 would be really interested to get their take on this whole
5 debate. And I encourage the Commission to do that to truly
6 make this a complete record.

7 I think that where we are at right now, and I want
8 to try to analogize this discussion today, this is very
9 reminiscent of the Communications Decency Act which the
10 court in Philadelphia is expected to rule this week sometime
11 on that very important First Amendment case. A lot of the
12 same components to that issue are here with this issue, as
13 they have been with the copyright issue, and as they are
14 with the encryption issue. And that is that there is a
15 blend of the role between the industry and other interested
16 parties and government, and a blend of technology as a
17 partial solution, and then the important aspect of
18 education.

19 And I think what we are going to see, I am fairly
20 confident, hopefully, that the court will rule in the right
21 way; that the idea behind the CDA to impose this big
22 government solution to sort of lure consumers into a sense
23 of security that government was watching out for their
24 children wasn't really going to work the way it was set up;
25 and that in fact a combination of technology tools that are

1 still in development, that are certainly out in the
2 marketplace, along with a really effective education program
3 might be an even more effective and meaningful solution to
4 the issue of child safety.

5 And I would argue that the same is true here with
6 respect to privacy. And I was encouraged by Barbara
7 Wellbery's comments, because I think that NTIA is looking at
8 it from that perspective as well. This is still very much
9 an evolving medium.

10 I am here on behalf of really the ISA. We have
11 been involved in this issue for a long time. In addition to
12 the ISA, DMA guideline process that's been underway for the
13 last several months, and I want to make the point here for
14 the record that that's a separate process from Project OPEN.
15 Project OPEN is a consumer education campaign.

16 And we got into that process because Maryland
17 introduced a bill last year that for the first time that
18 dealt with privacy and the online Internet environment, and
19 we made a commitment to the legislators in Maryland that now
20 was not the time for such a bill, and especially at a state
21 level because this is truly, at a minimum, a federal issue,
22 and certainly a global issue.

23 And the commitment that we made was that by June
24 we would have a really good down payment on some industry
25 privacy guidelines, and we have managed to fulfill that

1 commitment, and have made significant progress in the last
2 several months. So I think we are bringing more here than
3 just lip service to this issue.

4 In addition to that, the ISA were very involved --
5 the ISA companies, member companies, were involved with the
6 passage and drafting of the Electronic Communications
7 Privacy Act back in 1986. Several ISA member companies,
8 many of whom have been here, have privacy practices and
9 policies in place since the mid-1980s. ISA companies
10 pioneered the whole concept of online opt out in the early
11 1990s. And since that time, in 1995, most of the ISA member
12 companies now routinely strip out the identity of users as
13 they cruise the Worldwide Web, which preserves their privacy
14 unless they voluntarily wish to get out information.

15 And all of the ISA member companies involved in
16 the Internet industry have been active supporters of the
17 PICS process as well.

18 And, finally, we all joined together in 1996 to
19 create a thing called Project OPEN, the Online Public
20 Education Network. And the purpose of this was to take what
21 we felt were four critical issues. And this came from the
22 CEOs of these companies, and we have done this in
23 cooperation with the National Consumers League. And
24 essentially the campaign, which includes sponsors from
25 America Online, Compuserve, AT&T, Microsoft, Netcom and

1 Prodigy, and others are slowly coming on board, was to say,
2 you know, there is a lot of media attention about child's
3 issues, so we decided that's an important issue. There is a
4 lot of potential here on the copyright front in terms of its
5 impact on the future of the Internet, so we decided that was
6 an important educational issue. Overall consumer protection
7 was another one. And we identified privacy as a critical
8 issue here.

9 So what we will be doing is after these guidelines
10 or whatever kind of process we ultimately decide upon here
11 are implemented, we want to go ahead and educate and use the
12 unique power of our medium to education consumers about the
13 privacy rights, about the policies that we have all adopted,
14 and make it easy for consumers to truly make it a two-way
15 interactive process, so they can get their questions
16 answered online about their privacy concerns.

17 And I think when it comes to addressing
18 businesses, I think it's safe to say that the companies in
19 this room are the ones that care a lot about this issue, and
20 there are thousands of other companies out there in the
21 United States that will be part of the Internet in one form
22 or another. And I would love to see the DMA and the ISA and
23 the Federal Trade Commission and the National Consumers
24 League and NAAG and other groups work together to develop a
25 model curriculum, if you will, for businesses, to let them

1 understand why privacy is an important issue; what they can
2 do, some of the basics they can do to be safeguarding the
3 privacy rights of their customers, and then let's promote
4 that appropriately using the medium.

5 And maybe that's one of the solutions we are going to
6 come to here.

7 The other thing I want to point out on the whole
8 regulatory front is that I am not aware so far that there
9 has been a situation in which the Federal Trade Commission
10 has not been able to go after in an enforcement way the bad
11 actors when they are dealing with these issues.

12 And I think one of the things you run into with
13 the Communications Decency Act, because that debate got so
14 crowded by emotions and politics and everything else was
15 that a lot of the laws and regulations already on the books
16 already work. And my view is let's start there, and see
17 where we have problems. And I think that you all have been
18 quite active, and appropriately so, in going after some
19 people, and sending a message, and that is important. And
20 then let's look at those laws that exist, and if we need to
21 make some modifications, let's do that, and then we can go
22 from there.

23 And I think really what I am hearing most today is
24 that people are concerned about the self-regulatory approach
25 because of the enforcement side of it all. Maybe that's

1 where we need to focus our efforts on some more creative,
2 out of the box ways of putting teeth into these self-
3 regulatory approaches rather than say we need government
4 regulatory approaches just to come and get them.

5 And, finally, and this is a very personal thing to
6 me because I have watched this privacy debate now for two
7 years, and I have heard a lot of the same things here today.
8 We, all of us here in this room, whether you are an online
9 Internet provider, whether you are with the Federal Trade
10 Commission, or any other aspect of government, or whether
11 you are in the media, the media that are here that are
12 covering this event today, we have an affirmative
13 responsibility when it comes to education, to educate
14 responsibly and in an accurate way.

15 There have been a number of scary stories out
16 there, and some of them -- I testified in Maryland where it
17 was argued that AOL somehow can go into people's Quicken on
18 their computer and look at their bank account, and that was
19 a completely irresponsible, unfactual statement, and it does
20 nothing for the serious discussion and debate that needs to
21 occur on this issue.

22 So I would encourage those, particularly those who
23 are privacy organizations, to help us educate consumers, but
24 to do it in a responsible and accurate way.

1 And if you don't mind, I will turn this over to
2 Linda. Linda has been a tremendous help in realizing the
3 potential of this education campaign that we have mounted,
4 Project OPEN. And also just for your information I passed
5 around to the people up here our first brochure that we put
6 together, with an 800 number, and also available online to
7 our subscribers.

8 So, Linda.

9 MS. GOLODNER: Okay. I just wanted to echo what
10 Bill said about commissioners possibly bringing in some
11 consumers who actually are online.

12 Recently, HHS had a meeting with the Annenberg
13 Center in California. It was on cyberhealth, and I found it
14 very eye-opening to listen to individual stories of
15 consumers who were online, especially in support of chat
16 rooms, or support groups, when they had a condition that
17 they wanted to talk with people about. And I think that you
18 would learn a lot that way.

19 I also don't know if those consumers knew if some
20 of their rights were being -- their privacy rights were
21 being violated.

22 I think we have got to make sure that there is
23 proactive education both for consumers and for providers of
24 information. I think the better companies, obviously, will
25 be working on some proactive education of consumers on using

1 the Internet and using online services. But I always worry
2 about those bad actors, and I mentioned that before. They
3 are the ones that we always have to be aware of.

4 I don't think a lot of people really know what
5 personally identifiable information is. They don't know
6 that there is information that they should not give out.
7 They don't know how it's going to be used, and they don't
8 know how it can be used against them.

9 I think that a lot of purchases that people make
10 offline now, people are not aware of all the information
11 that's reflected about them, and how it can be used.

12 When we are educating consumers, we have to use
13 all sources available, and the media is one of the great
14 sources that consumer groups have found to get our messages
15 out, because this reaches millions of people.

16 Just doing a brochure and send it out to a few
17 people is not going to make a difference.

18 At the point of sale, point of sale of an online
19 service or where you buy a computer, obviously, is a place
20 where people are going to be concerned if they are going to
21 be going on the Internet, and they should be getting
22 information there.

23 People have to know what their choices are, and I
24 think it's an obligation of online services and on other
25 programs to provide information to consumers about the

1 choices of where they can check things out. They have to
2 know where they can go when there is a problem. They have
3 to know about the real people out there that can be actually
4 on a phone line providing information to them, maybe through
5 an Attorney General's office or through a consumer
6 protection office.

7 People have to be educated on what questions to
8 ask, what questions to ask once you get into an Internet
9 site, what are the warning signs that that site might be a
10 little dangerous for you as far as your privacy is
11 concerned. They have to know, as I said, who to call.

12 Consumers have to know what the rules are. They
13 have to know if there are rules in certain states or certain
14 jurisdictions that will protect them. Unless they know
15 those rules that will protect them, then they don't know
16 when their rights are being violated.

17 Last of all, I think that we should look at who is
18 using the Internet now, and I think that the statistics show
19 that more and more senior citizens are using the Internet,
20 and they are some people that we should be approaching now
21 with new information, and that we are going to be talking
22 about children tomorrow, so I won't touch on that.

23 But we should also look at who is going to be
24 using it for the future, and plan for the future and have
25 some proactive education for them.

1 MR. MEDINE: Thank you. You have done an
2 excellent job of focusing us on some very critical issues
3 here. Just a couple of quick technical announcements.

4 Additional copies of Chairman Pitofsky's
5 statement, which we ran out of earlier, are now available
6 outside for folks on the way out.

7 I just want to extend some additional thanks to
8 Ruth Sacks, Gregg Hill, Nichole Branch, and the many others
9 who helped out on this session.

10 COMMISSIONER VARNEY: I have a question for Bill.

11 The joint standards that ISA and DMA are working
12 on for Maryland, what are those standards about, and are
13 they privacy? Do they include some privacy? And when will
14 they be available? When will you be presenting them, and
15 when will they become operative? What's the time frame?

16 MR. BURRINGTON: Let me clarify it because the
17 standard guideline process emanated out of the bill that was
18 introduced in Maryland, the commitment we made to those
19 legislators. That's when we got going up here in Washington
20 with this item of very productive, several months worth, and
21 many hours worth of discussions and negotiations with DMA
22 and ISA.

23 So some of the principles, I think they agreed on
24 a number of them, and actually some of the preliminary ones
25 that we have, and our intent is to get that process

1 completed, you know, quickly, as soon as possible. We have
2 got a number of key components already that we --

3 COMMISSIONER VARNEY: Are they fair information
4 practice --

5 MR. BURRINGTON: They are privacy.

6 COMMISSIONER VARNEY: Privacy?

7 MR. BURRINGTON: Privacy, right.

8 Like in our case it's building off the ISA's
9 mailing list guidelines that we adopted last year dealing
10 with issues like spam and unsolicited e-mail, those kinds of
11 things. So it's going to the heart of these sort of
12 cyberspace privacy issues.

13 COMMISSIONER VARNEY: And when will you be able to
14 release them?

15 MR. BURRINGTON: They are in the back.

16 COMMISSIONER VARNEY: Okay.

17 MR. BURRINGTON: And we are still, again, are work
18 in progress, but considering the complexity of some of these
19 issues, there they are.

20 COMMISSIONER VARNEY: Okay. And have they been
21 adopted officially by ISA and DMA and are they binding on
22 the membership?

23 MR. BURRINGTON: I can't speak for DMA, if you
24 want to on that.

25 COMMISSIONER VARNEY: Yes, go ahead.

1 MR. SHERMAN: Yes, the principles have been
2 adopted.

3 COMMISSIONER VARNEY: Okay, and, again, the
4 guidelines are six months in coming?

5 MR. BURRINGTON: Yes, the principles have been
6 adopted by DMA, and from them the more refined guidelines
7 will be derived. Yeah, it will be this year.

8 The same with ISA. I mean, our board of directors
9 in fact meets tomorrow in New York to essentially put the
10 stamp of approval on the guidelines, and out of that we want
11 to get more meat on the bone, so to speak. And to be honest
12 with you, Commissioner Varney, that's the time we want to
13 reach out to you folks and then to others, to get input on
14 those.

15 MR. MEDINE: Okay, we started the day with CDT's
16 privacy screen as a way of demonstration -- educating
17 consumers about privacy.

18 Jerry, do you want to talk more about this issue?

19 MR. BERMAN: Well, I think we have been educating
20 ourselves as we set up our privacy screen. What we're
21 determining is that before we can educate consumers, there
22 has to be something to educate them about. There are the
23 beginning of privacy guidelines. There are some fairly well
24 along. Different companies have different sets of them.
25 But when we went out and said we want to put your guidelines

1 up, because we want to create an educational film where you
2 can click and find what company privacy guidelines are, some
3 companies were more ready than others.

4 The fact that there was public attention on those
5 guidelines, that they were going to be out there in the
6 market so that consumers could compare them, I think was
7 helpful in getting the online companies who had guidelines
8 to put them in different places, to take them -- to try and
9 present them. I think the pressure, these public forums,
10 which put the issue on very busy companies to begin with,
11 who are all out there growing by leaps and bounds, putting
12 attention on the issue help to focus them. And they say,
13 and really I said it -- I said it last time, I'll say it
14 again, there is a kind of crisis mentality which affects us
15 all, which is what's at the top of your plate.

16 Do we have to put up a guideline on the CDT page,
17 or do we have to send them to some congressional committee
18 who is holding a hearing, when is Commissioner Varney
19 calling them to be implemented in practice? Those are
20 deadlines, and they get people working as there are
21 deadlines on the Communications Decency Act, copyright or
22 any other issue.

23 To put privacy at the top of the page requires two
24 things. One is having a deadline like that, but the other
25 is to find the beginnings of something that looks like

1 progress or a consensus, or some way of bringing people
2 together around a step forward.

3 In my years, lots of people talk about the
4 Electronic Communications Privacy Act. What the Electronic
5 Communications Privacy Act, and most telecommunication bills
6 were, and privacy bills, will tell you is that without some
7 consensus between a good part of the privacy community, the
8 consumer community and industry, there ain't no legislation,
9 nothing goes forward.

10 So that if you state that our goal is to have a
11 big regulatory commission and an enforceable statute with,
12 you know, six regulators reviewing all the guidelines in the
13 world, you are saying it's a non-starter. Let's go home.

14 What was interesting this morning -- and on the
15 other side, we're going to continue to educate our consumers
16 as we go along. Some of that is real. Some of that can be
17 for all the best reasons disappear from the top line of a
18 company. So what was interesting this morning was that
19 there was -- between the, one the one hand, we need the big
20 law, and on the other, we don't need anything, there was an
21 interesting discussion in the technology meeting where both
22 technologists from MIT presented and said it is feasible in
23 interactive technology to not only do the kind of setting
24 up, labeling system so that EPIC or the ACLU can -- or the
25 FTC can set up a good guide, and you can go and block out

1 those sites if they don't have the right policy, but also
2 that the technology lends itself to on-screen communication
3 of what your or my privacy preferences are, allow companies
4 to meet those preferences, and say I will deal with you, or
5 I will meet your policy. Here is your policy, but I will
6 meet yours. I will do anything you want because I want to
7 sell you goods, or services or library books. And that
8 those could be, if there was a mismatch, that there could be
9 some negotiation and explanation of where we were in the
10 transaction. We want this, these are the trade offs, it's
11 my company.

12 That was a very sophisticated notice and knowledge
13 and opt in, opt out. I mean, it raises the distinction
14 between them, and it says for the first time interactive
15 technology versus signing contracts, adhesion contracts
16 almost, would kind of disappear into the back of lots of
17 agreements, because it's very hard for businesses to deal
18 with the consumer on an ongoing basis in an interactive
19 world there can be this back and forth negotiating process,
20 so that the technology lends itself for the first time as
21 saying, hey, consumers can have control over information
22 about themselves even though it may be held by or disclosed
23 to or given to third parties.

1 And at the same time businesses can negotiate back
2 to consumers to make more informed choices, and meet their
3 customer's needs and desires.

4 MR. MEDINE: Which is to say --

5 MR. BERMAN: I want to end it.

6 MR. MEDINE: Okay.

7 (Laughter.)

8 MR. BERMAN: But I have got to end it by coming
9 down on the process. To get that middle process requires a
10 process. It requires the consensus and bringing people from
11 the privacy community, the business community, the
12 technology community and saying, show us what you can do.
13 They said they can do it. Give them some time and say, come
14 back and show us how you can do it.

15 MR. MEDINE: I think the question is not only that
16 but how do you talk to the different ones out there on the
17 Net, if it's in your interest to do it. How do you
18 communicate that outside of this room?

19 Andy is next.

20 MR. STRENIO: It seems to me that there are
21 several additional points on the educational aspect we're
22 touching upon. First of all, I wanted to heartily endorse
23 Bill Burrington's notion of a focus group, if the FTC could
24 find it possible in its budget to spare those additional
25 resources.

1 But to strain the Commission's budget, further, I
2 would strongly argue that the focus group ought to include
3 and not simply be limited to current users, but be expanded
4 to people who aren't using it because there may be some
5 practical differences in their approaches or concerns to
6 privacy. And, in addition, these are folks that hopefully
7 will be coming on line over time.

8 I am certainly encouraged by all the work that's
9 already being done by the business community, as well as the
10 nonprofits and the governmental sector in terms of making
11 educational efforts as effective as is possible. Certainly
12 making them interactive helps reinforce the actual learning
13 process.

14 But, in addition, I think there is further room
15 for creativity as far as the particular venues for
16 educational opportunity to take place, or at least where you
17 can post messages alerting consumers to the possibility of
18 getting follow-up information. That can be done through the
19 computer manufacturers having standard materials inserts
20 when you purchase a computer. That can be done through the
21 computer retailers. That can be done through the online
22 services having screens that bring that to attention, so
23 that all those are possibilities as well.

24 David mentioned the question about how do you
25 reach the business community and get the message to them

1 that it's in their interest. And that's obviously a very
2 important question, as was brought out this morning, a very
3 high percentage of web sites currently don't have any
4 privacy guidelines that they post or even that they have
5 adopted, and that's most likely not out of malice, but out
6 of a sense of just not having reached those questions.
7 That's something that obviously needs to change over time,
8 not only to help them draw more customers who have greater
9 assurance that those privacy guidelines are in place, and
10 then they can decide whether or not they want to deal with
11 that particular business entity. But, in addition, I think
12 -- rather, the smaller businesses need to be educated about
13 potential issues and pitfalls for them in the world that I
14 think is coming.

15 For example, as the pressure grows for greater
16 consumer access to information about consumers that is put
17 online, and for the ability to correct that information, you
18 may have the businesses that are transmitting medical
19 records, HMOs, doctors transmitting patient records online
20 who aren't thinking about the security of the patients that
21 are present may, out of the most basic self-interest
22 motives, decide to type it up in a hurry if and when that
23 information can be gotten from them.

1 MR. MEDINE: Given our very short time, I am going
2 to exercise the privilege of the chair, and keep people as
3 short and to the point as possible.

4 Mallory, could you -- did you wish to say
5 something?

6 MR. DUNCAN: I am Mallory Duncan of the National
7 Retail Federation.

8 I wanted to pick upon something Andrew was saying,
9 that is, why there is not more activity on the part of
10 businesses. I mean, the first step is to determine what
11 information violates consumers situational privacy
12 expectations, and that is a much more difficult concept, a
13 very difficult concept to achieve in practice. From the
14 retailer's perspective, our goal is service. And service is
15 what creates the customers.

16 The kinds of things that makes successful service,
17 opening a door, a personal greeting, free delivery, notice
18 of sales, other events, all of those involve some tradeoff
19 of privacy in order to achieve that service. That is
20 probably unexplained. It is unconscious and yet it's
21 acknowledged by the consumers in the transaction.

22 And trying to formalize that in a way that could
23 be explained, whether it's on a screen or in a curriculum,
24 is extremely difficult.

1 I mean, if you go back 100 years, you were making
2 a -- this is important because of the discussion of
3 anonymity that came up this morning.

4 If you were back 100 years in a cash transaction
5 at a drive-in store, it's likely that the owner knew who you
6 were, he knew what you were purchasing, over time he knew
7 the pattern of your purchases, and frankly used that to
8 achieve a certain level of service, to say, "Mrs. Jones, are
9 you running low on flour?" Because he has seen the kind of
10 purchases you made.

11 That same use of data for service exists today,
12 and most businesses would be very surprised to hear that
13 their use of data in that way changes simply because they
14 move online.

15 Now, admittedly, consumers may not know -- we
16 pointed out earlier -- that this data is being collected.
17 And so we have to come up with mechanisms for filling in what
18 is a relatively small and temporary information gap.

19 MR. MEDINE: If I --

20 MR. DUNCAN: If I could have just one more moment.

21 The Commission has been criticized a lot in the
22 eighties for the permanent hair dye case, and this is a case
23 that individuals hadn't been told that the permanent hair
24 dye would not permanently change the color of your hair.
25 But what you were dealing with there was really an

1 informational problem. What you are dealing with is the
2 fact that there was something, it was a new technology, and
3 consumers did not understand how this technology worked.
4 But you did not need a permanent solution.

5 So what we really should be talking about now is
6 some sort of information -- is some sort of information that
7 can get the information out on a limited basis and then the
8 normal market forces will take over from there.

9 MR. MEDINE: Thanks.

10 Bob, did you want to --

11 MR. SMITH: I would like to distinguish, if I
12 could, educating consumers who are Internet users about
13 Internet uses of information about them. That's a lesser
14 challenge than educating consumers who are not on line about
15 Internet uses of personal information about them. Those are
16 two different challenges. The second one is much, much more
17 difficult.

18 The first one is difficult enough because it's
19 been shocking for me that a lot of sophisticated Internet
20 users were not clear about monitoring the news group, and
21 were not clear about cookies, they are not clear about how
22 Internet usage is monitored and the like.

23 But it's very important that we not limit consumer
24 education only to Internet users. And I want to point out
25 that PICS and the privacy screen do not answer that larger

1 constituency at all. That's extremely important to keep in
2 mind.

3 Secondly, I want to point out a Washington
4 phenomenon that I think everybody ought to be aware of. In
5 my experience it's been representatives of companies don't
6 know what their own companies are doing. And so I think
7 consumer education has to begin at home. I would be happy
8 to educate company representatives about what their own
9 companies are up to. They are always surprised and shocked
10 when they discover in fact that there are some things going
11 on in their company that they hadn't know about.

12 Bankers will tell you that they never share
13 information. Credit bureaus will tell you they have never
14 been hacked ever. Hospitals say that the law requiring
15 confidentiality, and we have never had a breach of that.
16 And I don't know about trade associations. I mean, some are
17 more actually in touch with what's going on than others.
18 Some of them, you know, even a level removed from what the
19 companies themselves know about. So I would say consumer
20 education has to begin at home.

21 I would like to thank the commissioners and the
22 staff for sticking this out. From my experience in this
23 town, we are usually talking to empty tables and empty
24 chairs about mid afternoon, and I very much appreciate your
25 sticking with it. I hope it's been helpful.

1 MR. MEDINE: I thank all the panelists who have
2 endured throughout the day as well.

3 Let me call on three more folks who asked for
4 attention; that is, Marc, and Steve, and some final remarks.

5 Yes.

6 MR. ROTENBERG: Well, I just wanted to say
7 something in the spirit of where do we go from here. And I
8 guess in some respects to raise a question about something
9 that both Bill and Jerry suggested, which I think is a
10 little bit unfortunate.

11 This sense that, you know, the privacy issues,
12 we're going to have, you know, the privacy extremists on the
13 one end and, you know, the industry extremists on the other
14 end, and the sensible people and the people that we like to
15 spend time with in the middle. I think that's really
16 unfair.

17 I think what we are seeing increasingly, certainly
18 in the privacy world, we can work with industry groups that
19 are not only against government regulation, they are against
20 government, truly, and they would like to see technical
21 solutions that avoid any need for government regulation.
22 And from a privacy perspective, we would say great. If
23 those solutions can be made to work, if they can be made to
24 work, you know, let's explore them.

1 And I think what we are going to see in the future
2 is not a division along this spectrum that Bill and Jerry
3 have suggested, but a very different division. A division
4 between those people who believe that the current system
5 basically works, that it may need some minor tweaking, some
6 notice online, some consumer education, and another group
7 which believe we need privacy protection equal to this
8 technology; that is, as bold, as creative, as
9 entrepreneurial, as forward-looking as the technology that
10 we are designing.

11 I mean, Thomas Edison said, you know, what man
12 creates with his hands, he should be able to control with
13 his head. And I think it's in that spirit that we need to
14 go through with. And you are going to see in the second
15 camp privacy advocates, industry groups and governments that
16 are going to proactively try to protect privacy, because it
17 is good for everyone. And you are going to be seeing
18 hanging back in the first camp the people that are going to
19 say, well, we just need to get out another code of fair
20 information practices, do another consumer workshop, and
21 that will take care of the problem.

22 And I think the reality is at the end of the day
23 the second camp will prevail, and the reason is that privacy
24 is not a consumer issue. In the twenty-first century it
25 will be the consumer issue. Privacy will be to the

1 information economy what consumer safety and product safety
2 has been to the industrial economy. And if you don't
3 understand that, about where we are heading, you really
4 don't understand what is going on out there. You cannot
5 have an information economy unless you have privacy
6 protection. The system will collapse.

7 MR. BURRINGTON: David, I need to respond since my
8 name was brought up, if you don't mind.

9 MR. MEDINE: Very briefly, 20 seconds.

10 MR. BURRINGTON: Twenty seconds, 17, 15 -- very
11 briefly. I just want to -- I think you mischaracterize a
12 remark that I said earlier. In fact, I was really saying
13 what you just said. We at least speak on behalf of the
14 online Internet industry, we get this, and we understand
15 exactly what you mean, because it's in our best interest to
16 understand that, if this medium is going to grow as a global
17 medium, and it's going to be a robust amount of commerce and
18 activity, and make this truly a mass medium. I was really
19 responding to your five points this morning that I think did
20 characterize this as -- this group as the stock group, and I
21 wanted to point out that there is a middle ground, and I
22 think that's what we are trying to do here.

23 MR. MEDINE: Well, we appreciate that everyone is
24 willing to sit at the table today and assess it.

25 Connie, if you could just --

1 MS. HEATLEY: Connie Heatley, from DMA.

2 I just want to add my voice to our commitment to
3 education. We see it as our mission to educate both
4 businesses and consumers. I have brought lots of show and
5 tell about the kinds of things that we have done together
6 with the FTC, with the Postal Inspection Service. We have a
7 web page up that has both our privacy policy, which is an
8 example to businesses about how to do it, and it is
9 connected to the commitment that we have made. And also, we
10 have consumer protection information out there.

11 We would like to move forward in working with any
12 organization that is interested in doing this, and we have
13 begun that process, certainly with CDT. We have had
14 elementary conversations with CME, and we would like to move
15 forward in the area of education.

16 MR. MEDINE: Well, thanks, and the last word of
17 the day goes to Steve.

18 MR. COLE: I am Steve Cole with the Council of the
19 Better Business Bureau. Thank you, David.

20 As an advocate for self-regulation and as a former
21 state consumer protection regulator, I hear two different
22 views of the world, especially this morning. I heard about
23 PICS and cookies and I/PRO codes and whatever, and I heard
24 Shirley talking about clicking 12 o'clocks on the VCRs. We
25 heard a lot about consumer choice, empowerment and even a

1 market. David, we talked about this even in your office,
2 setting up a market of people to compete on privacy
3 policies.

4 By word of caution, I wish I had solutions and not
5 just problems as the last speaker, consumer choice won't
6 work if it's too complicated. It simply won't work. It has
7 to be simple. Consumer choice isn't going to work if the
8 choices are too plentiful. If we turn this debate into a
9 supermarket, needing really great expertise to sift through
10 the different choices that are available, the choices may
11 turn out to be illusory. So we have to think of how to
12 present that also.

13 And also, consumers must understand the
14 consequences of their choices if their choices are really
15 going to empower them. And ultimately I hope all of us who
16 are working in this area, and particularly the experts here,
17 need to think of this average consumer who is going to be
18 with the \$250 Smart telephone or the \$500 Internet only
19 computer, it's not going to be all of us who us play online
20 every night, that's going to change. And that consumer
21 won't be helped unless they understand what may happen to
22 them, the benefits they will receive from information
23 sharing, and why informed choices will help them in the long
24 run as well as the short run.

1 You need tough standards, they need to be simply
2 stated, and they need to be graphically demonstrated.

3 MR. MEDINE: Thank you, and some final words from
4 Commissioner Varney and Chairman Pitofsky.

5 COMMISSIONER VARNEY: David, I want to echo your
6 thanks to everyone for coming and sitting at the table.
7 It's not often in Washington that you get such a diversity
8 of opinion at one table, having what I thought was a rather
9 challenging, yet extremely civil conversation about these
10 issues and where we go.

11 My question is where do we go? And I think I see
12 a couple of things. First of all, we are going to leave the
13 record open for a couple of weeks. I mean, we are going to
14 leave the record open for two weeks, and we have asked some
15 questions during the day, and we have asked you all to
16 submit your thoughts and comments on the record over the
17 next couple of weeks. I would ask you in your thoughts and
18 comments to address the question of where do we go from
19 here.

20 Secondly, I think that there will most likely be,
21 and I will certainly talk to my colleagues on the Commission
22 and the staff, there will be a staff report that will come
23 from this hearing, I hope, and in that staff report possibly
24 we will see recommendations to the Commission about further
25 action.

1 There were several people here today from Capitol
2 Hill. There will be several people here tomorrow from the
3 Hill, from both the Senate and the House side. And there
4 has been some expression of interest in a report to the
5 Hill. There has also been some expression of interest in
6 preliminary hearings after the recess, when they do come
7 back, on privacy on the Hill. So we will see what happens
8 there.

9 Finally, for the future Commission action, I think
10 that it's important for all of you to remember that we do
11 have ongoing enforcement authority and ability. And when
12 you find issues that you believe are clearly fraudulent and
13 deceptive, you need to let us know. You know, this is an
14 area that we are all struggling in. We are all trying to
15 protect the integrity of the medium, and we have a role
16 there to play, and we can only play it when we know what's
17 going on.

18 But when we separate out what we have identified
19 off and on during the day as kind of the two questions, one
20 is information collected about consumers who may not even be
21 online, who are not in the transaction; that information
22 moving around the Internet, being bought, being sold, being
23 put to different purposes, I think is a very serious policy
24 question that our staff ought to take a look at, and create
25 a record on.

1 The second question, when consumers go online,
2 whether it is for a transaction or pre-transaction, what is
3 the responsibility of the web site that they are going to to
4 disclose what they are doing with information, what are the
5 technological solutions that consumers can employ to empower
6 themselves to make choices, and what is business's
7 willingness to commit to make that a reality?

8 I have heard everybody at the table today say we
9 can do it, we can do it, it can be done, it can be done. We
10 will do it.

11 Well, I would like to talk to my colleagues and
12 invite you all back in maybe six months and let's see if
13 you've done it, because I don't know where we are going to
14 go if you don't get it done, and if it doesn't work. We
15 have heard a lot about what we need to have in place to make
16 these technologies work and we have also heard from all of
17 our friends at the table.

18 If they don't work, we will need to take the next
19 step towards looking to solutions, and I don't know what
20 that is, but I for one would like to see the entrepreneurial
21 spirit that has characterized America's success in the
22 global economy work here as well.

23 CHAIRMAN PITOFSKY: I think the bases have been
24 touched. It's been a fascinating day. I am happy I was able
25 to be here. I know there are very provocative issues on for

1 tomorrow, and I look forward to more discussion of these
2 questions.

3 MR. MEDINE: Thank you. We stand in recess until
4 tomorrow morning.

5 (Whereupon, at 5:10 p.m., the workshop was
6 recessed, to reconvene at 9:00 a.m., Wednesday, June 5,
7 1996.)

8 //

9 //

C E R T I F I C A T E

DOCKET/CASE NUMBER: P954807

CASE TITLE: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON
THE GLOBAL INFORMATION INFRASTRUCTURE

HEARING DATE: June 4, 1996

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: June 4, 1996

SIGNATURE OF REPORTER

Peter Knight Shonerd
(NAME OF REPORTER - TYPED)