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

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 PITOFSKY, 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 LANDESBERG, Bureau of Consumer Protection
JANLORI GOLDMAN, Deputy Director, Center for Democracy and Technology
LINDA GOLODNER, President, National Consumers League

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 LANDESBERG, 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

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 LANDESBERG, 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

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 LANDESBERG, 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

APPEARANCES: (Continued)

SESSION 5

MARTHA LANDESBERG, 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

P R O

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

privacy questions that implicate several consumer protection concerns.

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

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

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

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

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

David.

MR. MEDINE: Thank you, Chairman Pitofsky.

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

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

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

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

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

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

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

information. Again, people will be wary about taking risks

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

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

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

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

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

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

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

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

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

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

That's our demo.

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

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

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

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

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

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

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

Thank you.

MR. MEDINE: Thank you, Janlori.

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

(Laughter.)

MS. GOLDMAN: You will have to link to the anonimizer which I forgot to mention. You can link to the

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

MR. MEDINE: Thank you.

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

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

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

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

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

Okay, stop here. That long and awkward looking

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

We don't have a nice law enforcement act. You go at it a different way. We try to obtain the same ends through education, peer pressure, and a self-imposed process that we believe the system works, and will continue to be

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

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

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

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

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

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

request that their name not be transferred to other entities.

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

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

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

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

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

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

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

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

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

MR. MEDINE: Ron?

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

I just wanted to add one thing because I think this discussion about the privacy system that we have in this country and information about privacy, we have legislated in this area, and probably one of the few cases where law has preceded technology. In 1988, I think it was in 1986, I guess, the Congress enacted The Electronic Communications Privacy Act, and ECPA really was enacted

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

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

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

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

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

MR. ROTENBERG: That's Rotenberg.

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

Mr. Rotenberg.

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

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

there, and we are going to very soon, and what is happening

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

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

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

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

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

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

MR. MEDINE: Thanks.

Alan?

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

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

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

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

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

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

And that if we see how that shakes out, there may be a point at which the FTC or legislation would come in to

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

MR. MEDINE: Thank you, Bob.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Thank you.

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

So, first Janlori and then Ron.

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

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

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

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

There has been, again as David says, lots of

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

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

MR. MEDINE: Ron.

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

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

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

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

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

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

wouldn't have that continued authority, and I think that is

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

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

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

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

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

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

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

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

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

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

MR. MEDINE: Ariel.

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

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

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

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

MR. MEDINE: Thank you.

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

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

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

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

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

But I think there is a very real danger that if this market starts with a taint, that that potential is never going to be reached. And I think that one of the telling things statistically is to know the difference between those who have computers, which are now bought and sold like refrigerators, or the VCR that goes 12, 12, 12. The access which is tremendous, and the actual number of

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

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

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

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

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

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

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

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

MR. MEDINE: Thanks again.

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

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

MS. SARNA: It's another problem.

MR. ROTENBERG: This is the first panel. We are

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Whereupon, a recess was taken.)

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

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

Before we get started with our first demonstration, John Kamp didn't get called on at the last

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

So I only start with that because I think that many of the forces are here. I see Dan Jaffe and myself representing CASIE, an organization that has developed a set of goals on privacy for advertising in the advertising community, the Interactive Services Association, DMA and others, the organizations that need to focus on it, because

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

Thank you.

MR. MEDINE: Okay, thank you.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

So if the consumers say, well, if I were to send a complete set of information, obviously I would get a customized page that says the material, and they can know

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

So thank you.

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

MR. HARTER: Thank you and good morning.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Also, for those of you who access the Internet over low speed connections, waiting for the main home page to download and then find that little link at the bottom of the page, "click here for the plain text version." Imagine if the filed indicated to the server that you only wanted

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

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

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

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

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

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

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

Unfortunately, if member states of EU can opt out of the privacy Directive under the provisions of national security, public security, then I propose that French legislation, which is going to implement a trusted third

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

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

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

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

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

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

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

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

Now, is PICS useful in the privacy domain? We believe so. That's why we are here. It's a labeling technology. You have to extend it somewhat in order to use it in the privacy domain. However, just as in the rating

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

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

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

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

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

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

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

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

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

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

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

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

(Laughter.)

The parent says, "Sure."

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

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

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

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

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

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

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

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

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

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

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

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

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

want the organization to take responsibility, but it's okay

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

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

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

So this is a, I think, promising technology. It is certainly worth exploring. The big idea here is that if we put the notice into some standard format, and allow people to express their preferences, the software can

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

What would it take to ge this going? I think there are three issues.

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

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

The second issue is who is going to actually create the labels. In the indecency realm, the Simon Weisenthal Center can go out and find neo-nazi material and

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

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

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

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

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

Now, these sorts of things to maintain consumer confidence, as I said, are a cooperative effort. When I

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

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

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

That should be backed up by the technology. We

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

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

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

Now, self-regulation is about effective change. I

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

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

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

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

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

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

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

MR. MEDINE: Thank you.

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

Dan.

MR. WEITZNER: Thank you, David.

I am Dan Weitzner for the Center for Democracy and Technology, and you can see what happened to me. I have been working on first amendments issues for the last year

process comment than anything else, and get back where Al Vezza left off.

That less than a year ago the technology that Paul Resnick showed was even before vapor-ware. It didn't exist.

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

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

Thank you

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

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

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

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

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

Another benefit is that PICS is global in reach, and I think that one of the things we need to consider very carefully when we look at rulemaking in this country is that

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

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

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

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

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

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

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

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

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

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

MR. MEDINE: Commissioner Varney.

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

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

From our friends who are the privacy experts here, if we pulled out that other side of the issue, those merchants that are engaged in the collection and resale of your personal data without your knowledge or consent from this discussion, does that make a difference? If we were to approach that problem differently than this problem, if we acknowledge the dichotomy that we have just outlined, does that -- what does that do to PICS or other technologies

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

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

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

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

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

community on this issue. That generally in the past the advertising community, the agency community, the direct marketing community were very separate communities. What has happened here is that the whole business community has come to say that privacy is a very important issue, and that everyone of us has come forward with guidelines, goals, statements as to the protection of privacy. In other words, there is a convergence between the whole advertising community and the direct marketing community because on the Internet every advertiser basically becomes a direct

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

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

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

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

COMMISSIONER VARNEY: So presumably PICS would work.

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

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

MR. JAFFE: Our associations who --

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

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

COMMISSIONER VARNEY: Is it six months?

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

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

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

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

help marketers service them more economically and effectively.

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

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

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

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

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

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

Now, the other thing here is, in terms of maximizing choices, we should not forget that one of the choices that has to be available is anonymity. And anonymity requires the development of cryptography. And it really burns me if someone who, you know, my lines go back

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

MR. MEDINE: Al.

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

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

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

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

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

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

Joel.

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

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

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

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

I think the real issues in PICS privacy will come from a couple of places. One, there may be instances where we decide that certain privacy interests or rights are

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

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

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

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

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

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

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

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

MR. MEDINE: Thank you.

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

Daniel?

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

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

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

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

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

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

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

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

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

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

Bob Smith.

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

Does call blocking take care of all the issues,

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

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

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

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

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

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

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

I am troubled by quickly importing OECD standards, European Union Directive standards, even Canadian Standards

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

MS. GOLODNER: I agree with Alan.

MR. MEDINE: Use the microphone.

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

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

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

MR. MEDINE: Okay, thank you.

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

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

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

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

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

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

Imagine a telephone company that would say tomorrow to consumers, "We're going to cut off that dime a minute rate, and that lady who is always talking about dine a minute phone service. We're going to give you a nickel a minute phone service, and you can call anyone you want for five cents a minute. We're going to keep a lot of information, by the way, about your calls, and if there is

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

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

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

Steve?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Now, again, we are talking theoretical here, but the possibility of alleviating the burden that we currently have in an information-based world, the burden is on individuals to constantly ma

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

MR. HARTER: Maybe.

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

(Laughter.)

MR. HARTER: My father is an engineer and he hates the blinking. He puts tape over it. But bear in mind he's a computer engineer, has been programming mainframes since the late sixties and works for EDS. So he's very technical, but you don't use a VCR to tell time. You have a watch, you have a clock on the wall. The clock on the VCR is so far

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

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

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

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

MR. MEDINE: Okòi, let's leave encryption to a brief comment because that's not our mòin purpose.

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

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

Thank you.

MR. MEDINE: Al?

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

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

PICS technology is policy neutral. That is to say it is not

Canadian Standards Association-based rating, or the old 1970s HEW-based rating system. In fact, all of those three, and I don't agree with your categorization of each of these. I think all of the three share the same basic set of

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

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

You can have self-identified labels, the EPIC label attached to it, and you may have some third party organization with -- in this instance the cooperation of whoever the originator is, some sort of cooperation that says we have looked, we think that they are conforming to

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

Two quick things. One is somebody suggested that companies like I/PRO, that PICS would really thrive with the privacy regulation. I believe we are thriving without it.

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

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

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

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

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

Daniel, Marc and then Paul.

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

I just want to address the issue that was talked

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

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

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

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

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

//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//

A F T

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

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

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

Professor Westin.

MR. WESTIN: Thank you, David.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

As far as the health information, to take another example, a lot of people are revealing a great deal of information about themselves today in forums, chat rooms and other organizational settings where persons with muscular dystrophy or persons with AIDS want to chat and talk and communicate about themselves and their conditions. So that

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

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

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

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

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

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

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

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

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

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

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

a similar product about larger business from the same database.

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

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

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

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

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

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

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

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

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

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

MS. KOEHLER: Thank you.

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

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

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

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

What can a Smart Card do that a -- pardon the expression "a dumb card" can't? That is not to say what

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

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

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

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

A Smart Card can enable several providers to offer a common application. Stored value cards enable consumers

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

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

What are the issues? I will suggest a few.

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

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

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

Thank you very much.

MR. MEDINE: Thank you.

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

Is there anyone who -- Marc?

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

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

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

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

I would li 0 TD3.nsww.0198 bort atüme(5[63) Tj -36uia (7e

Let me give a commonplace example. Your monthly

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

(Laughter.)

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

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

MR. MEDINE: Bob.

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

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

Now, that is not to say that a consumer can't give out information voluntarily through questionnaires, through compiled lists, et cetera. And in those situations I believe the appropriate process should be that at the point that that sensitive medical information is voluntarily

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

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

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

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

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

Bob Smith?

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

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

As well, my digitized photo image. Think of the ways that can be altered and cut and pasted without my knowledge. I think many people would respond to the survey

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

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

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

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

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

When you think about what we are considering, we

results or following up in terms of complaints with medication.

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

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

So certainly the provider community right now is very troubled in terms of the fact that, you know, there is a lack of security, and the fact that many organizations do

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

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

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

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

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

MR. MEDINE: Thanks.

Robert.

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

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

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

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

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

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

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

MR. MEDINE: Bob.

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

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

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

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

MR. HENDRICKS: Well, I think that so far the panel has been very excellent in being representative, but I

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

There have been efforts in recent years to pass a federal bill that would protect peoples' medical records that incorporate a number of the principles that we are talking about here at this table: access to records, a

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

And I think that that is a fundamental sticking point. We have been at this for a couple of decades not, not me personally, although it feels like it. But there are people in this room who have been at it for a couple of decades and it's been a very discouraging, and I think in

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

A number of years ago I met with some managed care company who was looking at how they should put privacy rules in place for how personal health information was handled,

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

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

MR. MEDINE: Thank you.

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

Andy Strenio?

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

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

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

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

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

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

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

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

MR. MEDINE: Final word, Marc.

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

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

Now, Kawika has suggested in the financial world there is a risk of anonymity, and that is that it reduces accountability which, of course, banking and financial

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

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

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

will be no one there on their side to say you really shouldn't have to give that information out.

MR. MEDINE: I want to thank the panel very much. I think Marc left us on just the right note, which is we have a lot to think about in this area, which we will continue to do.

We are going to take a very quick five-minute break to switch over the chairs for the European Union session.

(Whereupon, a recess was taken.)

MS. SCHWARTZ: The topic of this session is the impact of the European Union's Directive on the protection of personal data. Now, this is a subject that has been coming up off and on throughout the day, and David has told you that we can talk about it later, so now is the opportunity.

The format that we have used up till this time, we are going to start off with some presenters, crystallizers. The first crystallizer is Joel Reidenberg, Associate Professor at Fordham University School of Law, where he teaches a seminar on information technology law, and global networks, and he has written widely on this field.

So I will turn it over to Joel who is going to speak from the podium.

MR. REIDENBERG: I guess I would like to start by commending the Commission for including this topic, which is quite different from the United States. Here in the U.S. we have heard already a discussion on some of our rights, self-regulation, the importance of practices, what's happening in the marketplace. -- what the regulate looks at a wide range of confirmation practice activities. Thirteen of the 15 European Union countries -- some of the things we tend to connotate with privacy in the United States, confidentiality concept traditionally spoken for the U.S. -- because faced with the situation -- the Directive went from draft -- changes were taken place in the union. The master came into effect -- in the context of free flows and free movements of information.

The Directive itself in its final form is designed to elaborate principles, and not to be technology specific or system specific. It was designed to set the framework, referred to as the framework directive. There are separate specific directives that are at least in the works. There is one in ISDM that is still -- I understand it's supposed to have a common position come out some time this month, So it is expected that there will be more specific directives targeted at particular applications.

The framework directive contains a set of substantive rights. And most of these are -- the core is

contained in Article 6. They require that the member states of the European Union enact national laws that include principles of fair and lawful collection of personal information, personal information which only should be collected for specified purposes. It should only be used for purposes -- for compatible uses to those specified purposes. It requires limitations on the collection of extraneous data, durational limits. You shouldn't keep data longer than you need it for the specified purpose. There are accuracy provisions in that individuals must be given

authority, data protection agencies. And certain data processing activities will have to be reported to the data protection authority.

For perhaps our greatest concern today is the Article 25 provisions, which mandate that European member states prohibit transfers of personal information to destinations that do not have adequate privacy protection. If the destination has insufficient privacy protection, data flows are supposed to be restricted.

Article 25 doesn't really establish very clear methodology or answers to what constitutes adequate. That is left vague for the moment, and we will be hearing a little more about that later.

If the destination country does not have adequate

from each of the supervisory authorities in the member states, which are the data privacy commissioners. And they are to assist the Commission in determining countries that

Thank you for the introduction, and as did Joel, I commend the Federal Trade Commission for convening what I understand is a sell out, sell out crowd, and I understand the overflow room has overflowed, which -- the lady doth protest -- I think it speaks to the importance of the topic and the timeliness of it.

I guess the question that keeps being asked is when does the spigot get turned off. Is it going to go from a solid line to just drips? Is it going to be a steady dribble? In our perspective, perhaps the spigot won't be turned off at all, and I will show you why.

Let's look at just one of our companies, Dun & Bradstreet Information Services, who are in 39 countries outside the United States, dating back as far as 1857. And in those 39 countries 27 have some form of data protection laws in place now; many of which have transported data flow restrictions, requiring either equivalency, adequacy as in contractual measures. So this is not a new issue.

In terms of what is the underlying issue in data protection, Joel talked about the context of data protection versus privacy. The underlying issue is balancing human rights issues versus societal needs for really creating a framework of protection for an information society.

The global information of Dun & Bradstreet, Bob Merold talked about one of our current companies, IMS in the health care area. I am just going to talk specifically about one, and that's in the business information area.

We capture information on over 40 million business establishments worldwide, and it includes everything from corporations to sole proprietorships, information about who the principals are from the directors, the owners, the

business characteristics and some information about the business performance. But one important point, just so that there is clarity, we are not in the business of capturing consumer information or doing consumer credit reporting. It's business information, and that's a very, very important distinction.

In terms of what our practices are, what do we do in our handling of information? Just as an opening point, everything you see we do voluntarily. We don't do it because the United States, that there are laws that say we have to. We do everything that you are seeing voluntarily.

One is notification about a business report. We tell the business principal when a report is created about them, or when there is a full update to the report involving information that the business provided to us.

Second is that there is an access and correction procedure. Third, there is an ability to stop marketing use. Where our information may be used, it's captured for the purposes of business credit purposes. If a business does not want their information also disclosed to a marketing list, the business to business marketing list, there is a very comprehensive process for taking their names off.

And then, finally, in our environment we have a contractual commitment with customers. The contractual

commitment limits uses, it limits who uses, but most importantly, and this is something I would underscore, is that in our agreement makes reference to obligations on the user with respect to both U.S. and foreign laws, and that's an important point, and I think Joel will cover some additional aspects of this as far as U.S. practices in compliance with third country laws.

Who gets trained? It's really everybody. There is comprehensive training for the people who collect the information. There is training for the people who handle it and data entry. There is training for the people who sell it, and then there is training for the people who actually use it. And just as a prop, this is the documentation that covers those four segments. This is not just blank paper. I didn't grab a stack of -- but if somebody wants to look through this, I can't let you have it because of it sensitivity, but this is how comprehensive what you see is.

There is also one other constituent that we train and that is our shareholders. In our annual report we have a statement on our business ethics, but also at the bottom on data privacy, and it specifically tells our shareholders how we are spending their money on issues involving the use of security and information accuracy.

So why do it? And I made the point if nobody is telling us to do this. We do it because in our judgment

it's good business and it's a necessary business. We live in an environment of a very voluntary system. The information that is provided to us is provided voluntarily, and it is dependent upon the confidence and trust of the data providers.

Data quality, a point about getting it right first, and why accuracy is important, and accuracy is best measured in terms of the data collection.

And then finally, in our judgment, good practice equals good continued cooperation. Somebody once said we could probably increase our customer base by 50 percent and reduce our information base by 66 percent, if we were selling information to people that our data subjects didn't want us to sell it to.

And also an important point is to anticipate what is ahead, because ultimately with the EU Directive the laws would be determined by the laws of what we call the controller, meaning the German -- each country will implement national laws, as Joel said, and therefore it will ultimately be the German law that dictates transported data flow issues between Germany and, for example, the United States.

I guess the final point I would just make as a parting thought is it's the right thing to do.

Thank you.

MS. SCHWARTZ: Thank you. We are going to invite Joel back to the microphone.

MR. REIDENBERG: Okay, I think I will do it from over here this time. It's a little easier.

MS. SCHWARTZ: Fine.

MR. REIDENBERG: What I am going to do now is address more specifically the U.S./European Union comparisons. I think Gary's presentation is a good illustration, certain background of how we can look at comparisons between what happens in the United States and the European Directive, which is the mandate.

Whether we li res8 -

has authorized the Michie Company to publish it in the United States. So that will be out.

But that's not the only aspect. The Commission is getting information about what will be happening, not just in the U.S., but abroad. They have an ongoing study right now looking at the methodology for determining adequacy. It's expected to be completed, I think, some time in the fall. They are about to start a study on interactive services and online privacy. They just closed a bidding process for that several days ago.

The working party of the member state commissioners has now, they have now had two meetings, and they too are preparing their thoughts on criteria for evaluating foreign countries.

And I guess I should point out in terms of how the U.S. fits into this, at their very first meeting back in January, Professor Schwartz and I were asked to come and discuss our study with them. So they were particularly interested in information about what's happening in the United States.

In looking at the U.S. particularly, I'll focus on the private sector, which is the area that I worked on for the study. One of the conclusions or arguments that we made is that context is critical when you are trying to determine whether or not you have adequate data protection in the U.S.

I think if you ask the question is there adequate U.S. law under the European standards, the answer there is no. Is there adequate date protection in the United States? I think the answer there is maybe. And the reason that I say that it's maybe is what we find is our targeted rights. We have targeted rights. But implementation then becomes critical to figuring out whether or not we match up. And we find in the private sector cases where -- we saw some examples of what one global company is doing. They are operating with global privacy principles that conform to the various laws in the countries in which they operate. And you can find examples of companies with excellent practices,

Secondary use of personal information, is the information being used for purposes that are compatible with those that caused the collection. And I think this has been historically particularly problematic for marketing uses in the U.S.

And then the third area that I think will come up is the enforcement area. The European standards are very keen on enforcement and supervision; that there be oversight and independent supervision, and that's something that is very hard to find and replicate generically in the United States. We can always point to specific areas where we do find it, we do see specific instances particular enforcement powers. But overall we can also point to plenty of areas where we don't.

I think that this suggests two global consequences for us. One is in the absence of U.S. laws, and the second area is in the absence of a data protection office in the United States, in the U.S. Government.

In terms of law, the absence of a U.S. law, I think, will mean that consumers will have higher levels of data protection consistently abroad. So if an American is surfing on the Web in a foreign site, in the U.K., in Germany or in France, what happens to the click stream if it is resident on the foreign site will be more consistently

matched with information practices than what would happen in the United States.

There will be, I think, as a result of that, transaction costs for dealing with privacy in the U.S. Therefore, U.S. companies, there would be increasing scrutiny of U.S. information processing, because in the absence of a law, for a foreign regulatory body to determine whether or not there was adequate data protection in the United States they need to know what the specific company is actually doing. It won't be sufficient to just have a code of conduct or a trade association statement of policy. What will be important is what is actually taking place.

within the U.S. government places, I think, a very important burden on U.S. businesses, and I can point to recent examples of American companies doing business overseas where they have found that they have had to go and persuade data protection authorities that protections were fine, enforcement was fine for the activities they were doing. And they face skeptical regulators, because the regulators have no U.S. government counterpart to point to.

The second consequence is that foreign data protection agencies will be setting the global policy agenda in the absence of a powerful U.S. voice. Presently, the foreign data protection commissioners get together several times a year. They have an annual conference where they all

with countries or sectors within countries as a whole, the absence of any central office in the U.S. will pose a practical negotiating problem for them.

Recently, European Union officials have come -- made visits here to the United States, and I would say within say over the last year I have been asked at least a half a dozen times by different foreign commissioners, when they want to make a visit to the U.S., who should they talk to, who is the right person in the U.S. Government to talk to the commissioners. And whoever the right agency was seven months ago is not the right agency -- not necessarily the right agency today.

particular solutions. We will see -- there will have to be practical solutions worked out.

I think the second point is that foreign pressures will force fair information practices on the United States through both legal and extra-legal means. And for the moment I think that's going to be forced on foreign ties, because that's where the more consistent, broader view, comprehensive view of data privacy is being mandated.

And then I guess my third, I will come back, I think we really need some sort of U.S. Government policy center to be able to advance the sorts of discussions that happened here today as well as the international dialogue.

MS. SCHWARTZ: Well, I have a very long list of issues that your comments generate. I want to turn first to Ron Plesser who I spoke with earlier about kind of reacting to the presenters, and giving us his views either directly addressed to Joel's comments, or otherwise.

MR. PLESSER: Well, let me very quickly say that Gary's presentation was terrific and demonstrates, I think, how self-regulation works, and how companies can respond to both market and regulatory demands without being subject to regulation or control, and I think that is a good example.

Turning to Joel, it was just so much and excellent, although I finally found something that I really very much disagree with Joel. We usually just -- we usually

just look at the picture, and I say it's half full and he says it's half empty, and we are both right, but it's a different perspective.

suspect that it compares favorably to what the Europeans are now suggesting to do on a directive.

Secondly, we do have ECPA, we do have the Fourth Amendment, we do have wire tap controls. We have controls on how information is used in storage. These are not academic questions. I counsel clients where European authorities have tried to get access in e-mail storage, and, frankly, if it's deposited in the United States, generally they have gone away because the answer is that they have got to go to the department, they have got to get a valid subpoena from their country of origin. They have got to go to the Justice Department. They then have to get a corresponding subpoena, and then it has to be served -- or a warrant, and then it has to be served in the United States, where in France, as I understand it, the captain of police can sign an administrative order, and all of your information can be obtained.

There is a difference in focus, and I think we really make a mistake if we get defensive about our laws or be convinced that somehow we are inadequate or secondary to the Europeans. We have focused historically on a different issue.

In terms of the transport of data flow issue and the impact in the United States, I think if what Joel says is right, that would be fine, or at least that's a start.

The Europeans, as I understand it, are not satisfied with just the point of presence for contact. The State Department has done that. Now maybe the CIA will do that. What adequacy is, at least as we hear it, or the question is whether or not there really needs to be a U.S. data protection commission with regulatory authority.

And I think today is a wonderful example of how we have regulatory commissions who work on substantive issues like unfairness and issues like that, will follow those issues where they go, will create privacy guidelines and debates, and really we don't need another agency, an independent regulatory agency on privacy. The Federal Trade Commission, the Trade Commission, the Securities and Exchange Commission are looking at some of these issues. This is really the way to go, and then perhaps the government -- I do agree with Joel that there should be more of a centralized policy within the government, but that's not what the Europeans are looking for. The Europeans are looking for enforcement.

The other issues, and let me just end with this, is everybody talked about data commissioners, and, you know, that that's necessary, or may be necessary for adequacy and the other issues. One of the elements of the European Commission -- two more points -- one of the elements of the European Commission is data registration.

Well, when we talk to the European representatives they all say, well, of course we don't mean that. We don't want you to do data registration. Well, why not? I mean, data registration is just as much an element of the European Directive as the privacy commission is or the enforceability rights. And so the question of this kind of picking and choosing is somewhat confusing.

The other point that I do want to point out, and I would like Mari Ann Blatch to talk about it, because she worked very hard on it, that in terms of the Directive in

I am with the Department of Commerce, and chief counsel of the NTIA, National Telecommunications and Information Administration, a part of the Department of Commerce.

And we are very involved in the issue of privacy as are other parts of the executive branch, as is obviously the FTC.

Last fall NTIA published a privacy report that

At the risk of being told that I am straddling the

One, because we are concerned that any effort to regulate the Internet right now might freeze the Internet or in some way interfere with its ability to continue to develop. It's an extremely fluid creative medium, and it should be -- and it's done wonderfully without regulation. And the trend in the U.S. right now, certainly in telecommunications, is toward deregulation. And so we shouldn't begin to regulate the Internet. Certainly not now, as we are deregulating other parts of the telecommunications market.

Second, we think it's premature to regulate in response to the EU Directive at this point. We are still at very early points in discussions with the EU. As Joel said, the EU is still defining what it means by adequacy, and its group is still working out what the various things mean. It's not clear how different provisions of the EU Directive will be implemented. I have heard the same thing that Ron has heard, that registration -- that transparency is more important than registration.

So I think we really need to be educating ourselves right now about what's going on in Europe and what the EU's view of the directive and how it needs to be implemented is. I think the U.S. Government needs to be educating itself about what the private sector is doing, and encouraging the private sector to do everything it can on a

self-regulatory basis. But I don't think this is the time to create any new bodies in the U.S. or to create any new laws other than the medical privacy law that I am aware is coming up now.

Thanks.

MS. SCHWARTZ: Thanks. Roger, will you intreslawno

The first is the extent to which national regulation can manage the protection or even contribute to the protection of privacy in an Internet environment, in a highly distributed Internet environment.

Others have mentioned earlier that the Internet is a global environment, and as such I think nearly all of us who have used it recognize that it is not difficult for a service provider to move from one country to another, or to relocate their service and facilities.

But by the same token, it's quite difficult for a national authority, whether it's the European Commission or a United States federal agency, to regulate the activities of service providers who can move quickly between national boundaries.

This, however, is not so much a problem, and not so much the case with dedicated and centralized private networks which are the main subject of European privacy directive attention.

And by the way, before leaving that, it's probably also worth pointing out that those highly centralized, highly managed networks today carry an enormous quantity of vitally important information. We haven't spent much time today talking about them because we have been spending a lot of the day talking about the Internet, but those private networks which the European privacy directive seeks to

regulate are critical to commerce and business in our every-day life.

The difficulty is that the regulatory framework that's used by the privacy directive is aimed at those networks, and not at the highly decentralized network or the Internet.

The second question is, which we touched on earlier, I think, in the discussion, about the role of technology and technology solutions. I think if there was ever a situation that will force an examination of how adequate regulatory tools can be in dealing with protection of privacy on the Internet, the effort by the 15 European governments to devise national legislation that implements this Directive as it relates to the Internet will be a perfect test case, because the -- the regulatory tool, as Brian Ek pointed out earlier today, is a relatively clumsy tool. It's slow to develop and even slower to change, but a detailed regulatory tool that's created under the preexisting structure that's aimed at private data networks is an even more difficult tool to use to regulate privacy on the Internet.

So I think, in conclusion, what I would say is that no one should miss the point that the European privacy Directive is a very, very important initiative on the part of the European Commission and the European governments, and

it will have an enormous impact on private data networks which are a vital part of commerce and our every day life. How it will relate to the Internet and the provision of services on the Internet is beyond most people's understanding, and certainly not an easy question for any regulator in the United States or much less in Europe to answer.

COMMISSIONER VARNEY: Teresa, before you move on, I think there is an important point here that I would like to get some clarity from the panel on. I have now heard today two sides of one position.

There seems to be a group of people on the panel who argue very vociferously that the EU Directive was created for, aimed toward, means to deal with large highly centralized databases.

There is another group on the panel that says no, that is not so.

Have I got that right? Panelists, is there a big debate in this community?

MS. SCHWARTZ: Let's ask Marc.

MR. ROTENBERG: I would be happy to defer on this to Joel, because I think his presentation was quite expert. But it's very important to understand how the EU directive came about as opposed to the European convention or the OECD guidelines.

The EU Directive came about because of the growing harmonization of the European Economy and an attempt to promote the free flow of information within the European Community. At its heart, this is an effort to standardize national, legal regimes.

Now, there are other interrelated directives, some of which address ISDN and some of which address network services, but I think that characterization would be actually a little bit misleading. It is not so much the big day-to-day 1960s model. It was, rather, to create an environment, and this is critical to understand the purpose, that reflects the commitment to human rights in this emerging economy of Europe.

And if I could continue to answer your question?

COMMISSIONER VARNEY: And I would be interested in testimony being submitted for the record on this point, because it does seem to me there is a lot of disagreement here about precisely what the EU directive is aimed toward and why it may or may not be consistent with the U.S.

MR. ROTENBERG: If I could continue.

MS. GOLDMAN: There is just one line in the Directive, I think part of the disagreement comes over what the Directive actually says, which is that it is meant to apply to the process of personal data that is automated or contained in a filing system structured to permit easy

access to personal data. And so they are fairly clear that

excellent. But I don't think it's perhaps quite fair to say, Gary, that part of the reason that Dun & Bradstreet has the very good policies that it does isn't related to the presence of privacy regulations in the different countries

conclude, if you even pick up this morning's paper and look at the front of the New York Times Business Section, that it is almost the opposite; that it is the United States due to the clipper chip, due to the FBI wire tap bill, through informal negotiations that are conducted not by our Commerce Department, but by our Justice Department, to expand the ability of foreign governments to surveil their own citizens. That is the cold, hard reality of privacy in 1996.

And it comes about, in part, because we do not have in place within the federal government an office that has tried to advocate privacy interests, whether they be in the private sector or the public sector.

So, I mean, my point is really not to so much disagreement with Ron. I mean, in 1986, the ECPA was very important for what it did. But what has happened since that point has been to, you know, set in motion forces that have served, you know, neither the private sector's interest or the citizen's interest, particularly when we talk about the development of international communication standards.

MR. PLESSER: Can I respond?

MS. SCHWARTZ: Very briefly. I have a line up here, and I am going to say the order in which people are going to speak. It's Mari Ann, Doug, Janlori and Evan.

So quickly.

MR. PLESSER: Thank God we have the ECPA. Otherwise that chipping away would have occurred with dispatch, and let us have the Europeans do something equivalent so that when we send our data over to Europe we know it's not open for government inspection.

MS. SCHWARTZ: Okay, Mari Ann. You should introduce yourself, Mary Ann.

MS. BLATCH: I am Mari Ann Blatch. I have been Chair of the U.S. Council for International Business Privacy Committee since we set it up. And I say "we," it was Reader's Digest, IBM, and American Express back in 1968, that petitioned our parent, the International Chamber of Commerce in Paris, to set up a committee on information policy, and particularly data protection laws, because if you are an international company you have to be involved in both the original private mainframe and then eventually the lease networks and now into the Internet, and we had an exchange of information there. How did we deal with the Swedish also? How did we get certified by the French law? How did we set up information officers in our German subsidiaries, et cetera?

That grew to a point where the business community petitioned the U.S. Government, the U.S. Council and others worked with the government back in the eighties and said, please go to the OECD. Please work to get privacy fair

information practices. Those principles, as Marc has said many times today, are well accepted worldwide. If you look at national data laws, privacy laws, information policy laws, many of them are still using those same principles. We are still talking about those same principles.

We are talking today, I think, there isn't a controversy, Commissioner Varney, I feel, because the original effort of the EU was to create a market and try to harmonize those laws which had to do with those situations at that time.

The U.S. Council for International Business has had many meetings with the EU since 1990, when the first directive was prepared. And in all of those conversations, with John Mold, the Director General of DG-15, he said we will work with international business. We do not want to cut off the free flow of information, but we would like to see that there should be an assessment in the light of all circumstances surrounding the data operation, the nature of the data, the purpose, the duration of the processing, internal laws, self-regulation laws. And we have had the, ICC and the European Commission have had a series of annual meetings. These were sponsored by the European Commission and by the ICC in Brussels starting in '94.

And at that first meeting we talked about alternative solutions, and that's where the idea of a

contractual possibility arose. But inside this private lease network you could have a sort of contractual protection and get security, your cryptograph. All the people that have been talking today about those kinds of protection, we're addressing those kinds of networks.

More recently, when John Mold was here a month ago, and met with a group of private and government agencies, and many of you were in that meeting, we talked again about how does he see the methodology that will be applied in the future, because in October 1998 they have to decide how they are going to apply it, and they are looking at that now.

And he told us that, number one, as Joel mentioned, there is a study out, and they will be looking at that in the working parties in September and December. But in the meantime, he said very clearly, "I can imagine," and he said this since 1990, the same thing, "I can imagine a sort of cocktail that could be made up of internal policies, rules, laws, regulations and a combination thereof."

What we are now talking about is when two representatives, or one representative from DG-15 and one representative of the Data Commissioners Working Party were here last week, they announced that following the

forum which is made up of business, government and data registrars, and they are looking precisely at the whole question of the Internet, and what regulatory regime you might need, and in what way would that be the same, in what way would that be different. And they foresee that the mechanisms that they have established will be also examined to see if that will carry them forward in this area.

So I don't see conflicts. I think we are on both sides, the EU/U.S., have to remember, and that's my role as the chairman of the U.S. Council for International Business, to say what Gary Friend said a minute ago, we are global companies. We are companies that have to build practices not because there is OI Sweden, although of course you are right, Marc, that helps, but because in order to do business around the world you need to establish policies and then work with their OECDs and then support the U.S. Government as it tries to work.

So we think that back in the mid eighties when U.S. business interests pleaded with the U.S. Government to set up a point person with a phone number and a fax, and they established in the State Department the Office of Ambassador for Coordination of Information Policy, and Diana Dugan was the first spokesperson. And then it did shift in January, and Diana and I were on many OECD delegations when

sometimes the leadership was the Office of Consumer Affairs, and sometimes it was another agency.

Not speaking on behalf of my committee but speaking personally, I am delighted that NTIA is now

I want to congratulate the Commission for including this particular session, and for the workshop. Unfortunately, those of us who work at the state and local level in consumer affairs do so in almost total ignorance on a day-to-day basis of the work of our counterparts in Europe. And even our federal colleagues, I think it's fair to say, don't always have a detailed familiarity with the activities that are going on in the European community and elsewhere around the world.

That kind of ignorance is unfortunate in any area of consumer protection, but in this area it can really be perilous, because the choices and policies that may be set by someone in a distant jurisdiction can drive and even

we are more like to speak about federalism and preemption and uniformity and state's rights and so on.

But I think there are some lessons there in this directive. Even more importantly though I think, and to me perhaps the most foremost lesson, goes back to a question that ran throughout this morning's sessions of this workshop. And that was the question who should have the burden, the person who is the subject of the personal information or those who would commercialize that information.

And I think the EU Directive, while it may be fraught with ambiguity, it does seem to have answered that question, at least as a starting principle. It proceeds from the premise that privacy is a fundamental right, and then the analysis proceeds from there. The design of the Directive assumes that the burden resides with those who would limit the right of the privacy, and it is their burden to demonstrate some competing interest sufficient to override the presumption of the protection of privacy.

At least with regard to certain types of sensitive information, including the medical information that we talked about in the preceding session, the EU has gone farther, and has found its balance point by returning to the premise that Evan Hendricks invoked several times this morning. That's the notion that we take for granted in so

many other areas, the idea that the prerequisite for compromising an individual's right is their informed consent to taking that step.

And here the EU Directive applies that presumption of informed consent, at least to the sensitive areas of medical information, information about one's sexual orientation or activity, racial and ethnic origin, beliefs on politics, and religion.

indicated an interest, Janlori, Evan and Al. So just if we can wrap it up in another five, six minutes.

MS. GOLDMAN: Thank you.

that we haven't seen any in the last five years to respond to the Directive.

MR. HENDRICKS: Thanks. I would like to start by answering Commissioner Varney's excellent question. And it's too bad we don't have a European to speak for the Europeans here, because I think it would be very instructive and helpful.

But I think there is no question to me it's not to regulate big information networks. The primary purpose is to advance the human right of privacy, and that is by giving people a legal interest in their own information.

Who owns your name? Do you own it or the people who collected on it? Who owns your information? It all says something about you. But it stems from the history out of World War II, and the Nazi abuse of personal information.

And going to Ron's point, in the nineties now there is a significant blurring of the line between the public and private sector. We have a Census Bureau. They are protected by statute. But a few weeks ago when Yahoo and Data Base America put up 170 million Americans on the Web, you could just dial in and find anyone's name and home phone number, and address. We got Janet Reno's address here. And as soon as she was writing her story, Yahoo pulled out 70 million names of the unlisted phone numbers out of that database.

If we had the kind of protection that I advocate, and which I think is the core of the European Directive, people would be able to consent, whether they wanted that to happen in the first place.

A quick story. The United Kingdom did not have a privacy law. A company there was going to get a contract to process identification cards for a Swedish institution. The Swedish institution was blocked by the Swedish authority from transferring the data to the U.K., because they didn't have a privacy law. The U.K. company lost the contract. They took their case to the government. The U.K. passed a privacy law. They have a privacy commissioner. They have a

If they would have had leadership from regulators, this terrible word "regulation," where they got out in front of this issue and said, hey, let's talk about down the road and standards, you know, maybe they would have helped our industry.

And so I think it's the same way. The only question to me is whether the Europeans are going to enforce their own Directive, Internet or not. It's personal information, it's your name. It doesn't matter what medium it comes through. And if they do enforce their directive, we are on a collision course that's going to have incredible implications for international commerce in line with what1e

The Worldwide Web was invented by a British citizen working at CERN, which is part of a physics laboratory in Geneva, Switzerland. Now, in 1994, I made a trip there and I started negotiations with him, and I was able to convince him to come to MIT to be director of the Worldwide Web Consortium. I was able to do that for two reasons, and I think we in this room have to understand why.

The first reason is, is that he viewed, and I think he was right, that the U.S. was more entrepreneurial than the Europeans. The second was that the Internet, which is far larger than the Worldwide Web, it's far larger in the United States. In fact, we probably at that time had 95 percent of all the Worldwide Web sites in the world here in the United States.

So he decided to come, and we actually set up a very interesting activity at MIT: 140 companies, as I said, are members.

Now, having said that, I have spent a week once every two months in Europe. I have talked to the European Union. I have talked to my partners over there. And I will say that I see a lot of change in the European Community. Just this January the Internet was endorsed by France Telecom. Now, France Telecom had an operation called Minitel, and had actually blocked the Internet almost exclusively in France. But because of this cooperation with

INRIA and because of pressure from the European Union they embraced the Internet and have now opened up the Internet in France.

I view that what is going to happen is that there will be a dialogue between the United States and European Union, and somewhere along the line we will come up with a solution to all of this.

But what I want to leave you with is be very careful about passing regulations at this point in time, or passing laws at this point in time that are going to be outdated in two, three, four, or five years. I think one has to look very carefully about what one does in this domain because the Internet is changing very rapidly. It's changing the people's preference very rapidly.

MS. SCHWARTZ: Thank you very much.

they have gotten messages, please check the message board outside on your way out.

Second, I would like to thank -- I don't know if he's in the room -- Randy Clark. I have never been to an Internet program where things have gone so well as far as demonstrations. And if Randy is here, I would like to thank him for that effort. I appreciate it greatly.

I would like to get you mentally back into the discussion, mostly of this morning, of what do we do to protect consumers' privacy online generally, get yourself out of the European framework, and get back into a domestic mindset.

And two questions we want to consider in this final session, I think, are critical questions. One is, how do we educate consumers about how information is used online, and how they can go about protecting that information And equally, if not more importantly, how do we educate businesses along the lines of the presentation just a moment ago that it's in the businesses' interest to have some sort of privacy protection? And how can businesses go about as a technical matter implementing privacy protections?

We are going to again follow the crystallizer format, and our first crystallizer, who has come in from the

west coast just to be here and crystallize for us, is Beth Givens from the Privacy Rights Clearinghouse.

MS. GIVENS: Well, if I tell you I was in California, you might think I am going to present you with other ideas of what you can do with crystals and crystallizing, but I won't do that.

I have been asked to describe what we do at the Privacy Rights Clearinghouse, which is at the University of San Diego, Center for Public Interest Law. So I will start off with telling you about our center and then go into what I see are some of the more important aspects of consumer education that should be considered in the online world.

The Privacy Rights Clearinghouse is a consumer education and research program, and we have been in operation now for three and a half years. We are grant funded from the California Public Utilities mostly, and we operate a toll-free telephone hotline for California consumers to call, ask questions, raise complaints, and get information.

I think I am truthful in saying that we are the only consumer education-focused privacy program in the country. We do not have legal authority to take action, but rather, we act as an information and referral service. We give very practical kinds of street level information to consumers on how they can take privacy protection into their

own hands. And we refer consumers to other sources of information, whether that's government agencies, industry representatives, other consumer groups and also the media.

Our arsenal of consumer information includes 19 publications which we call fact sheets. I have left one out on the table earlier. Including privacy in cyberspace. These publications are in paper form and also on the web site. We get about 10,000 calls a year which is, I think, considerable for a staff of three to handle.

Some of our part-timers are law students, and one of the things I am proudest of is getting young lawyers to be interested in privacy issues, consumer privacy issues in particular. So we are turning out a few, I hope, privacy advocates who are attorneys.

What have we learned in these past three and a half years that can be applied to today's discussions? I will make five points.

The first point has to do with visibility. One of the best things that we can do as consumer educators is to make the invisible visible. This is the first step toward empowering consumers to take action on their own behalf. One of the characteristics of the online world, and it's been mentioned a few times here already today, is that personal information can be gathered and compiled in ways that are invisible to users.

Now, a major theme of this workshop, and I think an action item that the workshop organizers probably want us to take away with us, or would want the participants to carry with them, is that online systems must be built with information gathering mechanisms that are visible to the user and which, of course, involve user's consent.

voice mail system where they give us their name and address and we send them publications.

We have learned something very interesting, I think, from a couple of surveys that we have done with a random sample of our users. Those who have talked with us directly are more likely to take action to protect their privacy than those who simply left their names and addresses on the voice mail system.

Now, how does this finding relate to the online world? Simply, when developing online forms of consumer disclosure and consent, the more interactive such methods the better. Consumers need to become actively involved in the process of deciding the fate of their personal information more than just reading a screen of text on log-on.

My third point has to do with feedback. Many consumer education initiatives do not involve feedback. A lot of pamphlets are printed and distributed, or web sites put together and that's it. But the learning loop is missing. As I mentioned earlier, we at the clearinghouse do have the luxury of talking to a lot of people, and I realize that in the overall scheme of things 10,000 calls a year is

it back to government agencies, legislators, industry representatives, other consumer advocates and so on, much

say, "I signed up for that mail preference service, but I don't know if it's doing any good, and besides how do I know if my name is really on it?"

So what does this have to do with the slogan "high tech/high touch"? That it's great to take advantage of the power of technology to give consumers access to this huge array of information and some services, but for those service areas in which consumers might experience problems, for example, privacy examples being credit fraud, unwanted mail, phone solicitations, the human high touch element cannot be ignored. There are times when consumers must get in touch with real people to help them solve their problems or answer questions that could not be conducive to online communications. And unfortunately, consumers are increasingly finding that the real time human interaction is in scarce supply.

Now, my fifth and final point has to do with youth or young people with a nod towards Sylvia Goodman of the Illinois Privacy Council, who is making this one of her

opportunities in the course of their every day transactions where personal information about them is being given up. They have virtually no expectation of being told that their personal information is being gathered, and that they have the opportunity to say yes or no about this.

Well, it's hard to teach old dogs new tricks, such as looking for those disclosure notices when they are there and then taking advantage of them by either giving or withholding consent. That's why it's so terribly important that youngsters learn about privacy when they are introduced to technology in school. This includes looking for and taking advantage of those disclosure and consent opportunities, learning the consequences of revealing personal information, and also being taught that when they don't like the information gathering process that they are seeing, they can and should take their business elsewhere.

Now, I must admit that I have had limited experience interacting with young people in my consumer education work, but in my few encounters I have been horrified at the lack of privacy consciousness or even interest in the topic. So I think there is a great deal of work that can and should be done in this area of working with youth, and raising their consciousness about privacy issues.

That concludes my remarks and I thank you very much.

MR. MEDINE: Thank you.

Our next crystallizer is a very familiar face here at the Commission's public exercises in finding out what's going on on the Internet. Bill Burrington is the assistant general counsel and director of Public Policy at American Online. He chairs the Online Public Education Network, Project OPEN, which he will talk about, and Interactive Services Association, and perhaps more importantly, Bill has chosen to be with us here on his birthday. Happy birthday.

MR. BURRINGTON: Thank you very much.

VOICE: Twenty-nine today?

MR. BURRINGTON: I've actually aged since I have been sitting here, so what a neat present this has been.

Thank you, David, and I want to thank the commissioners and the Commission staff and all of you. This is -- each time we have these, I think this is the third public hearing that I have been to, they get bigger and bigger, but we seem to be moving forward too and getting more understanding, which is great. And I know the logistics of putting this together have been a lot.

I want to just sort of put all of this in perspective. You have heard today about the role of

about technology. And there is a third component that is, I think, equally, if not sometimes, especially at this critical stage as this medium is evolving as a global medium, and that's education, the third component to this whole thing.

And I want to say, to put some of this in perspective and tell you a little bit about Project OPEN, and then let Linda Golodner, the President of the National Consumers League, provide her perspective as well on the education front.

And then there are sort of consumer advocates who are here, like Linda and others, who fill a very important role in this discussion.

But I think what has been missing, and what we need to do, and in fact sort of for the record I would like to suggest that this hearing record should not close until the FTC does or engages in some serious empirical consumer focus groups to take consumers who are actually using online services on the Internet today and bring them in here and ask them, to find out what they really think.

I mean, we all sit here in Washington, and many of us either live here or come here to visit, and we are all experts in this area. But it would really be nice to hear directly from consumers when presented with choices. I am sure we are going to hear that they care a lot about

think we are all sitting here assuming that all consumers are as interested in this issue as we are. We are very interested, and I know the consumers are generally, but I

still in development, that are certainly out in the marketplace, along with a really effective education program might be an even more effective and meaningful solution to the issue of child safety.

And I would argue that the same is true here with respect to privacy. And I was encou 0 co

commitment, and have made significant progress in the last several months. So I think we are bringing more here than just lip service to this issue.

In addition to that, the ISA were very involved -- the ISA companies, member companies, were involved with the passage and drafting of the Electronic Communications

Prodigy, and others are slowly coming on board, was to say, you know, there is a lot of media attention about child's issues, so we decided that's an important issue. There is a lot of potential here on the copyright front in terms of its impact on the future of the Internet, so we decided that was an important educational issue. Overall consumer protection was another one. And we identified privacy as a critical issue here.

So what we will be doing is after these guidelines or whatever kind of process we ultimately decide upon here are implemented, we want to go ahead and educate and use the unique power of our medium to education consumers about the privacy rights, about the policies that we have all adopted, and make it easy for consumers to truly make it a two-way interactive process, so they can get their questions answered online about their privacy concerns.

And I think when it comes to addressing businesses, I think it's safe to say that the companies in this room are the ones that care a lot about this issue, and there are thousands of other companies out there in the United States that will be part of the Internet in one form or another. And I would love to see the DMA and the ISA and the Federal Trade Commission and the National Consumers League and NAAG and other groups work together to develop a model curriculum, if you will, for businesses, to let them

understand why privacy is an important issue; what they can do, some of the basics they can do to be safeguarding the privacy rights of their customers, and then let's promote that appropriately using the medium.

And maybe that's one of the solutions we are going to come to here.

The other thing I want to point out on the whole regulatory front is that I am not aware so far that there has been a situation in which the Federal Trade Commission has not been able to go after in an enforcement way the bad actors when they are dealing with these issues.

And I think one of the things you run into with the Communications Decency Act, because that debate got so crowded by emotions and politics and everything else was that a lot of the laws and regulations already on the books already work. And my view is let's start there, and see where we have problems. And I think that you all have been quite active, and appropriately so, in going after some

where we need to focus our efforts on some more creative, out of the box ways of putting teeth into these self-regulatory approaches rather than say we need government regulatory approaches just to come and get them.

And, finally, and this is a very personal thing to me because I have watched this privacy debate now for two years, and I have heard a lot of the same things here today. We, all of us here in this room, whether you are an online Internet provider, whether you are with the Federal Trade Commission, or any other aspect of government, or whether

And if you don't mind, I will turn this over to Linda. Linda has been a tremendous help in realizing the potential of this education campaign that we have mounted, Project OPEN. And also just for your information I passed around to the people up here our first brochure that we put together, with an 800 number, and also available online to our subscribers.

So, Linda.

MS. GOLODNER: Okay. I just wanted to echo what Bill said about commissioners possibly bringing in some consumers who actually are online.

Recently, HHS had a meeting with the Annenberg Center in California. It was on cyberhealth, and I found it very eye-opening to listen to individual stories of consumers who were online, especially in support of chat rooms, or support groups, when they had a condition that they wanted to talk with people about. And I think that you would learn a lot that way.

I also don't know if those consumers knew if some of their rights were being -- their privacy rights were being violated.

I think we have got to make sure that there is proactive education both for consumers and for providers of information. I think the better companies, obviously, will be working on some proactive education of consumers on using

the Internet and using online services. But I always worry about those bad actors, and I mentioned that before. They are the ones that we always have to be aware of.

I don't think a lot of people really know what personally identifiable information is. They don't know that there is information that they should not give out. They don't know how it's going to be used, and they don't know how it can be used against them.

I think that a lot of purchases that people make offline now, people are not aware of all the information that's reflected about them, and how it can be used.

When we are educating consumers, we have to use all sources available, and the media is one of the great sources that consumer groups have found to get our messages out, because this reaches millions of people.

Just doing a brochure and send it out to a few people is not going to make a difference.

At the point of sale, point of sale of an online service or where you buy a computer, obviously, is a place where people are going to be concerned if they are going to be going on the Internet, and they should be getting information there.

People have to know what their choices are, and I think it's an obligation of online services and on other programs to provide information to consumers about the

choices of where they can check things out. They have to know where they can go when there is a problem. They have to know about the real people out there that can be actually on a phone line providing information to them, maybe through an Attorney General's office or through a consumer protection office.

People have to be educated on what questions to ask, what questions to ask once you get into an Internet site, what are the warning signs that that site might be a little dangerous for you as far as your privacy is concerned. They have to know, as I said, who to call.

Consumers have to know what the rules are. They have to know if there are rules in certain states or certain jurisdictions that will protect them. Unless they know those rules that will protect them, then they don't know when their rights are being violated.

Last of all, I think that we should look at who is using the Internet now, and I think that the statistics show that more and more senior citizens are using the Internet, and they are some people that we should be approaching now with new information, and that we are going to be talking about children tomorrow, so I won't touch on that.

But we should also look at who is going to be using it for the future, and plan for the future and have some proactive education for them.

MR. MEDINE: Thank you. You have done an excellent job of focusing us on some very critical issues here. Just a couple of quick technical announcements.

Additional copies of Chairman Pitofsky's statement, which we ran out of earlier, are now available outside for folks on the way out.

I just want to extend some additional thanks to Ruth Sacks, Gregg Hill, Nichole Branch, and the many others who helped out on this session.

COMMISSIONER VARNEY: I have a question for Bill.

The joint standards that ISA and DMA are working on for Maryland, what are those standards about, and are they privacy? Do they include some privacy? And when will they be available? When will you be presenting them, and when will they become operative? What's the time frame?

MR. BURRINGTON: Let me clarify it because the standard guideline process emanated out of the bill that was introduced in Maryland, the commitment we made to those legislators. That's when we got going up here in Washington with this item of very productive, several months worth, and many hours worth of discussions and negotiations with DMA and ISA.

So some of the principles, I think they agreed on a number of them, and actually some of the preliminary ones that we have, and our intent is to get that process

completed, you know, quickly, as soon as possible. We have got a number of key components already that we --

COMMISSIONER VARNEY: Are they fair information practice --

MR. BURRINGTON: They are privacy.

COMMISSIONER VARNEY: Privacy?

MR. BURRINGTON: Privacy, right.

Like in our case it's building off the ISA's mailing list guidelines that we adopted last year dealing with issues like spam and unsolicited e-mail, those kinds of things. So it's going to the heart of these sort of cyberspace privacy issues.

COMMISSIONER VARNEY: And when will you be able to release them?

MR. BURRINGTON: They are in the back.

COMMISSIONER VARNEY: Okay.

MR. BURRINGTON: And we are still, again, are work in progress, but considering the complexity of some of these issues, there they are.

COMMISSIONER VARNEY: Okay. And have they been adopted officially by ISA and DMA and are they binding on the membership?

MR. BURRINGTON: I can't speak for DMA, if you want to on that.

COMMISSIONER VARNEY: Yes, go ahead.

MR. SHERMAN: Yes, the principles have been adopted.

up, because we want to create an educational film where you can click and find what company privacy guidelines are, some companies were more ready than others.

The fact that there was public attention on those guidelines, that they were going to be out there in the market so that consumers could compare them, I think was helpful in getting the online companies who had guidelines to put them in different places, to take them -- to try and present them. I think the pressure, these public forums, which put the issue on very busy companies to begin with, who are all out there growing by leaps and bounds, putting attention on the issue help to focus them. And they say, and really I said it -- I said it last time, I'll say it again, there is a kind of crisis mentality which affects us all, which is what's at the top of your plate.

Do we have to put up a guideline on the CDT page, or do we have to send them to some congressional committee who is holding a hearing, when is Commissioner Varney calling them to be implemented in practice? Those are deadlines, and they get people working as there are deadlines on the Communications Decency Act, copyright or any other issue.

To put privacy at the top of the page requires two things. One is having a deadline like that, but the other is to find the beginnings of something that looks like

progress or a consensus, or some way of bringing people together around a step forward.

In my years, lots of people talk about the Electronic Communications Privacy Act. What the Electronic Communications Privacy Act, and most telecommunication bills were, and privacy bills, will tell you is that without some consensus between a good part of the privacy community, the consumer community and industry, there ain't no legislation, nothing goes forward.

So that if you state that our goal is to have a big regulatory commission and an enforceable statute with, you know, six regulators reviewing all the guidelines in the world, you are saying it's a non-starter. Let's go home.

What was interesting this morning -- and on the other side, we're going to continue to educate our consumers as we go along. Some of that is real. Some of that can be for all the best reasons disappear from the top line of a company. So what was interesting this morning was that there was -- between the, one the one hand, we need the big law, and on the other, we don't need anything, there was an interesting discussion in the technology meeting where both technologists from MIT presented and said it is feasible in interactive technology to not only do the kind of setting up, labeling system so that EPIC or the ACLU can -- or the FTC can set up a good guide, and you can go and block out

those sites if they don't have the right policy, but also that the technology lends itself to on-screen communication of what your or my privacy preferences are, allow companies

And at the same time businesses can negotiate back to consumers to make more informed choices, and meet their customer's needs and desires.

MR. MEDINE: Which is to say --

MR. BERMAN: I want to end it.

MR. MEDINE: Okay.

(Laughter.)

MR. BERMAN: But I have got to end it by coming down on the process. To get that middle process requires a process. It requires the consensus and bringing people from the privacy community, the business community, the technology community and saying, show us what you can do. They said they can do it. Give them some time and say, come back and show us how you can do it.

But to strain the Commission's budget, further, I would strongly argue that the focus group ought to include and not simply be limited to current users, but be expanded to people who aren't using it because there may be some practical differences in their approaches or concerns to privacy. And, in addition, these are folks that hopefully will be coming on line over time.

I am certainly encouraged by all the work that's already being done by the business community, as well as the nonprofits and the governmental sector in terms of making educational efforts as effective as is possible. Certainly making them interactive helps reinforce the actual learning process.

But, in addition, I think there is further room for creativity as far as the particular venues for educational opportunity to take place, or at least where you can post messages alerting consumers to the possibility of getting follow-up information. That can be done through the computer manufacturers having standard materials inserts

that it's in their interest. And that's obviously a very important question, as was brought out this morning, a very high percentage of web sites currently don't have any privacy guidelines that they post or even that they have adopted, and that's most likely not out of malice, but out of a sense of just not having reached those questions. That's something that obviously needs to change over time, not only to help them draw more customers who have greater assurance that those privacy guidelines are in place, and then they can decide whether or not they want to deal with that particular business entity. But, in addition, I think -- rather, the smaller businesses need to be educated about potential issues and pitfalls for them in the world that I think is coming.

For example, as the pressure grows for greater consumer access to information about consumers that is put online, and for the ability to correct that information, you may have the businesses that are transmitting medical records, HMOs, doctors transmitting patient records online who aren't thinking about the security of the patients that are present may, out of the most basic self-interest motives, decide to type it up in a hurry if and when that information can be gotten from them.

MR. MEDINE: Given our very short time, I am going to exercise the privilege of the chair, and keep people as

I mean, if you go back 100 years, you were making a -- this is important because of the discussion of anonymity that came up this morning.

If you were back 100 years in a cash transaction at a drive-in store, it's likely that the owner knew who you were, he knew what you were purchasing, over time he knew the pattern of your purchases, and frankly used that to achieve a certain level of service, to say, "Mrs. Jones, are you running low on flour?" Because he has seen the kind of purchases you made.

That same use of data for service exists today, and most businesses would be very surprised to hear that their use of data in that way changes simply because they move online.

Now, admittedly, consumers may not know -- we pointed out earlier -- that this data is being collected. And so we have to come up with mechanisms for filing in what is a relatively small and temporary information gap.

MR. MEDINE: If I --

MR. DUNCAN: If I could have just one more moment.

The Commission has been criticized a lot in the eighties for the permanent hair dye case, and this is a case that individuals hadn't been told that the permanent hair dye would not permanently change the color of your hair. But what you were dealing with there was really an

informational problem. What you are dealing with is the fact that there was something, it was a new technology, and consumers did not understand how this technology worked. But you did not need a permanent solution.

So what we really should be talking about now is

constituency at all. That's extremely important to keep in mind.

Secondly, I want to point out a Washington phenomenon that I think everybody ought to be aware of. In my experience it's been representatives of companies don't know what their own companies are doing. And so I think consumer education has to begin at home. I would be happy to educate company representatives about what their own companies are up to. They are always surprised and shocked when they discover in fact that there are some things going on in their company that they hadn't know about.

Bankers will tell you that they never share information. Credit bureaus will tell you they have never been hacked ever. Hospitals say that the law requiring confidentiality, and we have never had a breach of that. And I don't know about trade associations. I mean, some are more actually in touch with what's going on than others. Some of them, you know, even a level removed from what the companies themselves know about. So I would say consumer education has to begin at home.

I would like to thank the commissioners and the staff for sticking this out. From my experience in this town, we are usually talking to empty tables and empty chairs about mid afternoon, and I very much appreciate your sticking with it. I hope it's been helpful.

MR. MEDINE: I thank all the panelists who have endured throughout the day as well.

Let me call on three more folks who asked for attention; that is, Marc, and Steve, and some final remarks.

Yes.

MR. ROTENBERG: Well, I just wanted to say something in the spirit of where do we go from here. And I guess in some respects to raise a question about something

And I think what we are going to see in the future is not a division along this spectrum that Bill and Jerry have suggested, but a very different division. A division between those people who believe that the current system basically works, that it may need some minor tweaking, some notice online, some consumer education, and another group which believe we need privacy protection equal to this technology; that is, as bold, as creative, as entrepreneurial, as forward-looking as the technology that we are designing.

I mean, Thomas Edison said, you know, what man creates with his hands, he should be able to control with his head. And I think it's in that spirit that we need to go through with. And you are going to see in the second camp privacy advocates, industry groups and governments that are going to proactively try to protect privacy, because it is good for everyone. And you are going to be seeing hanging back in the first camp the people that are going to say, well, we just need to get out another code of fair information practices, do another consumer workshop, and that will take care of the problem.

And I think the reality is at the end of the day the second camp will prevail, and the reason is that privacy is not a consumer issue. In the twenty-first century it will be <u>the</u> consumer issue. Privacy will be to the

information economy what consumer safety and product safety has been to the industrial economy. And if you don't understand that, about where we are heading, you really don't understand what is going on out there. You cannot have an information economy unless you have privacy protection. The system will collapse.

MR. BURRINGTON: David, I need to respond since my name was brought up, if you don't mind.

MR. MEDINE: Very briefly, 20 seconds.

MR. BURRINGTON: Twenty seconds, 17, 15 -- very briefly. I just want to -- I think you mischaracterize a remark that I said earlier. In fact, I was really saying what you just said. We at least speak on behalf of the online Internet industry, we get this, and we understand exactly what you mean, because it's in our best interest to understand that, if this medium is going to grow as a global medium, and it's going to be a robust amount of commerce and activity, and make this truly a mass medium. I was really

MS. HEATLEY: Connie Heatley, from DMA.

I just want to add my voice to our commitment to education. We see it as our mission to educate both businesses and consumers. I have brought lots of show and tell about the kinds of things that we have done together with the FTC, with the Postal Inspection Service. We have a web page up that has both our privacy policy, which is an example to businesses about how to do it, and it is connected to the commitment that we have made. And also, we have consumer protection information out there.

We would like to move forward in working with any organization that is interested in doing this, and we have begun that process, certainly with CDT. We have had elementary conversations with CME, and we would like to move forward in the area of education.

MR. MEDINE: Well, thanks, and the last word of the day goes to Steve.

MR. COLE: I am Steve Cole with the Council of the Better Business Bureau. Thank you, David.

As an advocate for self-regulation and as a former state consumer protection regulator, I hear two different views of the world, especially this morning. I heard about PICS and cookies and I/PRO codes and whatever, and I heard Shirley talking about clicking 12 o'clocks on the VCRs. We heard a lot about consumer choice, empowerment and even a

market. David, we talked about this even in your office, setting up a market of people to compete on privacy policies.

By word of caution, I wish I had solutions and not just problems as the last speaker, consumer choice won't work if it's too complicated. It simply won't work. It has to be simple. Consumer choice isn't going to work if the choices are too plentiful. If we turn this debate into a supermarket, needing really great expertise to sift through the different choices that are available, the choices may

You need tough standards, they need to be simply stated, and they need to be graphically demonstrated.

MR. MEDINE: Thank you, and some final words from Commissioner Varney and Chairman Pitofsky.

COMMISSIONER VARNEY: David, I want to echo your thanks to everyone for coming and sitting at the table. It's not often in Washington that you get such a diversity of opinion at one table, having what I thought was a rather challenging, yet extremely civil conversation about these issues and where we go.

My question is where do we go? And I think I see a couple of things. First of all, we are going to leave the record open for a couple of weeks. I mean, we are going to leave the record open for two weeks, and we have asked some questions during the day, and we have asked you all to submit your thoughts and comments on the record over the next couple of weeks. I would ask you in your thoughts and comments to address the question of where do we go from here.

Secondly, I think that there will most likely be, and I will certainly talk to my colleagues on the Commission and the staff, there will be a staff report that will come from this hearing, I hope, and in that staff report possibly we will see recommendations to the Commission about further action.

There were several people here today from Capitol Hill. There will be several people here tomorrow from the Hill, from both the Senate and the House side. And there has been some expression of interest in a report to the Hill. There has also been some expression of interest in preliminary hearings after the recess, when they do come back, on privacy on the Hill. So we will see what happens there.

Finally, for the future Commission action, I think that it's important for all of you to remember that we do have ongoing enforcement authority and ability. And when you find issues that you believe are clearly fraudulent and deceptive, you need to let us know. You know, this is an area that we are all struggling in. We are all trying to protect the integrity of the medium, and we have a role there to play, and we can only play it when we know what's going on.

But when we separate out what we have identified off and on during the day as kind of the two questions, one is information collected about consumers who may not even be online, who are not in the transaction; that information moving around the Internet, being bought, being sold, being put to different purposes, I think is a very serious policy question that our staff ought to take a look at, and create a record on.

The second question, when consumers go online, whether it is for a transaction or pre-transaction, what is the responsibility of the web site that they are going to to disclose what they are doing with information, what are the technological solutions that consumers can employ to empower themselves to make choices, and what is business's willingness to commit to make that a reality?

I have heard everybody at the table today say we can do it, we can do it, it can be done, it can be done. We will do it.

Well, I would like to talk to my colleagues and invite you all back in maybe six months and let's see if you've done it, because I don't know where we are going to go if you don't get it done, and if it doesn't work. We have heard a lot about what we need to have in place to make these technologies work and we have also heard from all of our friends at the table.

If they don't work, we will need to take the next step towards looking to solutions, and I don't know what that is, but I for one would like to see the entrepreneurial spirit that has characterized America's success in the global economy work here as well.

CHAIRMAN PITOFSKY: I think the bases have been touched. It's been a fascinating day. I am happy I was able to be here. I know there are very provocative issues on for

tomorrow, and I look forward to more discussion of these questions.

MR. MEDINE: Thank you. We stand in recess until tomorrow morning.

(Whereupon, at 5:10 p.m., the workshop was recessed, to reconvene at 9:00 a.m., Wednesday, June 5, 1996.)

//

//

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)