FEDERAL TRADE COMMISSION

I N D E X

June 11, 1997

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

FEDERAL TRADE COMMISSION

In the Matter of:	)
PUBLIC WORKSHOP ON	) Session Two
CONSUMER INFORMATION PRIVACY	) Consumer Online Privacy

Wednesday, June 11, 1997

Room 432
Federal Trade Commission
6th and Pennsylvania Ave., N.W.
Washington, D.C. 20580

The above-entitled matter came on for hearing, pursuant to notice, at 8:50 a.m.

P R O C E E D I N G S

- - - - -

COMMISSIONER VARNEY: Good morning. Thanks for coming back, to those of you who were here yesterday, and welcome to those of you who are just joining us today.

Yesterday we had an extremely productive session, I thought, on databases, look-up services, and the issues attendant to their use. I think it is fair to say we didn't reach any conclusions yesterday, but hopefully today we will, maybe we will be able to reach some conclusions.

A year ago many of you joined us when we examined online privacy and what were the practices, what were the standards, what were the tools, what were consumer expectations. And we really found out quite a bit about what kinds of information were being collected about people with or without their knowledge and with or without their consent.

There were many people in the room last year who said, you know, government, you need to step in right now because this is a serious breach, and it needs to be taken care of. More people said: Wait a minute, let's see if there can be a marketplace for privacy. Let us see if we can develop the technological tools and the industry best practices and self-regulation that will obviate the need for the government to step in and regulate in the arena of

one-to-one interactions and transactions on the Internet.

So we are back. It is a year later. I think I saw a lot of you last October when I kind of jumped up and down and said for self-regulation to work, it has to exist. And I know that we had a huge amount of effort on the self-regulatory front.

We have also had a lot of effort on the development of technological tools. I think we will see three or four of them this morning. I think we are going to hear some updated news about what is the state of consumers' expectations regarding privacy and the information collected about them online.

I thank you all for coming and look forward to a good session today. Let's, without further ado, get started.

David?

MR. MEDINE: Thank you. Welcome back again. And we are now in our second day in our second session of our privacy week of the FTC.

We have a busy day ahead of us to focus on consumer online issues, and we are going to start off the day with getting a clear sense of what consumers' perceptions are of online privacy.

We are going to have two panels discussing survey results. The first will be, I believe, the first representative, national survey of consumer attitudes about

online privacy, followed by a second panel which will express results of focus groups, opportunity studies, and other evidence of consumers' views on online privacy.

Alan Westin has been working with the FTC staff to help us wrestle with the issue of online privacy as long as we have been in the business, so we greatly appreciate his efforts. After last year's session, he talked to us about the desirability of really getting a clearer handle on what consumers' perceptions were. And we are delighted he is here with us today to present his results.

He is the professor emeritus of public law and government at Columbia University where he taught for the past 37 years. For four decades he has specialized in studying, writing, and consulting about the impact of information technology on individuals, organizations, and society.

In 1993 Dr. Westin cofounded a bimonthly report on information service called Privacy in American Business. He is joined today by Humphrey Taylor, Chairman and Chief Executive Officer of Louis Harris and Associates. And Mr. Taylor will present first.

PANEL 1: CONSUMERS' VIEWS ON ONLINE PRIVACY

"What consumers think about online privacy and current interactive privacy-enhancing tools."

Panel 1A: Representative National Survey

HUMPHREY TAYLOR, Chairman and Chief Executive Officer, Louis Harris and Associates, Inc.

ALAN WESTIN, Editor and Publisher, Privacy & American Business.

MR. TAYLOR: Thank you. Good morning. Thank you very much for inviting me here today.

I must acknowledge that the survey data that I am going to share with you is very much the product of my colleague, Joy Sever, who has done all the work, for which I am now taking credit. And, off course, Alan, who has been my guru and mentor in privacy matters for 19 years. I guess someone even as old as I am can still have a mentor.

The survey is a survey of just over a thousand computer users. And we defined computer users as people who use a computer at home, at work, at school, or in some other place such as a library. And that is now just over half of the adult population of the United States.

We surveyed them by telephone. We finished field work about six weeks ago, so the survey is already out of date in this rapidly changing world.

I have got time to present about 1 percent of the

findings of what is a 170-page report. And I just would like to stress that, you know, Harris falls over backwards not to do hired gun surveys for anybody. This must satisfy and has satisfied our requirements of being a fair, balanced, and comprehensive study. And Joy and Alan ensured that we did that.

Just a very few of the findings then. First of all, of these computer users, 42 percent access the Internet at least once a month, and 33 percent use an online service. And we have about 25 percent who use both, and about half who use one or the other or neither.

Half of these computer users who do not currently access the Internet state they are likely to do so in the next year. That doesn't mean to say they all will, but clearly many of them will.

A similar pattern is observed for those who are not currently using an online service. And the factor they say which is most likely to influence them as to whether or not they use an online service is privacy protection.

Now, we want to be careful about going from what people tell us to the real world, but clearly privacy protection is a very important issue for many of the people who do not yet use the Internet or online services.

It is interesting to note that fears about online privacy and invasions of privacy in the electronic world

greatly exceed people's reported violations. Many people worry about security and confidentiality of their personal information in an online environment, but very few people report having actually been victimized while online.

5 percent of all Internet users say they have been a victim of what they felt was an invasion of privacy while on the Internet, but more than half, 53 percent, say they are either very concerned or somewhat concerned that information about which sites they visit will be linked to their E-mail address and disclosed to some other person or organization without their consent or knowledge. And we find a similar pattern of answers when we ask about online services.

Computer users are more concerned about the confidentiality of communicating by E-mail over the Internet than they are about other widely used forms of communication, including the telephone, fax machine, and the mail. This concern is greatest among computer users who do not actually communicate via E-mail. They are, indeed, twice as likely as E-mail users to be concerned. And that's a pattern which I will mention more in a moment.

When it comes to the handling of confidential information, computer users have less confidence in online companies than they do in many other institutions which handle personal information. While 75 percent of computer users are very or somewhat confident that employers,

hospitals, clinics, and banks use in a proper manner the personal or confidential information which they give them, only 48 percent express the same confidence in companies providing online services; 46 percent for companies providing direct Internet services and 40 percent for companies offering products and services on the Internet.

Computer users' privacy concerns translate into what we have called privacy sensitive behaviors. Of those who use the World Wide Web, having been asked by a site to provide information, the majority say at some time they have declined to give that information.

The majority of those who did not provide information say they would have provided it if they were aware of and comfortable with the information use policies of those sites and if they were more familiar with those sites.

And there is a pattern that runs through these data of people being willing to do a lot more than they do now or do things differently from what they do now if they had more knowledge and more trust in the privacy policies of the various organizations.

We find other privacy sensitive online behaviors are practiced by smaller proportions of Internet users. 12 percent of Internet users say they have encrypted or coded information sent through the Internet. 20 percent of the users say they have participated in chat groups and forums

that have discussed privacy issues.

On the question of unsolicited E-mail messages, very few computer users who receive or have received unsolicited E-mail messages offering to sell them products and services welcome them, and more than a third of E-mail users would want their addresses removed from all others, if possible.

Interestingly, we find that 43 percent of Internet users who receive -- who send and receive E-mail say they sometimes receive unsolicited E-mail messages. And of those who did receive these unsolicited messages, 42 percent said, and I quote, "it is getting to be a real pain and we want to stop getting these messages."

Another 55 percent say it is a little bothersome but we just delete the ones that don't interest us. And a very few, 3 percent, say we like to receive these messages because they interest us.

We found that computer users express more interest in Internet software products that would help them become more familiar with the companies they deal with online and their information policies than they are about other Internet software procedures, so, again, privacy is a really important issue for these people and they want to be able to do better protecting their own privacy and they want help doing it.

We find, by the way, big differences between men and women when it comes to privacy issues. Compared to males,

female computer users are less likely to have heard, read, or seen a great deal about the Internet, and they are less likely to access the Internet, but of those who are Internet users, females spend less time on the Internet. Females also express greater concern about many online privacy-related issues. And on every question were much more likely to express those kinds of opinions.

When we come to the role of government, we labored long and hard to draft a question which we felt would be fair and balanced. And we gave people three choices and asked them which one of these choices best fit their idea of what government's role should be.

And the one that comes out top is for the government to pass laws now. Let me read you, if I may, the exact responses. 58 percent of computer users feel that the government should pass laws now on how personal information can be collected and used on the Internet. 24 percent, a quarter, say the government should recommend privacy standards for the Internet but not pass laws at this time. Only 15 percent feel that the government should let groups develop voluntary privacy standards for the Internet and monitor any problems, but not pass laws at this time.

It is interesting to note that compared to lighter Internet users, heavier users are less in favor of government regulation. And females are more likely than males to favor

government regulation.

The computer users most in favor of government regulation are also those least familiar with the Internet. And indeed Internet users who use the Internet more, the more they use it, the less they favor government regulation.

Let me just say, as I pass the baton here, that we are measuring attitudes that are surely and behaviors that are surely changing very fast. And you know many or most of the things that will be done on the Internet in five years' time haven't yet been invented.

I think I can say with confidence many of the opinions we have measured here are not as yet deeply held or carefully throughout through or deeply held convictions and that behaviors, attitudes, hopes, and fears will surely change in the months and years ahead, based on the experience and the events and of what people read and hear.

Thank you very much.

MR. MEDINE: Thank you. Dr. Westin.

MR. WESTIN: As someone who has been working in the privacy field for quite some time, let me start by saying how important I think it is to do representative national surveys of the public or of large groups like computer users.

First of all, these data provide the basis then by which all opportunity surveys and focus groups and so forth can compare their populations with the representative

national survey to see how the groups that they are surveying and these special populations compare with the national sample and, thus, understand how they are different, stronger, weaker, attitude sets different from the base line data.

Secondly, since virtually everybody working in this field believes that they know exactly what the American public thinks, we have at least here some semi-scientific or scientifically oriented ways of saying back: Well, if you put this question to a representative sample of the public in this way, this is what you get. And if you depart in a major way in saying that you know better what the public thinks, at least ask yourself whether this is a wish or a scientific statement that you are communicating to policymakers.

Finally, I have learned over 20 years or so of working on privacy surveys that this is a very complex issue and every survey we do is a challenge. It combines a lot of artistry along with scientific survey research methodology, and that anybody who looks at what we have come up with here or any survey like this has to look closely and carefully at the strengths of what we have come up with, as well as the limitations, which are usually in good methodology openly stated as the limitations of the survey.

And so it is in that spirit that I want to offer some interpretation and commentary on findings.

First of all, as I said, this is a very rich and detailed survey. There were over 120 items asked about. 74 of them covered the areas which other privacy surveys with Harris have used as our topical areas, what knowledge people have, what experiences they report, what concerns and attitudes we can have them express, what policy preferences they have, and especially what kind of actions and remedies did they think would meet the concerns and attitudes that they have expressed.

As Humphrey mentioned, we have four populations, really five, represented here. All computer users, about 100 million, the 42 million people using the Internet, 33 million that use online services, and 49 million who are not yet online. We also have 14 million Net parents, that is, the parents of children under 16 who are using the Internet.

And I will be reporting the May results about our findings as to Net parents and their attitudes at the FTC hearing tomorrow afternoon. We included on the survey trend questions from prior privacy surveys, and some indexes that we used to measure levels of distrust in institutions, fear of technology and so on, which in previous surveys have been good indicators of what the underlying or driving forces are behind people's attitudes and policy preferences.

We will be handing out after this presentation a fairly detailed document for you that has the questionnaire

and all of the tabulations listed, the executive summary of the main parents report, which runs about 120 or so pages, and my interpretive essay that will be in the main document.

In about two weeks we will have available a full 175-page report with graphs and tables and all kinds of good stuff in it. And that will be available either through Privacy in American Business or the Interactive Services Association, which has been our colleague in developing the survey.

Let me start by expressing our gratitude to the Interactive Services Association and to a group of 13 sponsors from business and industry that made the survey possible -- American Express, America Online, Citicorp, Cybercash, Dun & Bradstreet, Electronic Messaging Association, IBM, MCI Communications, Metromail, Microsoft, Netcom, Nynex and The News Corporation -- a very Catholic group of enterprises engaged in a very wide swath of information activities and services in the online world.

We also were very fortunate in having an Advisory Committee that helped us with the choice of topics and issues for developing the questionnaire from the Center for Democracy and Technology, Consumer Federation of America, the Electronic Frontier Foundation, National Consumers League, Privacy Journal, and the Privacy Rights Clearinghouse, plus the staffs of quite a number of Federal Government agencies

that work in this area that helped us not only with the questionnaire but as we began to look at some of our analysis.

I would like to take a minute to say quickly how to understand the sample that we have because they are not the general public and, therefore, to compare them with the general public is important at the outset.

Computer users, first of all, are concerned about issues of personal privacy at about the same level as our studies show the general public. That is, when you ask a question whether people would agree or disagree with the statement: Consumers have lost all control over how their personal information is being collected and used by companies, the computer users we found scored at the same 80 to 82 percent level of agreement as when we have asked that question of the general public.

As a whole, our data show computer users are younger, have higher education and higher incomes than the general public, so they are a more advantaged subset. On the other hand, they are less fearful of technology and less distrustful of institutions than the general public.

They are the ones who recognize that they are more or less running the society and, therefore, being technologically engaged, they are not quite as fearful of technology getting out of control or that institutions are

not to be trusted at all compared to those in the public who are not using computers.

And when we look at our Net user sample, the 42 million people on the Net, they are even younger, even higher income and even higher education, even less distrustful of technology and even less distrustful of institutions.

In general, we found as a matter of a question that we have used over the years that computer users share the same attitude with the general public that if companies and industry associations adopt good voluntary privacy policies, that would be preferable to regulation, and in the 70 to 72 percent range, our sample of computer users and Net users and so forth echo that general principle, which we found the general public to share.

How do we begin to explain what might be seen as a surface contradiction in our findings that while only 5 percent of users on the Net, 7 percent of online subscribers, report that they have been personally victimized, we get in the 50 percent levels of concern over E-mail being read, visits to Websites being potentially tracked, having to give personal information to visit sites, discussions in forums and chat rooms being monitored or getting too much junk E-mail.

Those are the concerns, yet we have such an extremely low level of people who say they have been personally

victimized. Incidentally, when we asked in general public surveys in the off-line world: Have you been the victim of something that you felt was an invasion of your privacy? We generally get 25 percent and some sectors 35 percent of people who report that they have, they believe they have been personally victimized through invasions of privacy. So reported invasions are much, much lower in the online Internet world.

Why do we have high concern, but very low reported incidents of direct victimization? I think this is at the heart of understanding how to interpret the survey findings.

First of all, if you have been reading the mass media, watching television, going to the movies, or if you read online computer technology and Net publications, the last two years has seen a steady drum beat of accurate stories saying that you mustn't expect much privacy and security in the current state of the online Internet world.

That is, the reports point out that you can have your clickstream monitoring of sites, that cookies is a technology that has been widely used, that, in fact, a great deal of unsolicited E-mail has been received by people who use E-mail.

So the media, in a standard fashion, have emphasized to people that this is not a safe place, this is not a secure place for your confidential information. So that's part of

what I think our concern level is.

Secondly, we found it quite interesting of people who participate in chat rooms and forums, 20 percent say they have discussed privacy issues online. And that's 2 or 3 million people who say they are discussing privacy in their use of chat rooms and so forth.

We also note in our findings that very few people are encountering Websites that openly on their screens tell people what the information and policies will be in handling their information. So people have not yet seen the kind of bargain or communication and choice that everybody would, I think, in principle say should be the mode of fair information practices in the world of the Internet.

And we found that only small numbers of people are aware of new software control, personal information control tools that they could use. So if you look at those contributing elements, it is not at all hard to understand that the concern is not driven by actual violation as much as it is by perception of the world in which these people are engaged.

But I want to underscore what I think is the strongest single factor that explains the levels of concern on the part of users. And in the past we have always found that when you ask how much confidence people have in industry by industry to use the information they collect about their

customers or consumers in a proper way, respecting its confidentiality, that that correlates very highly with their attitudes about privacy threats and their desire for any kind of regulation or remedy.

Here we listed ten industries and asked people how much confidence they had in their information handling. And very high marks, high, what we call high and medium trust, was given to employers by 80 percent of computer users, hospitals, 79 percent, banks 77 percent. But we fell into the 40 percent ranges when we asked about confidence in the online companies.

Humphrey mentioned that only 48 percent gave that confidence to online service providers, only 46 percent to Internet service providers, and only 40 percent for companies offering products on the Internet.

Then when we compared the confidence index, high, medium and low confidence, with the answers to all of the major privacy questions, concern about junk mail, the children's privacy questions, desire for regulation, there was a direct correlation between the level of trust in the online companies and the attitude and concerns about privacy and desire for intervention.

Humphrey mentioned, and it is one of, I think, our main findings that women users of computers in the online world are even stronger in being concerned about privacy and

wanting action than women already were in the off-line world.

We found, for example, that in our survey 11 percent of women were more concerned, very concerned that sites could get their E-mail address, 11 percent higher in opposing sites selling or renting children's information to third parties, 7 percent higher that putting public records on the Net would be a privacy problem and 7 percent higher that being able to surf the Net anonymously was important to them. And women were a full 18 percent higher in feeling that government should pass laws now in order to protect privacy on the Internet.

Children's privacy is a major concern, we found, in the survey. And the complete data about that will be presented tomorrow. But I think it is important to note in my discussion right now that the 14 million Net parents have intense feelings about what could be called information extraction from their children using the Net and by majorities that range from a low in the 50 percent to a high of 97 percent. They simply don't find it acceptable for businesses to collect information from their children, even when it is said to be -- and the way we worded our question -- only going to be used, one, for statistical purposes, two, to help improve the products of the companies that are marketing, three, to use it by the company itself for additional marketing to customers and, four, the

97 percent figure for renting or selling that information to other marketers for marketing to children or to the families of children.

And when we asked whether companies should be held legally liable if they violate the stated policies for using information collected from children, 96 percent, a virtually unanimous vote from Net parents, agreed that companies should be held legally liable.

Perhaps the most important point to discuss is the finding that Humphrey reported that 58 percent of our sample support government passing laws now on Internet privacy.

First of all, is that inconsistent with the finding of our survey that 70 percent generally favor voluntary policies over regulation? Not really, if you analyze it.

First of all, past surveys show that there is always public support for sectoral laws addressing issues on a sector-by-sector basis, and I think here the Internet or the online world is being perceived as a sector.

We know the public does not support, by 66 percent, a federal regulatory agency, like European Data Protection Commissions with authority over the whole private sector, the whole business community, but that's different than what we obviously were asking here.

The support for voluntary always depends on the public's perception that business is doing enough or is

capable of dealing with the problem under the existing legal structure. And it is clear from what we have already presented that the public does not yet see on the Internet and the online world the activity by business that would meet those criteria.

Finally, the children's issue is what we call an intensifier. And it is obviously a very important concern on the part of people. Humphrey noted that a majority of people who are using the Net do not support government intervention. They are in the 40 percent range.

Now, our question did not go into the particulars that anybody in public policy would be careful to think about before deciding just what it is that the public is saying when it says government should pass laws now. We didn't specify whether it would be the federal or state government, what would be the rules and standards and what would be prohibited, who would regulate, what remedies there would be, and especially how you would balance the competing interests of free speech and consumer choice with the desire to have privacy protection on the Net.

When you open up those issues, we would expect that the numbers would take on a quite different configuration, though I think the sense that government should act probably would come through as a general matter.

What are the overall implications of the survey? I

start with a premise that the Internet world reproduces all of the good and evil in a society and it forces us to reconsider the balances that have been set in the off-line world among three vital values in democratic society: Individual privacy, public disclosure, and society-protective surveillance, but now it is the new environment with dangers and opportunities that this has to be applied in.

I think that the survey is quite clear in saying that online users want some privacy law and order on the cyber frontier, that the day of the cattlemen and hacker gunmen and the sheep herders and all of the busyness of the frontier needs a little schoolmarm, minister, sheriff, and judge in order to achieve the balance that people want to see in this exciting new environment.

What are the implications then for the specific communities that are represented in a hearing like this? First of all, it is a very early snapshot, as Humphrey mentioned, and people did not yet know, I think it is clear, what industry has been doing in the last months or year, rolling out new guidelines, but they are not widely known.

There are new ways that companies are announcing what their information policies are, but not a majority by any means yet. Some new personal control software and techniques are developing, but they are not widely used. And no experience has been developed with them. And the kind of

major educational campaign that I think is absolutely necessary to tell people about these choices is yet to be rolled out on a national scale.

And we haven't yet had the policy debates about what kind of legal controls would be the appropriate ones for the public.

So the implications I see for the players are that the online industry is going to have to find ways to earn higher trust and confidence by their deeds in communicating their policies. 71 percent of people in online services say they do not know what the information policies of their online service providers are. So the online industry has got to find a way to communicate better and to support the privacy code that will develop on the Net.

The technology community needs to forge new personal control software, support encryption, enhance the biometric identifiers that can be used to make information more secure. Industry associations and their public interest allies need to roll out their programs with major educational support and find ways to monitor and ensure wide compliance.

For businesses that offer electronic commerce, it seems the survey is absolutely clear. Announce your information policies, give visitors a choice as to how they will communicate with you, and recognize that's the bargain, that's what will make the difference in whether people will

use your online Internet commerce.

Finally, for government, my sense is that government needs to hold solid hearings, just as these have been last year and this year, to identify the problems that are emerging, to monitor how much industry is doing, to protect standards and practices that work, and as the survey concludes, to see where it may be necessary to put some legislative standards in place, especially to deal with violators and those that reject what is the emerging fair information practices ethic for using information in the Internet world.

Thank you.

MR. MEDINE: Thank you very much, Dr. Westin. We will have some questions. I mean, I think the results are startling in the sense of the interest in government involvement in this area, and at a time when there is less confidence in government than one might otherwise like to see, and, as you said, 66 percent of the people don't want a federal privacy agency, but there still seems to be a high demand for government activity in this area. I guess I have a couple questions about that.

First, in your prior survey results, surveying privacy issues, do you see anything like this demand for government action in other privacy contexts or just in other contexts generally?

MR. WESTIN: Yes. This does match the kind of figures, even higher, of the public support for, for example, federal regs in the health and medical privacy area and very heavy support for what President Clinton announced in his Morgan State speech, that he would sponsor bipartisan legislation to forbid the use of genetic tests for health insurance underwriting.

So in particular areas you get very strong support by the public for legislation.

MR. MEDINE: And it also appears -- there seems to be an interesting correlation between the more you know about the Internet, the less concerned you are about privacy, but that also seems to suggest one of the reasons why the Internet may not have taken off as a medium of commerce is that people are scared to get on it because of privacy concerns.

Was that consistent with your findings and does that really suggest a need for either industry to step up to the plate and start really protecting privacy more clearly and more explicitly or for government to act to protect consumers' privacy?

MR. WESTIN: Well, we thought it was interesting to give people a number of reasons or factors that might entice them to come on to the Net, and we were hard-headed so we said lower prices and more flexible and easy to use software,

et cetera, but the one that scored the highest was better protection for personal privacy in communication and commerce.

And the second one that scored highly, not at the top, was more control over unwanted advertising that would be sent to you if you use the Internet. So I think that a very clear message of the survey is that the people who are not yet using the technology have probably been alarmed by the Sandra Bullock movies and other kinds of things that say that if you order pizza, the dark forces of the night will get to you.

MR. MEDINE: We actually thought about showing a clip from "The Net" this morning to set the tone for things, but we didn't want to be alarmists, but maybe we weren't being alarmist in those concerns.

It sounds like this may be a situation where an investment by industry and added cost of providing consumer protection would really pay off substantially in increased confidence, because more people would be willing to engage in commerce.

MR. TAYLOR: Yes. And let me just add on this question of government, we all live, as you mentioned, in an era where people have little trust in government, amongst other things, but they turn to government when all else fails.

And they would prefer, as you heard, to have the private sector do things so that no government intervention is necessary, but when they do not have the confidence that the private sector can do that, then they turn to government. And that's what we are seeing here.

MR. MEDINE: Commissioner.

COMMISSIONER STAREK: Thank you. I am curious about this statistic that we have been talking about or the results that we have been talking about that indicates that as people become more and more familiar with the Net, they are less and less likely to think that the government needs to regulate or legislate in the area.

Why do you suppose that is? In other words, I am confused by that. Do you have any further data that would explain why it is that people who are much more familiar with the medium would be much less likely to think that the government needs to play a major regulatory role here?

MR. WESTIN: I am glad you asked that. I think there may have been a little miscommunication here. When I said that Net users were less favorable toward government, it is a figure like 46 percent, if I remember correctly, as opposed to 58 percent. So it isn't as if they are saying leave us completely alone. It is that in that spread there are people who probably are libertarian citizens, old timers for whom government is never the answer, and my guess is that that

crowd accounts perhaps for the difference between 46 and 58 percent. That's one thing.

Secondly, I think that the people who are on the Net may be much more aware that they have some tools and they use the tools like encryption. 12 percent of people on the Net say they are currently using coding or encryption techniques. So, there again, you have got a piece of the Net population that may feel that they already can exercise some control and they don't need to rest on a piece of legislation to help them.

I wouldn't agree with the way you said it at the beginning that the Net users are not as concerned about privacy. It is the difference in where they think some of the remedies and controls could come from, I believe.

MR. MEDINE: Commissioner Steiger.

COMMISSIONER STEIGER: Doctor, is there anything in your findings that would distinguish between, let's say, personal privacy in general and economic privacy? I am trying to get at whether there is a strong fear of using a credit card method of payment that might explain the Net's, let's say, not strong takeoff as a business tool?

MR. WESTIN: There have been so many surveys we are aware of that asked people would you be concerned about using your credit card on the Net and the figures come up saying 75 percent, say, we would be concerned. We didn't waste the

question in our survey on that.

We did ask whether people would be more likely to purchase if they were aware of how the information that was collected about them would be used, and that shows through very strongly. So not the credit card point, but that if an organization explained what ways they were going to use their information, people would be much more likely to give their personal profile to companies that said if you tell us more about yourself, we will give you special offers, we will make you aware of things that match your interest.

The big difference in people's attitude toward using that service was whether they would be told how that information would be used and could control what additional uses would be made of it.

MR. MEDINE: You emphasized the disparity between the number of reported incidents of privacy invasion and the high degree of public concern, but I wonder if that's not really all that surprising in the sense of if I lived in a community where 1 to 2 percent of people were mugged, I would have a high degree of concern that there be a lot of police around, even though I may not even have a likelihood of getting mugged, it is the kind of thing I would absolutely want to prevent happening.

It doesn't seem to me it would be all that surprising that a small degree of incidents should necessarily result in

a high degree of concern.

MR. TAYLOR: Let me add one thought. I think you are right with the analogy. The big contrast is between the online world where, in fact, we find very large numbers of people claiming that their privacy has been abused or violated, excuse me, the off-line world, and I guess the good news for the industry is that these numbers of people who say their privacy has been violated online are very, very small, and I hope it stays that way.

MR. MEDINE: I suppose one possible explanation is people aren't doing the kinds of things online that might lead to privacy invasions because they are apprehensive.

MR. WESTIN: When we asked the 5 and 7 percent what was the invasion that you felt, the two were getting junk mail and having to give their personal information when they visited sites as a condition of using them. So I think that's quite rational.

On the other point, on the other hand, my sense is that somewhere like 5 to 7 percent of the public believe that martians have dropped into their neighborhood and have engaged in secret interrogation of them, so you've got to be very careful to understand the crazy level that there can be in our society about things that happen to us.

MR. MEDINE: There is a noise level in every survey, I take it. If we don't have any further questions --

MS. BERNSTEIN: May I ask one, David? I know we are going to take up children later, Dr. Westin, but I was intrigued with the findings apparently that a very high percentage of Americans don't think any kind of information should be collected about children. Is that correct?

MR. WESTIN: Yes, if you put in without parental knowledge and consent as the indicator. In other words -- and I will go into this more tomorrow. I think that parents are reflecting, based on our low confidence finding, that if the children give information to sites that are not yet saying how they are going to use it and are not bound by any limitations, that the parents perceive that their children can be put at risk. And I think that's what is driving that.

MS. BERNSTEIN: Thank you.

MR. MEDINE: I would like to keep Dr. Westin and Mr. Taylor, if he wants, at the panel and invite some other folks to join the panel as well, if they haven't already, to present some survey results. We will give them a minute or two to make their way up to the table.

(Pause)

PANEL I: Consumers' Views on Online Privacy

Panel 1B: Surveys based on random samples of online users and surveys of self-selected online users

STANLEY B. GREENBERG, Greenberg Research, Inc.

TOM HILL, Director, Cyber Dialogue, Inc.

MICHAEL KLEEMAN, Vice President, The Boston Consulting Group

TARA LEMMEY, Chief Executive Officer, Narrowline

DEIRDRE MULLIGAN, Staff Counsel, Center for Democracy and Technology

JAMES E. PITKOW, Research Scientist, Xerox Palo Alto Research Center, Graphics, Visualization, and Usability Center, Georgia Institute of Technology

***

MR. MEDINE: Thank you. What we would like to do in this next expanded panel is to really get a sense of whether the other surveys that have been done are consistent with the reports of Dr. Westin's survey and where there are differences and maybe hot points in what we might learn from additional surveys.

First I want to call on James Pitkow, who received a Ph.D. in computer science from the Georgia Institute of Technology, where he began the Graphics, Visualization, and Usability Center's World Wide Web user surveys in 1994. He

is currently working at Xerox Palo Alto Research Center in Palo Alto.

How do you take these survey results and how do they compare with results that you have obtained in the past?

MR. PITKOW: Well, we are very grateful, as I said, for having national representative samples to compare results to. They are absolutely essential, critical for these quicker-type snapshots and general impressions to be framed and contextualized with. Thank you, gentlemen, for your very good work.

We have been conducting these surveys for three years, and we have been focusing on data privacy issues for a year and a half now. A lot of the results that we show are very consistent with the national representative samples.

In particular, we do show that females are more concerned about privacy. We do show that experience on the Internet impacts roles and perceptions of privacy, et cetera.

We also asked some questions that they do not get to, issues that help identify where there is actually a perceived boundary in security and in privacy. So, for example, we asked people whether or not use of demographic and behavioral information helps improve the design and relationship of a site? And people tend to express relative agreement that this is a good thing. If you understand your user, you will

be able to get better information.

However, when it comes to the ability for content providers to actually resell this information, they are very much less favorable about that. So there is kind of a sandbox for which this information actually can be contained and people feel comfortable with.

We also note that people generally are very much so more protective of this new medium than they are with other mediums. So when we ask: Well, do magazines have the right to resell this information, more people express this is okay, but when we talk about online content providers, less people are more favorable in that. And in general there just tends to be an increased perception and protective nature of the people in those areas.

One of the things that we have shown is relatively strong stability in people's perceptions across the surveys in the time course that we have asked them.

There are very few questions that we ask, and even when we perform longitudinal analysis on people who have taken this survey, then the next survey, and then the next, where their perceptions change that radically, so on an aggregate level, as well as an individual level, there seems to be stability in a lot of people's perceptions.

We also show that people do support government regulation in this area. People do feel there should be new

laws. 80 percent of the people do not believe in persistent identifiers that can track users across sessions.

People are not tremendously well educated about the use of persistent identifiers or cookies, so 40 percent of the population doesn't even know that such identifiers exist. And in our longitudinal analysis of people, we show that there is some minor education that actually occurs when people become more informed about what information can be passed, although it is not tremendous. So there is definitely some areas for improvement there.

One area that we show a difference in -- and this may actually get into how the question is worded -- is in how often people falsify information online. We show a very high increase as compared to the 5 to 7 percent that come from the national representative samples.

Since I haven't had access to the questions and how they are framed, it becomes difficult to say exactly why there is such a difference. We show that significantly more people falsify information online.

So in general there is wide agreement and consensus between the survey methodologies. And then this helps us increase our confidence that even though we don't use scientific or random sampling methods, that our numbers are actually representative.

MR. MEDINE: We appreciate that. I think one thing

that struck me with your results was that people are more protective online and that seems certainly consistent with what we have heard in past workshops here; that is, because more information can be gathered about you online, people would tend to be more concerned about their privacy.

And do you have any better understanding of why there is a higher degree of concern?

MR. PITKOW: It is not only that more information can be gathered. It can also be compiled quicker and without human intervention. And so there is really multi-dimensions that actually shift when you change into this medium that need to be considered.

As far as why people are more protective, we don't really get into that. Maybe some of the focus groups here who actually do interviews with people and can push down a little bit further on that, have more information about that.

I think there is just a generalized concern that since this is a new medium, new frontier, people generally have the perception that other information is out of control, that they see this possibly as an opportunity to help restore some balance.

MR. MEDINE: One conclusion I guess one could draw from that is firms that are going to do business online need to be more privacy protective than firms off-line.

MR. PITKOW: I think certainly there is this notion that privacy becomes a value-added commodity within a business model of self-regulation.

MR. MEDINE: Thank you. Why don't we go to your right, Deirdre Mulligan, from the Center for Democracy and Technology.

MS. MULLIGAN: Thank you. Like Mr. Pitkow, I was quite happy with the national survey, but more for the reason that rather than the Center for Democracy and Technology, we are not generally in the business of doing surveys, but we are in the business of trying to give you an idea of what we think the public policy implications of different decisions are. And I think --

MR. MEDINE: I am sorry, I didn't give you a full introduction. We have seen you so many times, but I want for the record to indicate that you are staff counsel for the Center for Democracy and Technology, and prior to joining CDT you worked on information privacy issues and emerging technologies in the Electronic Frontier Foundation and ACLU. I am sorry. Go ahead.

MS. MULLIGAN: Last year in our testimony before the FTC we stated pretty strongly that our belief is that if we failed as a society to adequately protect privacy, the people not only would lose the ability to retreat but they would also be unwilling to step forward and participate.

And I think for the first time I not only have anecdotal evidence to put forth to support that, but we have hard statistics here that say people are retreating and people are concerned.

I think that the findings of the seven surveys are probably more impressive because of their commonality; that we find an overwhelming kind of degree of public anxiety. We find a desire to know more about information practices. We have an increased concern in this electronic environment.

We have seen a very strong desire for things that are as kind of privacy protective as anonymity, and I think these should send very loud, clear signals for policies that reflect these consumer needs.

I wanted to respond to a question that you posed earlier about why is it that the quantifiable number of people who have experienced privacy violations is small, while the concern is high? And I think that we could use the Social Security Administration's experience with the PEEBS database, not to overwhelm them with publicity, but that Social Security Administration online database, many, many people accessed PEEBS' information, we have no idea how many people's privacy was violated because there was no way to verify who was accessing that database, and that, unfortunately, privacy violations are often very hard to quantify.

They are hard to identify. People sometimes have to experience some other type of harm before they can identify themselves as a victim.

And that, you know, as someone who has worked on privacy issues, the question is how do we protect privacy on the front end without putting people in the position of having to figure out where that harm came from? We found that very strongly yesterday when Beth Givens was talking about people who were unaware of why it was they were unable to get a job. It was very difficult for them to figure out that it was because of some information that was collected somewhere else that may or may not have been accurate.

Finally, perhaps because Beth is not on a lot of panels, I am going to use a lot of her information, that I think one of the most valuable things that the FTC is doing ties directly to kind of a plan, how we go forward. And these surveys play into that, also that in looking at the role of public education, there is an article by Beth Givens, who is the director, I believe, at the Privacy Rights Clearinghouse, wrote an excellent article that I would really direct you all to on the last set of caller ID and consumer education.

California did a very, very active campaign to educate consumers about that caller ID was coming to market and that they had options to protect their privacy on the

dialing end, that you could opt for selective blocking of your line or selective blocking per call. And what happened was about 50 percent of consumers in California opted for per line blocking, which is a very strong statement about privacy.

Beth, in mapping out kind of a what can we learn from the caller ID experience, came up with a three-step plan. And the first one was to conduct a privacy impact assessment of the technology. And I think that is what the FTC has been doing, I think what these surveys gives us the ability to do.

We can see not only the impact on industry. I think the eTRUST survey or the Boston Consulting Group survey says this has down sides for commerce, and I think the Alan Westin surveys and these other anecdotal or less statistically national surveys show us that there are real down sides for consumers.

The second one was to require the entity which introduces the technology to build in privacy protections. And I think later on in the day we are going to look at a number of ways in which technology is actually being used to build some of those protections into the medium. And I think clearly that is something that consumers are clamoring for.

One of the most interesting results in our rather short brief survey was that people said: I would love to be

using these technologies. I would love to be turning my cookie prompt on. I would love to be encrypting my mail. I would like to use an anonymous re-mailer. I don't know what they are.

And public education really needs to accompany any effective program to protect privacy, whether it is policies or technology.

And that was Beth's final point, that nothing is successful without public education. And I think that the escalating concern that we see among the public really should tell the FTC and certainly advocates such as myself, and I think the industry players that are here, that education is an incredibly important thing. And that you have to start to be involved in it, otherwise no one is going to be on the Internet.

MR. MEDINE: Thank you. I think the challenge will be to get the word out to consumers that they are taking place.

Why don't we move to Stanley Greenberg, Chairman and Chief Executive Officer of Greenberg Research, a national survey and polling firm.

MR. GREENBERG: I, too, want to thank you for the opportunity to participate in this discussion and respond to the study done by Dr. Westin and by Harris, and also to thank Harris and Alan Westin for years of probably the most

dependable research available on this whole issue, not just the Internet but the privacy issue, which many of us have tracked over the years and use as our bible for this.

It is also important for those of us who are doing focus group research, qualitative research, and are trying to understand what Americans are thinking as they come to these questions, it is critical that one have the guidepost of a quantitative survey that enables one to put in proportion one's findings.

Focus groups are very good for generating provocative hypotheses. Quantitative surveys are much stronger for establishing strong findings.

Let me begin just at the outset on the issue of the role of government. It is the part of this which was featured in the presentation and picked up by others and by Commissioners and others here on the panel.

And I want to urge a great deal of caution on the conclusion one has drawn here. Let me just say I am not one who is averse to a large role of government, as some know in other areas of my life, so as I come to this question I don't begin with a presumption against a regulatory response.

But the data here is actually, I think, reflecting a cry from the American people for somebody to do something, and I think Dr. Westin was right to say that it is a cry for law and order, privacy law and order. And I think that is

right.

I think people are looking for limits and rules and responsibility, but I believe they are also open to a broad range of ways of achieving that.

And we may be too quick to jump on this question of expanded government. Let me just speak very specifically to the finding of this study, which found 58 percent supporting a legislative response.

Let me say at the outset I understand the choices one has to make in a survey. Something has to be asked first and something has to be asked last. But the way things that are asked in the survey do influence the responses one gets in the survey.

The question on role of government follows a page and a half of questions on E-mail and people reading your E-mail and immediately follows that battery of questions. I think it is a reasonable conclusion that the specific response on that question is reflecting, I think, a very real concern that E-mail may not be held private, people may be reading one's E-mail, but that is a different question than necessarily the one that we are addressing here or at least is a part of the question, not the whole of it. And we ought to interpret it in that context.

In the survey, immediately following the question about the 58 percent supporting role of government, the

survey, when asked whether the private sector ought to take the lead or whether government ought to take the lead, 70 percent say the private sector. Good efforts, serious efforts on the part of the private sector is a better way to address the problem.

And in the page after that, the survey asks about whom you trust on this question, trust on these issues, whether business will do more good or harm or whether government can be trusted to address this. By two to one, the responses are that business will, is more likely to be trusted to do good in this area.

I recognize that there are things that people, there are areas here where people do want a regulatory response, but you want to be very careful in taking the specific finding and broadening that to people wanting a broad governmental response.

In fact, the findings from the last Harris survey, the Equifax survey, when asked about a commission that would offer regulations in the area of privacy, two-thirds were against such a large notion.

Then also I should just mention in terms of findings presented by others on this panel, we should not jump to a conclusion when people say a practice is unacceptable, for which there are many that are deemed unacceptable by online users, that therefore the best response to that is

governmental. Being unacceptable does not mean that the best way to end that practice or limit that practice is a governmental response.

When asked specifically in this survey of online users, when given a real set of alternatives, a majority in that survey said they prefer an opt-out register and only 5 percent preferred a government regulation. So when offered a real set of alternatives to a real set of problems, people respond in a more nuanced way.

Let me go to the question that Dr. Westin posed, which is a very important question of why there is a high concern about privacy but low victimization. I want to suggest that we are here in this room today because of the privacy issue, but that American people are here in this room today for a bigger set of reasons, for which privacy is only a small subset, which is the main thrust of the focus group research that we have presented.

For anybody who has done focus groups, and many I am sure on this panel have, if you begin those sessions and say what is going right and wrong in America today, you will get an extended discussion about the moral decline in the country, the breakdown of family, the fact that children face very bad influences, can't be set on the right course in life, that parents don't have the tools to be able to educate their kids, protect their kids, and those are very big

concerns, they are real concerns.

This issue is important to parents, it is important to ordinary citizens because it is part of a larger sense that the family is less and less able to protect their own family, protect their children, ensure that children can move, get a good start in life.

However, when they think of issues that concern them, privacy is not at the top of the list of things that they are trying to protect them from, whether we are talking about the Internet context or non-Internet context. Outside the Internet context they are much more concerned with crime and violence and drugs and a broad range of other issues, way down the list of things that constitute an invasion of families, and when you get to the Internet, I am sure others can speak to it with their own data, the first overwhelming concern is that the children will be exposed to indecent material.

They are concerned that people on the Internet will make advances to their children or advances to their family, and they are concerned that information will be passed out that jeopardizes the family, but that is not the same thing as companies soliciting information for which there is a much lower level of concern.

So there is a reason why women are much higher, I think, expressing much higher levels of concern. We are

talking to them here about privacy because that's the subject of this hearing. They are concerned about protecting their families from all kinds of intrusions. Privacy is a small piece of this and much lower down the list. And on this there is some sense of opposition.

People do want governmental responses in areas important to their lives. There is a certain skepticism in this area of whether the government can handle this effectively. There is a considerable openness to other ways of addressing the problem. Including, for example, and I will end on this, including -- and in the study done by Dr. Westin, 85 percent, for example, who say that they want parental control software as a way of giving people the tools to address the problem.

People are open to a broad range of responses and we ought to be cautious, I think, about interpretation of this survey suggesting that public wants a set of laws to deal with it.

MR. MEDINE: Thank you, Mr. Greenberg. I wanted to request, I guess, you made some points about how surveys are performed and the questions that were asked and you talked about your survey, how you began sessions and what content there was in those sessions, but unfortunately we don't have the benefit of those in evaluating your work.

Would you be willing to provide the staff a

transcript of your focus groups, so we can understand the context in which these issues arose?

MR. GREENBERG: For parts of it. As I indicated, as I talked to the staff at the very outset, we did not do research specifically for this. We did research on a broad set of issues.

And what I said to the staff at the time is if they want the material, I am delighted to provide the material for those parts of the research that were relevant to this. And I should tell you in terms of what we provided for the blocks of material that were included relevant to this subject, none of the material was edited. All quotations were as presented to my client six months ago.

MR. MEDINE: Although you point out it is very important to understand what preceded that and the specific context and understand what quotes were concluded in your summary. If you could provide us as much of the transcript you are comfortable with, it would help us in evaluating your results.

COMMISSIONER VARNEY: David, I have one question for Stanley. Given the good circle that you drew for us, putting this in context and being cautious about government responses to perceived problems, does that hold true across the board or given what you have said -- and I know we are going to talk about this tomorrow, and I don't know if you are going

to join us tomorrow -- but are children a different arena?

MR. GREENBERG: Stakes are higher when children are involved. I think the call for action is greater when one involves children, but it doesn't -- people are desperate. And they are not desperate on privacy, which is a small piece of this. They are desperate on these intrusions on their families. And they want help and they want tools.

There is an openness to regulation. There is an openness to private sector self-regulation. There is an openness to tools for themselves. What is going to work, what is going to be effective in setting some limits, some rules and empowering parents to be able to help their kids.

COMMISSIONER VARNEY: Thanks.

MR. MEDINE: Thank you, again. Tom Hill is Vice Chairman of Yankelovich Partners and Director of Cyber Dialogue, an online research and database marketing company. He has been conducting interactive marketing since 1968 and was a founder of New Media Marketing.

What do your results show in terms of what you have heard this morning from others?

MR. HILL: Well, thank you for inviting me to be here. I was quite impressed and appreciative of Lou Harris and Dr. Westin's research, which they have provided us. I am, as you said, representing both a qualitative focus group type of firm, Cyber Dialogue, as well as a quantitative firm

in Yankelovich that has done similar nationally projectable studies on this issue in a broader context of studies on cyber citizens.

In summary, the results presented here that I have had a chance to study, certainly we confirm broadly. I have seen enough research both from our companies and other sources and now the studies presented here today to say there is a pretty good consensus on these basic issues that we presented here.

I would like to comment on a couple of nuances in regards to the results and how they compare with the results we have obtained in our studies.

One thing, I think, to keep in mind very much in discussing the off-line world versus the online world and the differences between them is that in our research we have found that both the online and off-line, cyber citizens and non-cyber citizens, have very similar feelings about the issue of privacy.

And, secondly, it is the off-line world that has taught the online consumer to be distrustful of marketing and the misuse of information. So we must keep in mind in discussing this subject in the limited context of online that, in fact, it is part of a broader issue of the perceived misuse of information that has been occurring in the off-line world for years. And that is simply being carried over to

the online world inasmuch as many of the same organizations are showing up online and consumer attitudes have been formed based on off-line experience.

To give you an example, the misuse of information as seen in the form of junk mail by post, as well as unsolicited telephone calls trying to sell products and services are seen by the American consumer as considerably more intrusive and invasive than an IRS audit, for example. So it is an issue which is very much felt by the American public. There is a measurable degree of anger.

The American consumer is very sophisticated at this point. We have taught, through our marketing efforts in the last 30 years or so, we have taught the American consumer a great deal about the marketing process, and particularly the paradigm of mass marketing and direct marketing. They are well aware of the value of the information that they are not receiving any return for, and all they see is the abuse and the violations and they are not happy at all with it.

So it is important to keep in mind that the issue is broader than how to simply create a new paradigm online, because as long as the abuses are still perceived to be occurring off-line, the problem is going to persist; very difficult to separate them.

Secondly, to complicate the question a bit, I think you have to look at this issue of privacy in somewhat of a

tradeoff analysis. That is to say, looking at the privacy side by itself can be a bit misleading when you are not explaining at the same time what the consequences would be of restricting marketers' or information providers' ability to get information about individuals, i.e., the ability to personalize an interactive medium such as the Internet because what happens is that the consumer wants both.

And our studies clearly show that there is a high degree of preference for personalized communication via the Internet and World Wide Web. People want to be treated more as an individual. They want to have information provided that is based on historical patterns and preferences stated, et cetera, so when on the one hand they say we do not want our privacy invaded, on the other hand they say we do want personalization.

There is obviously a tradeoff issue here, and I am not sure if any of these studies have fully developed that analysis sufficiently.

Thirdly, one of the Commissioners asked the question about do you see varied response based on type of information requested. And Dr. Westin said he has seen a lot of that. We certainly have done a good part of that research ourselves and certainly the answer is yes, there is a tremendous variation and willingness to provide information based on the type, just to give you a rough fix in one study we did, the

question of providing information about your hobbies and your interests, we had over 90 percent of all online users saying they would be happy to do that; whereas almost the converse was true about credit card and personal financial portfolio information.

So there is, of course, as you would expect, a tremendous variation in the type of information being requested and the willingness to provide it.

Another point I would like to make is certainly to reinforce Dr. Westin's point about trust. The interactive paradigm, if it is to succeed, is very much a paradigm requiring trust and relationship building. It is the nature of the paradigm.

So unless and until trust is established or enhanced in the online world, we are not going to realize the commercial potential of that, of this technology.

Value given for value received is certainly a guiding principle that the public seems to respond to as regards establishing a more trusting environment, but certainly the other points mentioned about being very clear about what your policy is as regards the use of information and getting consumer agreement in advance to use that information appears in our research to be certainly a major way to solve the problem.

Finally, in closing, the point about private versus

public regulation. It would appear, if you look at the data we have, that there is an enlightened self-interest here for industry because in establishing trust and working in this interactive paradigm, they really do want to do the things that otherwise they would be regulated to do, so in a way there should not in the longer term be an issue in my view between the desire of the public to protect their privacy and the willingness of industry to, in fact, do that voluntarily.

So I would hope there could be a great deal of private regulation, self-regulation as a solution because it makes sense.

MR. MEDINE: That's a very good introduction to the panel that follows. So one question I had based on our prior workshops, there was a lot of emphasis on consumer's ability to control information about themselves and have a choice. That would seem to reconcile the two, apparently conflicting interests and concerns about privacy but wanting personalization.

Do you have any more information about that? Is that consistent with what your results are?

MR. HILL: Yes. I mean, obviously choice is a key issue. Not everyone wants personalization at the same level. And so certainly I think choice is a very key element of the solution as well, but if it is clearly understood

that, you know, it is your choice, the more information you provide, the more personalized the services you will receive, and if you choose not to, you have a way to opt out of it.

MR. MEDINE: Thank you very much. Michael Kleeman is a vice president of The Boston Consulting Group, specializing in technology and Internet areas. He has worked for a wide range of service providers, as well as Internet and traditional communications worldwide.

And, again, your views on what you have learned compared to what the other panelists are findings.

MR. KLEEMAN: First of all, I think our base data are quite consistent with the other findings we have seen here. I am delighted at the representative sample survey. Our data was taken from an online survey of 9300 people that were directed to a site, provided by eTRUST, now TRUSTe, our work was done for them to determine what consumers' attitudes were on privacy and impact on electronic commerce.

Slightly differently than the other data here, our data was drawn from a global sample, around 85 percent was North America, where we had very good data from elsewhere and virtually no difference in overall attitude, although there was some heightened sensitivity with Asia, which may have to do with political issues, we believe, about privacy.

Let me contrast what we found rather than repeating what people have already said. We think that the Internet

basically heightens people's concerns about privacy for a few reasons.

One is online businesses have -- there is a perception that online businesses have the ability to correlate data more quickly and more completely than businesses in the "manual world."

A lot of sites are actually asking consumers for information that no one does in almost any traditional commercial environment. For instance, you are asked to give detailed personal information online just to gain access to a site. No one asks that when you walk into a store.

A number of sites are collecting information from people without their knowledge or permission. And when they find out, they feel that's inappropriate. A lot of sites actually offer information that people weren't aware was available, and they reflect back on what that may mean for them.

And when we started to look at the question of privacy, reflecting what other panelists have said, we believe privacy is closely linked with concepts of security, both electronic and personal security and authentication. In other words, who is the party I am working, interacting with. Can I trust them and will the information I provide be safely secured to them and how will they use it?

Quick summary, consumers have very strong concerns

about privacy on the Internet. It limits their engagement in electronic commerce, and they are generally less willing to disclose more sensitive information to businesses they are not familiar with.

On the extreme case, 94 percent said they were uncomfortable or very uncomfortable providing personal health or financial information to an organization they had no interaction with, no familiarity with. 58 percent, even if they already knew the institutions, were uncomfortable providing personal information, but in contrast, 13 percent were uncomfortable providing information to, say, a bank they already had a relationship with if it was demographics, but if they didn't know the institution, that level rose to 63 percent. So there is this question of authentication and security.

Consumers also recognize and have crude control so what they do is either opt-out or disguise their identity. 30 or 40 percent of the people basically falsify information when they are asked to provide information online. And it is usually based on a subjective assessment of trust in the institution they are dealing with.

Some quick other data. 76 percent expressed concern about sites monitoring their browsing. 42 percent of consumers refused to give registration information because of privacy concerns. Now, what I would like to do; flip to the

positive side. 39 percent said they would pay a half a percent higher selling price if privacy was assured online. People will pay for it. 39 percent will pay for privacy assurance, 29 just for disclosure.

People are willing to say, look, if you give the information about how you are going to use information or disclose it, I will be much more willing to do business with you.

Also in terms of providing information, if sites simply disclosed how they were going to use information, almost 20 percent said they would be more than willing to give information. And if sites assured people that they would use information in a specific way and not violate it, it is almost a 50 percent increase in the number of people that would provide information.

So that leads us to our primary summary findings in terms of the business impact that businesses, if they properly support privacy concerns of the consumers, are actually benefitting themselves. We believe that assurance of nondissemination of personal information, would have significant impact, increasing consumer willingness to participate in electronic commerce by a factor of 2 to 3.

Disclosure would increase almost 50 percent alone if you take that assurance of information privacy and you look at forecasts that come from a number of different sources on

electronic commerce. We are talking about a combined positive impact of $6 billion by the year 2000, if industry takes part in just assuring people how they will be used.

MR. MEDINE: One question. I think you have provided the basis and linked the points together, consumer awareness of information practices. You have indicated consumers would be willing to pay if they were more aware of a company's practices, you have indicated consumers would participate at a higher level if they were aware of companies practices, and you have also indicated consumers have a high degree of concern about privacy.

I take it the link is consumers are not aware in large numbers of how information is currently being gathered on the Web?

MR. KLEEMAN: There is a significant fear. I think what you have, as other people said, is concern about the fact that in the nonelectronic world, there is this general concern about privacy and growth. I think the Harris poll was interesting. It said 82 percent were concerned that businesses had control over personal information, and then you look at that with the confluence of a computer sitting on your desk with all this power and it just amplifies it.

MR. MEDINE: Thank you very much.

COMMISSIONER STAREK: David, excuse me, before we leave, I had a question here. You indicated that your

survey, I think I heard you right, was conducted online, right?

MR. KLEEMAN: Yes, sir.

COMMISSIONER STAREK: You indicated 40 percent of the people who responded to your survey when they were asked for personal information to get into Websites, lie about it.

MR. KLEEMAN: Yes.

COMMISSIONER STAREK: How many people do you think lied in your survey? Do you have a way to factor that out?

MR. KLEEMAN: We disclosed how we were going to use the information, first of all. They were directed through it through a number of trusted sources, with pretty explicit information of how it is going to be used.

We asked general demographic information, no personal information or identifier, except offering if they wanted to take part in a drawing for a pilot organizer, they could supply the information. And we assured that would be kept separate from survey information.

Yes, certainly there is going to be an error rate introduced. We don't believe it is significant based upon the other data we saw about what people will respond to.

COMMISSIONER STAREK: Thank you.

MR. MEDINE: Thank you. Again, Tara Lemmey is Chief Executive Officer and Founder of Narrowline, an Internet advertising research and transactions company.

Before starting Narrowline she was an advertising executive and founding partner of Digital Threads.

MS. LEMMEY: So I get to represent business here. We have a global Internet advertising transaction system, which means we buy and sell impressions from people for major companies such as McGraw-Hill and Match.Com, which is a dating service, and the Chicago Tribune.

There are significant amounts of information that we have on a consumer level that we buy and sell. And our Research Department actually enables the buying and selling of that. We have a responsibility to the people we deliver advertising to because we do deliver advertising and have the ability to track.

What we did, we are very concerned about the issue because if people are afraid to look at Web pages or people are afraid to acquire information, then we don't have a business because that's where we make money.

And we have a very large consumer research group. So we did two things. Two pieces of information that I think follow off of Michael's very well. One, we did a survey to say how frequently have you not gone after information because of fear that privacy might be compromised, and more than 70 percent of the people that we queried, which was a base of 5,000 people who have previously answered online surveys, said that 70 percent of the time, at least, they

have decided against accessing information because they were concerned that their privacy might be compromised.

Over 60 percent of the time they cited the fear of becoming a target of unwarranted marketing efforts as the cause. In addition to that, they said the belief of information being used, being accessed which they didn't want the content provider to have was about a third, and the content provider requesting more information than they felt comfortable with was about 40 percent of the responses.

So we went very clearly at a deep way of looking at this because the more people don't go to pages, the less impressions there are. Therefore, the less money is being made by the content provider.

We followed on that question very easily saying what would allay these fears? How can we get over this? They basically -- the overwhelming response was they would like to see third-party verification that their privacy is not being compromised and they would like anonymous or one-to-one environments. About 60 percent of the time that was a clear winner, which is what we expected.

We have cross-correlation data to say male, female, or age range. We have a pretty good feeling for how accurate this data is based on the fact that our samples come out of people we have surveyed previously for different content sites. And one of the really interesting pieces of

information is when we do surveys online, we have a strong privacy policy up, we are Founding and Steering Committee members of TRUSTe -- let me get that right, we just keep saying it over and over -- and we put up our privacy policy and gave people the ability to answer surveys in secure environments and nonsecure environments.

And when we do these surveys what we do is go back and take a look at the data which they give us, full demographic data and full psychographic data, as well as editorial information. And we cross-correlated that with some of the zip code information that we had to figure out if those demographics were statistically accurate for the area they said they were coming from.

And over 87 percent confidence level that the information that we had was accurate, and over 30 percent of the time people go out of their way to leave the environment they are in to go into a secure environment to transmit the data to us.

The people that we survey were people who in addition to saying this, said they would like to participate in further research studies and for absolutely no -- for information as it relates to privacy and information that we want to put forward to the marketplace. So we have a fairly high degree of confidence that the information is accurate.

And we are quite concerned that if we don't as a

business community take a look at privacy issues, we are going to have some issues, people are going to self-censor, so it is bad from the impressions level, from an economic level, and also bad because you don't want people censoring the information they are getting for many other reasons.

MR. MEDINE: Thank you. Questions? Thank you all very much. This is a very rich content, full panel, and I think it will help inform the rest of today's proceedings. Thank you very much.

Again we will take a ten-minute break and resume at 10:30.

(A brief recess was taken.)

PANEL II: Self-Regulatory approaches to Online Privacy Issues

"A Review of current efforts and the status of industry proposals submitted at the June 1996 Workshop."

JOSEPH L. DIONNE, Chairman and Chief Executive Officer, The McGraw-Hill Companies, Inc.

ESTHER DYSON, Chairman, Electronic Frontier Foundation, eTRUST

RONALD S. GOLDBRENNER, General Counsel, Promotion Marketing Association of America

PETER HARTER, Global Public Policy Counsel, Netscape Communications Corp.

KATHERINE KRAUSE, Senior Attorney, US West, Information Industry Association

WILLIAM M. RANDLE, Senior Vice President, Director of Marketing and Strategic Planning, Huntington Bancshares, Inc., Member of Advisory Group for the Banking Industry Technology Secretariat

JEFF B. RICHARDS, Executive Director, Interactive Services Association

H. ROBERT WIENTZEN, President and Chief Executive Officer, The Direct Marketing Association

***

MR. MEDINE: Thank you very much. After an enlightening session on survey results, we would like to now

turn to industry responses to the concerns consumers have raised.

First let me correct an omission of mine, which is to introduce Martha Landesberg, who is the staff person that has made today possible. We all owe her a great debt of gratitude for her work with all of you to make today happen.

(Applause)

MR. MEDINE: I would now like to introduce Chairman Pitofsky, who will introduce our next speaker.

CHAIRMAN PITOFSKY: We move now into a very significant portion of the program dealing with self-regulatory approaches to online privacy issues and a review of industry proposals that are beginning to be developed in many sectors of the economy.

Our leadoff speaker, I am pleased to say, is Joseph L. Dionne, who is Chairman and Chief Executive Officer of McGraw-Hill, having served previously as President and Chief Operating Officer. He joined McGraw-Hill in 1967 as vice president of research and development at the Educational Development Laboratories.

He is a director of several companies in the education and communications field and also serves on the Board of Trustees and the Board of Governors of the United Way of Tri-State. He holds Bachelor's and Master's degrees from Hofstra University and a degree in education from

Columbia University.

It is a great pleasure to welcome you to these proceedings.

MR. DIONNE: Thank you, Mr. Chairman, fellow Commissioners. It is a real pleasure for me to be here and to represent the work of my colleagues. We want to share with you our new customer privacy policy.

As sort of an orientation, McGraw-Hill is a $3.1 billion global publishing, financial services, and media company. We have 16,500 employees around the world in 430 locations.

We are the world's largest educational publisher. And in the area of financial services our principal brand is Standard & Poor's. We are also very proud to be the publisher of Business Week, which is the world's leading international business publication.

McGraw-Hill Companies is committed to providing the information and analysis our customers want, when they want it, and in the form it is most convenient for them, whether it is print, CD-ROM or online.

In the last ten years the demand for information in digital formats has increased at a geometric rate. Our company has refitted and restructured itself accordingly. 90 percent of our editorial content is now available in digital form. More than 80 percent of all the information

published by Standard & Poor's is read from a screen.

The online distribution of Business Week and a number of our other publications provides us with an unprecedented opportunity to interact with our readers to learn what it is that is of most value to them. And our business units now maintain more than 60 Websites, including DRI/McGraw-Hill, Engineering News-Record, offering potential customers a very direct and interactive way of communicating with our company. Later on I want to talk about the importance of this interactivity.

We are in no doubt about the future of our company. It is global, electronic, and interactive. As this is our vision, we are committed to facilitating the growth of electronic exchange and the unprecedented opportunity it provides for economic growth and the development of human potential.

We recognize that a commitment to the new technologies must include a commitment to their responsible and ethical use. This is both a moral imperative and a business necessity. As we heard from the previous panel, unless the public feels secure in its use of electronic networks, the potential of this technology as a medium of exchange will never be realized.

The McGraw-Hill Companies has long been conscious of the need to conduct itself with unimpeachable integrity in

every aspect of its operations. Our information and analysis is credible because we have earned the trust of our customers over the more than 100 years of our existence. We must continue to earn that trust in the information age.

Not only do we recognize the imperative of meeting consumers' reasonable expectations of privacy, we believe it is our responsibility to serve as industry leader in addressing this issue.

That's why we are pleased to have the opportunity to provide the Commission with an overview of what we have accomplished to date.

Before I proceed with the details of the new policy, perhaps I should provide some relevant background. The McGraw-Hill Companies has had an official policy relating to consumer privacy for approximately 20 years.

When we implemented our first policy in the 1970s, it was, of course, tailored to the print medium and pertained to such matters as the privacy of consumer information on order forms and subscription lists. While these concerns are still relevant, it was clear to us that much more needed to be done in the age of electronic information.

For example, when potential customers click on our Websites we may have access to what is known as clickstream data, personal information provided by consumers as they interact with the date. Clearly consumers must have

confidence that this data will be handled responsibly or they will refuse to participate or, worse, they will leave false information due to their privacy concerns. According to a recent survey, more than one-third of consumers have done so already.

To take another example, Standard & Poor's is preparing to launch an online financial services product, an advisory service. Our customers will be entrusting to us their sensitive information relating to their finances. It is essential, for such a product to be viable, that the most rigorous standards of security and privacy be maintained.

In response to this need to update our policy, we formed a company-wide online privacy task force in August of 1996. Its mission was to develop and help implement a policy based on two main principles.

First and foremost, we recognize our obligation to handle the personally-identifiable information of our customers in a diligent, responsible, and ethical manner.

Second, we recognize that there are legitimate business uses of personally-identifiable information which are beneficial both to us and probably more importantly to our customers.

Responsible collection of consumer data helps us; one, to develop customized information products and qualify customers to receive them. For example, our LAN Times

publication uses data collected from consumers to refine both print and online products.

Business Week uses information collected about an individual's employment status to determine if she or he is eligible, to determine if they are entitled to receive special editions, such as the Industrial Technology edition or Business Week Enterprise, just to name two.

The point of the technology is we are able to publish. We can customize information for a single reader or viewer, only if we have relevant information about his or her interests.

Responsible collection helps us to personalize navigation through a site to help users locate information of the most interest to them and do it quickly. A number of our sites are using this technique to great success, including our College Division which has refined its Website to make it easier for professors to search and locate relevant course materials across disciplines.

It helps us to conduct electronic commerce and to enter into contracts, particularly in our educational and professional publishing groups, such as the McGraw-Hill Book Club, and to track product interest for internal research and development purposes, which ultimately leads to more product offerings for which consumers have more choice.

An effective privacy policy must strike a balance

between both concerns, that of privacy and that of quality and relevant materials.

As the task force proceeded with its deliberations, we developed programs to raise awareness of this issue throughout the organization.

In November 1996 we conducted our first company-wide forum on privacy in which we introduced the privacy issue and communicated that successfully addressing it was a priority for The McGraw-Hill Companies. A second forum in May presented the new policy and set the stage for company-wide implementation.

Our policy is based on the following general principles. The first is notice. Our customers and business prospects should be advised as to the type of information being collected as well as the internal and external uses that may be made of the information.

The second principle is choice. Customers and prospects should be notified of the opt-out mechanism by which they may refuse permission for their personally-identifiable information to be distributed for external use outside The McGraw-Hill Companies.

You will see on our home page here in the lower right-hand corner there is a privacy policy and all of this material is spelled out simply by pressing the button.

The third principle is security. The McGraw-Hill

Companies has a responsibility to its customers to maintain the security, privacy, and integrity of their personally-identifiable information.

In keeping with this principle, only employees who have a legitimate business need to do so will be authorized to access this information.

Before I summarize our specific implementation policies and procedures, let me provide you with two pertinent definitions. We define personally-identifiable information as information about individual customers or prospects, such as postal and E-mail addresses, billing information, employment status, job descriptions, or birth dates.

In addition, personally-identifiable information includes the subcategory of sensitive data. We define sensitive data as personally-identifiable information that requires an extra degree of protection. It includes Social Security numbers, credit records, or mother's maiden name. It also includes certain types of personal financial data, such as salary and net worth of specific investment portfolio of an individual.

Certain types of personal medical information are also clearly falling within the scope of sensitive data, such as the fact that someone has a specific medical disability.

In addition, information about children should be

considered sensitive data. It is our policy that sensitive data will never be distributed outside of The McGraw-Hill Companies.

It should also be noted that the aggregated form of these types of information, where no identifiable individual data are referenced, would in most cases not be considered sensitive data or personally-identifiable information.

Let me now outline the policies and procedures which, once fully implemented, will govern our use of all personally-identifiable information.

First, personally-identifiable information will be collected only when reasonably necessary to serve a legitimate business purpose.

Second, customers and prospects will be notified of the uses to be made of this information.

Third, customers and prospects will be given the opportunity to opt-out of allowing personally-identifiable data to be distributed for external use outside McGraw-Hill Companies.

Fourth, appropriate safeguards will be implemented to ensure the integrity, security, and privacy of this information.

And, fifth, procedures will be developed to allow customers and prospects to review and correct personally-identifiable information upon request while

maintaining the security and integrity of our databases, and without violating contracts with external parties.

Sixth, procedures will be implemented to ensure that personally-identifiable information is used only for authorized purposes and by authorized persons when the information is accessed by a third party outside The McGraw-Hill Companies.

Seventh, additional standards for use of sensitive data will be developed throughout the corporation. For example, sensitive data will not be rented or otherwise made available for external distribution outside the corporation.

In addition, customers will be given the opportunity to opt-out of permitting their sensitive data to be shared among different units within McGraw-Hill. That is, if you provide sensitive data to one unit of McGraw-Hill, you can prevent its distribution anywhere else in McGraw-Hill.

Finally, solicitations and other marketing materials will not be sent to customers or prospects who request not to receive such materials.

Let me flesh out these policies and procedures with a few general observations.

To begin with, an organization's policy is only as good as its commitment to implementing the policy. We have been extremely pleased by the way our people have embraced these principles and demonstrated their understanding that

the privacy issue is critical, both to our values as a corporation and to our continued expansion into the universe of electronic commerce.

Indeed, our Educational Publishing and Standard & Poor's business segments have already responded by creating their own internal teams to develop policies and safeguards to protect the especially sensitive information to which they might have access.

Meanwhile, the mission of our online privacy task force continues as it issues guidelines for company-wide policy implementation. The corporation will maintain a standing committee to respond to questions from our business units concerning the various elements of the policy and to continuously review the policy and amend it when required.

We believe that education is an integral part of the implementation process. First, we must continue to communicate to our employees the urgency with which we regard this issue and make it explicit that progress in implementing a policy will be continually monitored.

There will be audits of these policies. Those audits will be done by the internal audit staff. And that report will be given to the Audit Committee of the Board of Directors so it reaches the highest levels in the enterprise.

Every McGraw-Hill employee is expected to recognize and affirm a code of ethics, and privacy is now included in

the code of ethics.

We must educate our customers about the details of our policy so that they will recognize our commitment to the responsible use of their personally-identifiable information, understand the nature of the information we are collecting, and be aware of the mechanism which will allow them to guide the way in which it is to be used.

Finally, as one of the world's leading information companies, we have a responsibility to demonstrate our leadership by working together with the Direct Marketing Association and the Information Industry Association. We believe that, just as we do, our colleagues in the industry have a commitment to maintaining their customers' trust and that the policy we have developed may serve as a guide in developing other policies.

We are confident that a policy of self-regulation by information providers can be workable and effective. All content providers have a stake in being ethical and trustworthy. All are aware that their customers have become increasingly concerned about the privacy of their personally-identifiable information. For both ethical and business reasons, the industry has every reason to take swift and effective action on this issue.

Government can play a role in facilitating the development of a comprehensive private-sector response. To

use Teddy Roosevelt's expression, government can use its bully pulpit to raise awareness of the issue and educate the industry and the public on the need for responsible behavior.

The FTC has been extremely constructive in this regard, and we wish to commend the agency for highlighting the issue in forums and workshops such as these.

As I indicated, the information industry as a whole has a clear interest in respecting consumer privacy. If in isolated instances a company should violate this responsibility, its misconduct reflects badly on the entire industry, and we would welcome government action to assure the public that its privacy concerns are being addressed.

Finally, the government can play a role by serving as an advocate with trading partners overseas. As you are aware, the European Union has issued a Privacy Directive that beginning in 1998 could limit access to its markets to countries that do not institute privacy protections comparable to those existing in the EU.

Our U.S. trade representatives can make the case that existing legislation in this country, for example, the Telephone Consumer Protection Act, already provides sufficient protection for EU requirements and there is no need for further government action.

In summary, we believe that a policy of comprehensive industry self-regulation can effectively address consumer

privacy concerns. We have formulated and are implementing a privacy policy that may serve as a model for self-regulatory approach.

We look forward to working with government agencies, our colleagues in the industry and concerned members of the public to make sure this critical issue is addressed in the most effective and expeditious manner.

Once again, I thank you for having us here today.

MR. MEDINE: Thank you very much for an excellent presentation. If we could ask maybe a few questions. Chairman Pitofsky.

CHAIRMAN PITOFSKY: Thank you very much. I hadn't heard the proposal before, but my first reaction is it is a very serious and impressive set of proposals.

I wonder if you could say a few more words about the use of sensitive data, which is what people are really concerned about. You had mentioned that if people don't opt-out, that within the company the data will be used for legitimate purposes.

I wonder if you could tell us a little bit more about what the legitimate purposes are within the company for which you would use this sensitive data.

MR. DIONNE: We said for the sensitive part of the identifiable information, they could opt-out, even within the company. But for that which is not considered sensitive, we

would use it.

And the reason why I think it is important for us, to take the most sensitive area of all, children, the more we know as publishers of children's materials about a child, the better we can reinforce instruction that's taking place in the school and help the parent in that process.

If we know something about his interests or her interests, we can pretty much create materials which will be read and of interest. If we know something about how they process information in terms of preferring auditory or visual, if we know something about how the child constructs his mental world in terms of his cognitive style, we can create materials that will educate him better. All of this information.

Now, at present the network is pretty much electronic, but voice is here, multi-media will be here, and we have to anticipate an environment where multi-media interaction among consumers and ourselves is possible. We think it will be here shortly, so we are trying to create policy that will embrace that kind of information as well.

We know that in knowing how children learn and how the curriculum is organized in the school, that when we are organizing information in an electronic setting, we are not limited by the white space of a magazine or a book. We can have incredible depth and we can access other information,

but the efficient organization of that information can best be understood by knowing where a child is in the curriculum.

So we need to have more information about that, if we are to be effective in presenting the information.

We are working on a system of having parental participation in this process. Our concern so far is that with many of the children in America, after school are in the care of adults other than parents. And the question is how do we identify that as a responsible person?

But, nonetheless, the education task force within The McGraw-Hill Companies is looking at this issue as to how to have parents participate in the process.

MR. MEDINE: Commissioner Steiger.

COMMISSIONER STEIGER: Yes. Chairman Dionne, you mentioned that you were extending these privacy protection policies to the sharing of information with third parties, information that might be personal and sensitive.

Can you describe an instance where you would need as a business transaction to share that kind of transaction, and can you tell us what if any safeguards you believe The McGraw-Hill Company can put in place that affect the third party receiving the information?

MR. DIONNE: Okay. Let's stay with children here. The fact of the matter is that as wonderful as we are, we don't have all the information that a child could use. There

are a lot of other publishers that have very valuable resources that we could refer to if they knew about this child and his interests or her interests. So we would share with them what we have learned about this, hopefully.

We know all of those parties, we would select the information carefully. That's in the world of books. In an electronic environment, as we know that it is possible now, and I think you will see a number of schools engaging in this, to create an environment that is controlled but is a look-alike to the Net, in other words, you can access certain Websites but others cannot be accessed, and as a product that will be developed and can be sold, and there is a lot of technological solutions on the way here.

In the meantime, there are strong advisories to parents as to which sites are appropriate. And you have a number of those people participating here and they have done a good job. But there are legitimate reasons for sharing the information.

In return, we will acquire information from others. For instance, we have a process for creating instructional materials that are customized. If a professor says they want to have their own book, we will create it for them in 48 hours and get back to them. It could be a chapter from this book, that book. The books may or may not be ours. They can be someone else's.

And if they have information about that chapter or that book this professor has and how it is best used and what kind of professors found it most valuable, that can be extremely valuable to us.

So we see this as a net positive for everyone. The information is more usable and it is more efficient in its use.

COMMISSIONER STEIGER: But what about let's say a financial, the use of Standard & Poor's, the individual who is going to make use of the new service that you are putting up.

MR. DIONNE: All of that information will be dubbed sensitive data. It is not available to anyone outside of the company, and only available inside of the company to the people who are responsible for the product.

COMMISSIONER STEIGER: There would be no third party involved in that?

MR. DIONNE: No.

COMMISSIONER STEIGER: Thank you.

MR. DIONNE: There will be no third party data in any sensitive data activities at all. There will be no third party sensitive data transactions.

MR. MEDINE: Commissioner Varney?

COMMISSIONER VARNEY: I wanted to echo the thoughts of my colleagues and say thank you very much for coming,

Mr. Dionne. I think your company has shown the way that good business sense also makes good privacy sense.

And if everybody did what you did, we would be out of business, happily, so thank you very much. I look forward to working with your staff and finding out more in-depth how these principles are really working and what kind of problems you are encountering as you try to implement them.

MR. DIONNE: We welcome your visits or anyone else who is interested in seeing how we do it.

COMMISSIONER VARNEY: Thank you very much for coming.

MR. MEDINE: Thank you. Now I would like to call up remaining panel members that may be here, and I would like to next turn to the Direct Marketing Association and its president, Bob Wientzen, who is also chief executive officer.

The Direct Marketing Association is the largest trade association for businesses interested in direct marketing and database marketing, with more than 3600 member companies from the United States and 49 foreign nations. I will add that he has been extremely helpful to the Commission staff as we prepared for last year's workshop and this year's workshop as well.

Give people a moment to settle down. Are you ready?

MR. WIENTZEN: Yes. Thank you. We appreciate the

opportunity to be here today. Clearly these hearings are extremely important to the future of the Internet and, in fact, for the future of electronic commerce.

We have heard already this morning about consumers' concerns about whether their privacy is, indeed, protected online. And we just heard, I think, Mr. Dionne eloquently talk about the commitment his company is making to promote user privacy in an effective commercial way.

Companies that want to build businesses on the Internet must have the confidence of consumers if they are going to succeed, so this is really an economic incentive. There is absolutely no doubt about it. That's why the DMA is committed to helping consumers understand how to protect their online privacy. Along with our members, we are committed to responding to the concerns that consumers express.

Now, I think we have to carefully, however, discriminate between what I think of as fears versus anxiety. Fear is understanding a danger and assessing it and having a legitimate concern about it. Anxiety I think of more as fear of the unknown and concern about the unknown, so part of the job here is to eliminate some of the unknowns, eliminating, reducing the anxiety, I think, is going to help us all.

Privacy protection, on the other hand, doesn't

de facto mean government control. I think we have heard that already.

Everyone, consumers, businesses, advocates, certainly, and government, I think have a role to play in assuring that our privacy is, indeed, protected.

We hope that these hearings, I really believe, in fact, that the FTC can help consumers gain a better understanding of the true state of user privacy on the Internet.

We need to separate fact from fiction and replace some snap assumptions with sound judgment. I think the stakes are high, no doubt about that. If we fail to read the landscape correctly, I think we could easily disrupt the development of a very useful tool for consumers and, indeed, a useful tool for business, which is going to have a significant impact on the U.S. and on global economies.

Most of all I want to do today is help you understand the steps that industry has already taken, at least the steps that we see that have been implemented, and the efforts that we are going to continue to make to do our best to ensure that businesses meet the expectations of consumers regarding privacy.

Now, last year in conjunction with the Interactive Services Association, we presented draft guidelines covering notice and choice at Websites. We talked about unsolicited

E-mail and marketing to children.

In January, this past January, the DMA formally approved these guidelines. And I think you have a copy of them before you. They have been formally approved and we are now educating our members regarding these guidelines.

We intend -- in fact, I can commit to you that we will do our best to enforce these guidelines through ethical peer review processes.

These principles state that Websites should disclose what kind of information they collect, should explain how the information is used and provide consumers with a legitimate mechanism through which they can specify that they don't want information shared with third parties.

We have launched an aggressive campaign called Privacy Action Now. And I am supposed to be wearing a pin. I forgot to put it on. But Privacy Action Now, with the "now" stressed, which I think is important, and what we have done as part of this program is really focus on helping our members understand the importance of this issue.

In fact, it is a new one as it regards online marketing, so we have some educational work to do. Now, as part of that effort we have distributed copies of our online marketing guidelines to every member of the DMA, both here and overseas. We showcased them at every single major Direct Marketing conference that we have had.

I don't know how many thousands of these things we have distributed, but virtually everywhere we go we have distributed them. I think I distributed several hundred in Brazil last week, as an example, at a privacy conference that we held.

We have collected for you today, in addition, already, dozens of examples of privacy notices and consumer choice options that have been posted on the Websites of some of our members and others. You have a few of them in this.

I think there are something on the order of 50 or so that we have already collected. We are in the process of collecting more. It is an ongoing work. I think already we are finding that we see an acceleration of adoption of these principles, and that's very important, but we also know that this is just the start.

We know that many of our members are still new to these issues and, in fact, the whole issue of online privacy. We have begun to contact sites that are not in compliance with the guidelines to help them understand what they need to do.

In fact, we are working aggressively to identify those that simply haven't gotten the word, no matter how hard we try. I think we will make a difference.

We have also organized 22 other direct marketing

trade associations from five continents into an International Federation of Direct Marketing Associations. And we have agreed to work on joint self-regulatory principles as part of their joining this organization.

Now, it is important here to note that the reason we are doing this is because, as you know, the Internet is a worldwide medium and a worldwide marketplace. So in implementing guidelines, I think it is foolish for us to simply look internally to the U.S. We have got to look beyond our shores, and we are in the process of doing that.

I was delighted in Argentina last week to already see a Spanish translation by the Argentine Society of our guidelines which were handed out in the conference that I attended there. The DMA has had an ethics peer review process for 30 years now. Its purpose is to bring companies into compliance with our guidelines.

We have a committee on ethical business practices which gets complaints from members, from staff, consumer organizations, and from the public. We contact the company, as soon as we get the complaint, and we call for change. If our requested changes are not made or, rather, if they are made first, we will handle those, we close the case, and that happens the majority of the time. If they are not made, there is indeed action that we can take.

The committee can refer the case to the board of the

DMA. And in the case of a member we can, in fact, expel the member from our association. In fact, we have improved that peer review process just recently. We are now releasing a public document three times a year that describes all matters considered by the committee on ethical business practices, the practice that was in question, and violations that the DMA found. And this is one of those guidelines and you have a copy of it there in front of you.

We recently have given the committee additional authority in dealing with future cases to release the names of companies that refuse to comply with our guidelines. That's a major change. We are, in fact, taking public those companies that say that they simply cannot abide by those guidelines.

We have also provided support to the World Wide Web Consortium and the Internet Privacy Working Group to help promote the development of technology to support a seamless communication of consumer privacy preferences and Website information practices. I know we are going to hear a lot more about that later today and perhaps tomorrow.

There are many exciting things happening in this area, and I think Joe referred to some of that earlier. We know that technology companies are already responding to consumer privacy concerns through their own product development. Many, many more are on the Web.

We have also taken some proactive steps to respond to concerns about unsolicited E-mail marketing and marketing of children online. And we will provide a lot more information about that during pertinent panels of these hearings later on.

For more than 30 years, as I indicated earlier, the DMA has also worked to promote confidence in the direct marketing business. Effective self-regulation to date has enabled direct marketing to become a $1.1 trillion business. Given the chance, we believe that self-regulation will enable online commerce to reach its full potential as well. And I think that is a vital premise we need to keep considering.

The DMA has always supported disclosure of information collection practices and offering consumers the opportunity to limit how their information is used. To that end, we have assembled detailed information on our Website to help consumers, particularly parents, understand how they can protect the privacy of their family. You have heard the importance of that earlier.

These efforts include links to all of the major parental control software tools that parents can use to help protect their children's privacy, so we have got a list of them. If a parent comes to our site they can have a choice and go directly to any of those software sites and get information that they can use very easily, I think, to deal

with some concerns about children's privacy.

Also today I am very pleased to be announcing the release of a new booklet entitled Get CyberSavvy. This is specifically designed to head the digitally-challenged parents, and I know there are many of us, understanding privacy and safety issues online.

Get CyberSavvy has been put together in conjunction with the Children's Advertising Review Unit of the Council of Better Business Bureaus and the consumer group Call For Action.

Copies are available through the DMA offices and the text in its entirety is available on our Website. A parent can print this booklet directly on any home printer so there are lots of opportunities here for parents to get information on how to be comfortable in dealing with the Net.

We think consumers need to understand the information that is collected about them and express their choices about how it is used. We also believe that many of the new companies that are springing up on the Internet are very new to these issues and may need help to understand how they can and should respond. That's why we have devoted the effort to develop a tool on our Website to help other Websites create online privacy policies for their site.

You heard earlier today about the importance of sites having a policy, expressing it so consumers at least are

aware that there is an issue. We think this is an important contribution to making that happen. We believe very strongly, in fact, we are going to aggressively posture ourselves as requiring that sites have a posted privacy policy, whether or not they collect any information, and that's going to help consumers feel comfortable, that there is not a question when they go to a site, they will know do you or do you not collect information?

So we think we can cut through some of the hype and hyperbole with this and help consumers understand exactly how Websites are using their information, if, in fact, they are using any information at all.

A great deal of the Websites out there are not using information. They are either not sophisticated enough or they don't really have an interest in it. But consumers have to know.

It costs nothing to use this tool. It can be used by everyone from the largest Fortune 500 company, and there have been several who used it already, down to the smallest nonprofit association. If a company is found to have made an inaccurate representation in expressing these policies, we think it would be subject to the FTC's regulation about deceptive practices.

If you get online and express what your policies are and you don't follow them, we think you could be subject to a

deceptive practice charge. By using this tool to demonstrate how the tool works, we will show you steps taken by the Disabled American Veterans, a DMA member, who used the tool recently to develop the policy that you will find, I think, in our compilation of policies in the large book.

So the first thing that happens, I think, as you see is that when you come online, you are asked to provide information about who you are, your E-mail address, your name and address and so forth, so we in fact, know we have a policy statement that clearly states who you are dealing with. In addition, we are asked, the system asks you to respond to a number of questions that basically help us compile the things that you do regarding both the collection of information, the use of information, and any dissemination of the information that you collect.

In addition, we ask questions about how you are going to allow consumers to opt out of the process. Are you going to give them choice? So we have covered the areas of notice, we have covered the areas of choice, and we provide various mechanisms for opting out.

When you get through with this policy, answering all of this questionnaire, if you would, online questionnaire, you are asked what kind of output do you want? In one instance you can ask to get the output in a form of completed computer programming so that, in fact, it can be posted

directly to your Website and we will show you what that looks like in a second. You can print it out, if you like. You can review it. You can send it to your attorneys so that they can fine-tune it or whatever you like.

The reality is that you have most of the work done for you and you have lots of options regarding the output. So I think you will see in a second here what it looks like after you have -- after it is a written policy, if you would, so now we have a written policy, it has some hypertext in it and so forth.

Once that policy has been finalized, you can then post it directly to your site. And you will see here in a second we will have, in this case, the DAV's policy complete with graphics and complete with hypertext so that it is a fully operational policy. It provides all of the elements that are custom to that particular enterprise and at the same time it has made the work very, very easy, very, very quick. And I think there can be little reason for folks to feel as though it is too difficult to do or it is something that they don't want to get involved in.

MR. MEDINE: I hope it is more apparent than it is on the screen, but I suspect it probably is. It is anonymity, not privacy.

(Laughter.)

MR. MEDINE: We would like to ask you a couple

questions and get on.

MR. WIENTZEN: I have one last comment. We are going to take all of the energies that we have and do the best job we have to kind of continue a process that was started 30 years ago to make sure that self-regulation does work. And the reason is simple. It makes good economic sense.

It isn't a matter of altruism. And while it is consistent, certainly, with public policy and ethical behavior and so forth, the reason that we think this makes sense is because without the trust of consumers, we are not going to develop an interactive commerce business that we think has a potential to change the way Americans shop.

If, indeed, we can provide adequate opt-out choices for consumers, we are confident that this will be a change that will produce significant business and lead to the development of the Internet as well.

MR. MEDINE: Thank you very much for your presentation.

MS. LANDESBERG: Mr. Wientzen, I have two questions. First, your marketing online privacy principles and guidance are not mandatory at this point for DMA members.

Wouldn't your enforcement activities be enhanced if you made them mandatory?

MR. WIENTZEN: Well, I suspect they would be, indeed. As you know, there have been a number of questions

in that regard, including questions of antitrust activities. The chairman recently addressed those questions in a speech he gave before one of our conferences, and I think both those comments and the discussions that we have been having as a board have led us to explore that possibility, which is currently ongoing.

MS. LANDESBERG: Finally, your commentary states DMA's Guidelines for Personal Information Protection apply in all media. They too are permissive. A 1997 study commissioned by the DMA found that fewer than one-third of the DMA members surveyed have implemented the privacy mechanisms set out in the guidelines.

What do you think accounts for this finding and what does it say about the future of self-regulation in your industry?

MR. WIENTZEN: Well, I think the first thing you need to recognize is there is a difference between the number of companies adopting the guidelines and the amount of the information or the process that's being covered by the guidelines.

I would counter, not to indicate that the numbers that you described are inappropriate, but the fact is that about 95 percent of the "large companies" that are members of the DMA are following the guidelines. The best evidence that we have, and it comes from the same survey, indicated that

somewhere between 90 and 95 percent of the material that goes out is distributed by companies that are following the guidelines.

The big problem we have at the moment is two pieces. One, a lot of new companies that come on board do not start out recognizing that they have to deal with this issue. They are either too busy or simply don't understand.

No. 2, a lot of very small companies have felt that it is inappropriate or it is unwieldy or they simply can't afford to do some of the things that we think are necessary. So, indeed, we do have a lesser number of companies than we would like adopting these policies, but on the high side I think the issue is we do feel as though most of our large members are doing it and most of the material that is being sent out is covered by it.

MS. LANDESBERG: Thank you.

MR. MEDINE: Commissioner Varney.

COMMISSIONER VARNEY: I know you are trying to move quickly through everybody. I want to say for the benefit of everybody in this room, whether or not you all agree with every single thing that's in the principles, DMA has worked extremely hard to put them together. I think we all recognize it is a starting point.

I think, you know, when the disadvantage of stepping up to the plate like our friends from LEXIS-NEXIS did

yesterday, when you step up to the plate you keep getting whacked a bit. Now we are going to lean on you to get them broadly implemented. Some of us are going to like to see them broadly implemented.

Whether or not that's mandatory or whatever mechanism you get them broadly implemented, we are going to want to look at what is the consequence to the industry? I mean, are people taking these policies, are they putting them on their Websites, are they adhering to them? What percentage are? What aren't? What is the consequence for the business? What are the economic dynamics when you look at your companies that do have privacy policies and those that don't?

So I want to really emphasize how impressed I am that you have put these policies together. I think it is the beginning, it is not the end, and I look forward to continuing to work with you.

MR. MEDINE: Commissioner Steiger.

COMMISSIONER STEIGER: One very brief question. Thank you for all of your work and all of the continuing intelligence and expertise you are providing for this Commission.

I do have one question on an admittedly very quick-look at the sample outline, which I know we will find useful. I see repeatedly flagged check this box if you would not like to receive news and information from X. Do you

consider that privacy protection? I don't see anything else that says if you don't want your information used, let us know.

You don't presume, I trust, that whether we wish to receive or not receive information is an adequate notice of the use of our questionnaire if we fill it out?

MR. WIENTZEN: Not at all, Commissioner. That's simply one element of a multiplicity of elements. We do provide the consumer the opportunity to say I don't want the information, don't transfer the information, I don't expect that you are going to be able to do anything with it beyond the purpose for which it was originally acquired. That's just one element of a company's statement.

COMMISSIONER STEIGER: Thank you.

MR. MEDINE: One of our tasks, at least from the staff point of view, is to evaluate how far self-regulation has gone in the two years we have been looking at this issue and you have demonstrated impressive efforts to try to facilitate companies having privacy policies that are effective.

What benchmark would you set for your industry in terms of adoption of privacy policies? Should we look at two months, six months, in a year? What point should we be able to surf the Web and find that a vast majority of DMA members have stated privacy policies?

MR. WIENTZEN: The first thing we are doing, David, is that we are going out and talking to our members and asking them to sign on, literally sign on. We are in the middle of that process. We have something just under half of our members who have literally signed a statement saying I think these are great and I am going to adopt them, count on me, that sort of thing.

We are publicizing it in that way. And I think we are halfway there already, after less than a year. Secondly, we are policing, if you would. We are sitting down and doing what you are doing. We are looking at sites, we are calling them up. I think we did 80 or 90 last week. And we are just getting it rolling.

So my suspicion is that next year at this time we are going to be looking at something on the order of three-quarters to 80 percent of our members who are going to have policies and who are going to be doing their best to enforce them. That doesn't mean, you know, that it is going to be a perfect world because this is a business.

As somebody said earlier, that's changing so fast, companies are coming on board so quickly that it is a constant education process. I don't think we are going to get to the point where we are at 100 percent, maybe never, because of the educational requirement that's going to be part of this thing.

MR. MEDINE: Thank you. Commissioner Azcuenaga.

COMMISSIONER AZCUENAGA: Just a minor comment. I think these hearings have been so wonderful, there is enormous value to a bully pulpit, and I think the Commission has done a great deal to get dialogue going and to educate ourselves and to have various groups with various interests educate one another.

I am very delighted at the progress that has been made, some of which has already been described here this morning. I do have to say, however, that although Commissioner Varney was very careful to speak only for herself, that in terms of leaning on you, we have no authority to do that.

However, we are going to continue to watch over this. And we do still have some role to play in continuing the education, No. 1, and possibly making recommendations to the Congress. So as you go forward I hope having learned more from these hearings as we have, perhaps enforcing your guidelines, perhaps making them mandatory, that's all to the good, but you should do it based on your own understanding. We have no authority to force you to do that.

MR. WIENTZEN: I certainly would like to encourage your helping to push us, if you would, and partner with us in this process of education. Getting the word out on this kind of information or on the guidelines is a cooperative effort,

so we would appreciate any help we can get.

MS. BERNSTEIN: That's exactly what I was going to ask you about, Bob, knowing the answer. We have had such a good partnership with you and education in other areas that I am assuming that you would be again happily partner with us in the overall public education to guide these issues.

MR. WIENTZEN: Absolutely. I think the research we heard this morning really highlighted for me what I already recognize, and it really strengthened the fact that an awful lot of people are not aware, people who are on the Net as beginning commerce entities, they are simply not aware of the fact that this is a concern, or if they are aware of it, they are too busy to focus on it.

I think education will cause them to focus on it. And then we give them the tools. I hope we have got some of the tools, and we will have more this time next year, we will have a lot more.

MR. MEDINE: Thank you very much, again, for your presentation. Let me next turn to Esther Dyson, who is the chairman of the Electronic Frontier Foundation, a cosponsor of eTRUST -- now we have been told TRUSTe -- and president of EDventure Holdings. She is writing a book about digital age issues including privacy self-regulation.

MS. DYSON: Good morning. I am very pleased to be here. And what I am going to do is talk quite briefly

because I hope to be -- hope to provoke questions, rather than answer them all in everything I am going to do.

TRUSTe, which was born as eTRUST, but we observe intellectual property and, anyway, we gave it up to somebody else, TRUSTe, it is not so much an attempt at self-regulation, we believe that the alternative to government regulation is not really self-regulation but it is customer regulation.

What we are fostering is the concept that customers should be informed and that they should themselves regulate the vendors they deal with by choosing whether or not to do business with them and on what terms.

So as it says here, we have got a privacy program that provides a standardized method for assuring customer control of personal data to informed consent. We do not assure what happens. We assure customer control, what happens. I think that distinction is very important.

We firmly believe not all customers have the same preference, each individual customer may have different preferences about different kinds of data, different preferences according to the vendor they are dealing with, so what we are trying to do is create a decentralized market, decentralized enforcement mechanisms.

We are bringing in validation partners, accounting firms, starting with Coopers & Lybrand and KPMG but we hope

extending to others.

In the proper spirit of the Federal Trade Commission, we welcome competition. We don't want to be the only guys out there. And we really do hope there will be other such systems. With that, let me go through the slides.

We came up with something very specific, tangible and practical for how to accomplish this. We have what are called trust marks. And we license them to people with Websites. And they can put up these trust marks on their Websites after going through a process of validation with us.

They can also use different trust marks at different places on the site, in which case the overall trust mark for the home page is, of course, if you like, the broadest trust mark. If anywhere on your site you collect data where you allowed third-party exchange, that has to be the initial trust mark on your site.

I trust you can read these. They say no exchange, no personally-identifiable data are used by the site at all. One-to-one exchange, they are collected only for the site owner's use in communication with that particular customer. And third-party exchange, that's kind of, let's face it, the Pandora's box that raises further questions. We will use your data and we will give them to third parties and now we are going to explain to you how we do it, so you have a

choice.

And I could imagine a Website where they had a choice of, you could select one box where they have third-party exchange trust mark and another where they did not, so that the consumer would have the option of what terms they want to do business under.

This is our own Web page just telling you welcome, listing our sponsors, doing the usual commercial things. And here is the Web crawler page. Down at the bottom you can see the eTRUST trust mark, and next you want to know specifically -- did I say eTRUST?

COMMISSIONER VARNEY: You did. That's okay.

MS. DYSON: May lightning bolts strike me. Here you see down at the bottom specific information about what it is that they collect and what it is that they do. And that's what we are encouraging all our licensees to do.

And it goes on. Here is what we did. Here is who we share it with. In this case we don't share it with anybody else. You can opt-out. The consumer watchdog, this is a page you can go to to post if you have any problems and so forth and so on.

This is how we actually do our dealings with the Website that uses our trust marks. This is very different from content control. Content control is an interesting thing because you can go to a Website and see a dirty picture

there, you may argue about how dirty it is, but it is visible. With privacy you don't know what happens behind scenes. You can't look at the Website and say, uh-huh, you can tell they are collecting your data but you can't tell what they are doing with it.

So we go through a process with the Website owner and they actually run through a checklist with us, they complete legal agreements so we now have a legal, they now have a legal obligation to abide by the statements they are going to make and, therefore, they can be accountable to the FTC if they do something bad.

And the one thing we do is we see the site with false data. We learn from our friendly commercial partners when somebody has a mailing list and they want to know if it is being misused, they put fake data in it. Then they see if the data are being misused. For example, I may sell a list for one time use. I put my mother's name in. If my mother gets two pieces of mail, I know my trust is being abused, and we use that same procedure with eTRUST to ferret out misrepresentations.

We also do spot audits where we actually call in an auditing firm to look through the data processing system the company uses, what they actually do and so forth and so on. And we encourage our larger sites to do this any way with the help of Coopers & Lybrand and KPMG. It is much like a

financial audit.

They come in, they check your books, they look at your computer systems, they interview your employees, they see what really happens and make sure that not only do you not formally use the data in the wrong way but your employees are properly trained and they don't give information out to strangers and so forth and so on. Then you get your TRUSTe marks.

I went through this already. Now if somebody is found not to be behaving properly, the remedies begin with breach of contract with us, with eTRUST. If somebody doesn't have a contract with us, but they were using the trust marks anyway. That's a trademark infringement. And, of course, there is fraud or deceptive practices when they are making misstatements.

This is our broad, but we hope growing industry support. And beginning today TRUSTe is available for commercial use. It is not restricted to the United States, as Mr. Wientzen said, this is a worldwide Net and we can neither rely on nor can the industry be regulated by a single government. So we are very happy that our trust marks are valid even if you are doing business with us from, for example, Russia.

I would like to make just a couple more points. First of all, we see ourselves as very complementary to the

people you are going to hear this afternoon. Our system is about disclosure and about validation of the representations that people make.

What is also necessary and valuable is ways of representing this information electronically so that a person can, for example, set his Web browser to deal only with sites that follow certain privacy practices.

So you can actually set your browser up to negotiate automatically, just as you can set up a browser not to down-load any dirty pictures, you could, for example, protect your child from. Some day we hope to have a child trust mark. You could limit your child to visiting only sites that had, for example, a child trust mark.

We believe that this is an important thing for commercial outfits, but we would also encourage the government to use it.

The people that we are working with now, they are commercial organizations. You have a choice as a consumer whether or not to deal with them. There are many government organizations where you do not have any choice, but it would be nice if you at least had a choice about whether your data was used only by the Department of Motor Vehicles or whether they were also sold by the Department of Motor Vehicles to third parties.

So I would encourage the government itself to adopt

this system or something similar to help set the path for the commercial sector. And I would be delighted to answer questions.

MR. MEDINE: Chairman Pitofsky.

CHAIRMAN PITOFSKY: I think your whole approach to this is very appealing, which is to put consumers in a position where they can protect their own interests and that's something that's very consistent with many things that we do here at the agency.

But zeroing in on the mark, which indicates that the information that is provided in the course of doing business could be sold to some unknown third party, it seems to me your choice when you see that mark is either not to do business with that company or to go ahead and do business and run the risk of some personal information will be sold.

Am I wrong that you could do business with the company and still opt-out from allowing your personal information to be disclosed?

MS. DYSON: Yes. Let me run through it again. First of all, I come to a site and the front page says some third-party information may be exchanged. And so I say hum, I would like to know what third-party information is going to be exchanged and with whom. And this is not required, but clearly we encourage further disclosures to be made as you saw at the bottom of the Web crawler page.

And we encourage the sites to allow the customers. You can have opt in or opt-out as well. It is an overall notification: Hey consumer, ask a few more questions, maybe they are going to offer you a choice, maybe your only choice is not to do business with these guys, but at least you know what you are getting into.

What we don't want to do is have 49 different trust marks and confuse the matter, partly because each company is going to have different categories, different kinds of information they collect. I don't mind if the flower company sends information about what kind of flowers I like, but I don't really want them sending out the information about who I sent the flowers to because, you know, maybe my fourth boyfriend will find out about the third one or something like that.

So you want to give the site the encouragement to disclose more information but you don't want to make it too confusing up front. In a sense, the third-party exchange trust mark is a yellow light that says caution, ask more questions.

CHAIRMAN PITOFSKY: But the burden is on the consumer?

MS. DYSON: Yes.

CHAIRMAN PITOFSKY: What is the reason for not having a sort of sub-A under the third trust mark, the mark says it

might be sold to a third party and then there is something you click on and you say count me out?

COMMISSIONER VARNEY: To add to that, why as a policy reason, why wouldn't TRUSTe require anybody who is going to participate in their program to offer opt-out as a condition of participating in the program?

MS. DYSON: We frankly believe in customer choice. Put it this way. If companies find people don't want to do business with them on the basis of free exchange, they will offer that option. We do not make it a condition because we don't think it is necessary, to be honest.

I would encourage it, but there may be some cases where, you know, what we are trying to do is create a clear and well-lighted market. We are not trying to restrict, we are trying to foster honesty. And we are trying to foster the ability of the consumer to make a choice.

And, yeah, I mean, clearly there are things we like better than other things but no, we don't make that a condition of the third trust mark. We do for practical purposes say you should disclose further what it is you are going to do.

MR. MEDINE: I guess looking at the analysis from last year's report, which had four guiding principles of notice, choice, access and security, it would appear that TRUSTe really only just partially addresses the notice issue

and not fully because it doesn't necessarily require full disclosure of all the information practices and it doesn't address choice at all.

MS. DYSON: It addresses choice to my mind perfectly well because the customer can decide they don't want to --

MR. MEDINE: The choice is really all or nothing. There is no middle ground. I would like to do business with you, but I wouldn't like you to -- I don't want to share this particular information with you for use with third parties.

MS. DYSON: No. I beg to differ. There is a range of how it works. A site may or may not offer very, very specific and detailed choices. We do not require them to do that because we believe the range of choices is going to vary so much from site to site that trying to require it ends up being overly complex because there is always the choice to say no, I do not want to do business.

When you get down to I want to do business under certain conditions, then that's going to be site dependent, and that's where we think that our licensee should decide what options to offer and let the customer choose whether they are acceptable.

MR. MEDINE: One of the things we have learned as a technological matter is that the minute you hit a site, certain information about you can be obtained, not maybe your identity but your domain, something about your Web browser,

where you have been on the Web.

That would occur at the same time that the consumer is getting the disclosure of the trust marks, they are also having their information captured by that Website. Does TRUSTe have a policy or require a policy by Websites to not use that information that they gather on the first hit because a consumer hasn't had a chance yet to get the disclosure of the site's policies and hasn't had a chance to exercise their option of not doing business with that site?

MS. DYSON: That's a very good and very obvious question, and I am embarrassed that I don't know the answer, but clearly that should be one of our policies. I hope it is. But my TRUSTe trustee isn't here. That makes an awful lot of sense.

MR. MEDINE: Director Bernstein.

DIRECTOR BERNSTEIN: Have you had an opportunity to ascertain the level of acceptance of the system? I understand it is just beginning, but I thought perhaps you had either tested it or done focus groups or had some empirical knowledge about the level of acceptability.

MS. DYSON: We are doing a lot of fooling around with it in various ways, seeing how the process works, trying to find out how much it costs to go through all these things, trying it out on people, but we can't give you any real good solid statistical information, unfortunately. We are just

starting.

Some things seem obvious, but we haven't tested it on a random user population, and so we can't give you that. Obviously we are trying hard to make this something that is trusted at both ends.

I am very concerned that we have strong enforcement because the value of this trust mark can easily be destroyed if we are not careful.

MR. MEDINE: Commissioner Starek.

COMMISSIONER STAREK: Your program sounds to me to be somewhat similar to the Better Business Bureau online certification program. Although I guess the difference would be that theirs is trying to assure consumers who are engaging in electronic commerce that they are participating with a reputable company as opposed to one who protects privacy.

Is there any coordination or have you done anything together with BBB's online program?

MS. DYSON: Not specifically. We would like to work with everybody in this room, the DMA, the PMAA, the Better Business Bureaus, everybody, but we are a startup. It has been hard to get respect. And so we are very happy to be here.

COMMISSIONER STAREK: The program that you have outlined certainly in my view commands some respect. I had one other question.

You mentioned in your remarks, if I heard you correctly, I thought you said governments couldn't regulate or legislate at this time or regulate the Internet because it is a worldwide system here. I wondered if you could expand on that. Exactly what were you thinking when you indicated that governments don't have the authority to regulate the World Wide Web?

MS. DYSON: Clearly governments have the authority to regulate businesses and so forth and so on. The thing I am thinking about is if somebody sets up shop in Antigua or in Russia or Yemen or should they ever have an Internet in North Korea and starts sending or making fraudulent offers to American consumers, you are going to have a tough time going after those guys in North Korea.

There are obviously various kinds of treaties and so forth and so on, but it is very difficult.

And this is the same issue when you are talking about dealing with the European Union. You are now as an American vendor, you are de facto making offers to French consumers which may be against French law.

A friend of mine got into a big fuss because he was trying to -- he was a British resident and trying to buy stocks through Etrade or something like that and the Brits didn't like it, so it creates a lot of complications. And that's why these systems that are -- instead of being

geographical jurisdictions, are actually worldwide and operate by contract between the customer and the site and between the site and call it the certifying authority, make a lot of sense.

Clearly we welcome the United States' endorsement and so forth and so on, but there are interesting problems that are going to arise in this area.

MR. MEDINE: Commissioner Varney.

COMMISSIONER VARNEY: Esther, have you given any thought to how the symbol gets displayed when people are surfing the Web and you are hot-linking in and out of various sites? I think Tara and I were talking this morning about on the Web, you don't always enter every site from top down, so if you have a front page that has a trust mark, that may or may not be where you come in.

What are your views on, you know, should we all just be careful to go to the front page first or should Netscape and Microsoft think about making space on the top of every page for any mark?

MS. DYSON: We would love for them to do that. Screen real estate is getting limited, is the problem. I think clearly as I mentioned anything that is worse -- your home page is going to have your worst trust mark on it, so to speak.

We do not yet, I believe, have a policy of putting

the trust mark next to every point where you collect data because, again, there are issues of screen real estate, but it is a very good question. And these are the kinds of things we are going to be wrestling with over the next year as we roll out more fully, we have been doing some of it, and seeing what happens.

I also want to just quickly go back to a previous question, the issue of when you even land on a site and you get this third-party exchange problem, that's why we need things like P3 or the open profiling system so you can avoid even getting to the site if you really don't want to deal with it.

MR. MEDINE: Thanks. We will be hearing from P3 later and get a sense of the interaction between the two technologies. Thank you very much. This was an enlightening discussion.

We don't have much more time left, but I would like to press on with Jeff Richards, who represents companies in the field of Internet and online services, the Interactive Services Association. ISA has -- I think, Jeff, you can stay at a microphone.

My understanding is, to summarize ISA's policy along these lines, is to require disclosure of information practices on Websites and to also, if personal information is collected, to indicate what the nature of third party use of

that information is and also provide an opt-out mechanism. Is that basically correct?

MR. RICHARDS: That's basically correct. We moved, let me talk about opt-out for just a moment. Within the association there has been a vigorous debate about whether opt-out in itself is the final solution, whether opt-in is preferable and, in fact, it goes back to a theme we have heard over and over today: Is consumer choice, and better than that, informed consumer choice, contracts between consumers and providers and the like.

Perhaps it is my background as a health educator that makes me realize how complicated information today that is presented and how much through marks, through simple language, through making concepts clearer and recognizable, how much basic education needs to be done by industry and providers today, and so ISA's members realizing, I believe, that disclosure is key, believe that choice is key.

MR. MEDINE: And does ISA require that its members adopt these practices online?

MR. RICHARDS: We don't require it at the moment. Frankly, we have just released our new guidelines. We did ours last year with DMA, and now we have sharpened our concepts.

And so we are in the process of getting member feedback and we expect to see tests again. We are very

serious about this. We need to see how disclosure actually works. We need to understand what choice means when it is uniformly applied within a reasonable framework that an industry and association can do. So we hope to report those results to you and others as we achieve them.

MR. MEDINE: Do you know today what percentage of ISA members are complying with the guidelines?

MR. RICHARDS: We have just released them three weeks ago.

MR. MEDINE: Last year's guidelines?

MR. RICHARDS: Last year's guidelines. Last year's guidelines were broad in application. That's, in fact, why I don't think we saw lots and lots of our members adopting them in a uniform way that we could identify and catalogue, which is why we went back to the table and said let's get clearer about these principles. Let's simplify it to the concepts that we can actually test in practice.

MR. MEDINE: I guess the same question I asked Bob Wientzen, what is a good benchmark for our determining whether ISA members have gotten the message and are starting to comply with these procedures? At what point should we be able to surf around and see a high degree of compliance by ISA members?

MR. RICHARDS: This year will be the important first part, which is making sure this is working, making sure that

we actually get consumer feedback on choice and on disclosure. By this time next year I think we will see wide compliance because we will have tested this in real practice.

MR. MEDINE: We look forward to continued efforts on your part.

MR. RICHARDS: Great.

MR. MEDINE: Katherine Krause is here, a senior attorney with US West and is chair of the Information Industry Association's Privacy Committee. And I assume you are primarily wearing your IIA hat for the moment.

MS. KRAUSE: Yes.

MR. MEDINE: What is IIA doing in this area and what percentage of adherence among IIA members should we be looking for?

MS. KRAUSE: I think I should begin by mentioning that although I am sitting here in this online hearing, one of the things we have talked to David and his staff about is that IIA is not particularly an online organization. And so the self-regulation issues that are being addressed from yesterday through Friday generally are of interest to us across the board.

IIA first adopted fair information practices and principles in a formal way in 1994. It has got over 500 member companies. It is very diverse in terms of its

membership with online and off-line providers, commercial and customer providers, database companies and retailers, print and electronic medium.

One of the things I think you are seeing both yesterday and today is a tendency for some of these privacy principles and guidelines to develop in niche markets and niche industries, so you have an Interactive Services Association principle and you have the eight members that were here yesterday with their kind of lookup service principles. And you have DMA, which is a little bit broader, but, again, directed toward marketers.

So one of the challenges when IIA first put its privacy principles and fair collection practices together was to try and come up with principles and guidelines that actually addressed the diversity that I just mentioned to you.

Many of the companies in the association, in fact, have adopted the OECD guidelines or had signed on to the guidelines in the '80s. That was our starting point. It served us very well in terms of coming up with notions about no secret databases, which was taken to the Privacy Act and then modulating the OECD guidelines, so those have been in place since '94.

They are currently being revisited, in part, because during the course of these hearings and hearings last year

and conversations with staff personnel I think there are concerns that the principles don't address every aspect of what people think ought to be addressed, even if there is just a narrative statement saying how the association addresses it.

I don't have any metrics for you, David. Again, the association is terribly diverse. I do have one thing to say that kind of echoes DMA, however. In part, this may be because of my geography. As I told you, we are in the middle of the country where you just don't see this on the front page every morning, but the larger businesses are easier to sign on to some of these things, either because they are associated with other larger businesses that have also signed on to them or because they see that as both an economic issue for them or because they feel it buys them something in terms of the regulatory postures.

Smaller companies very often don't see the need for these kinds of policies or principles without, as has been stated, some real clear education. And even then if their customer markets are not clamoring for it or if they don't serve consumer mass market customers, it is oblique to them, so there is still a great deal of education that needs to be done in the associations, I think, with regard to the smaller companies and that, I would assume, because IIA does have lot of entrepreneurs in smaller companies, would take us a little

more time.

MR. MEDINE: You had indicated in your comments you were in the process of revising your guidelines. Two questions about that. One is do you have a sense of when you are likely to complete that process of revision and, second, do you plan on specifying in greater detail the type of notice you expect your members to provide to consumers about information gathering practices?

MS. KRAUSE: We are halfway through with the first round of discussions about the guidelines, meaning we have made our way through half of the guidelines.

My guess is after we make our way through the second half there will be an iteration which will then go back on the table and we will start all over again, probably because frankly we cut off discussion on the first three after like 12 and a half hours. So we are moving through.

I hear people talk about this time next year. My guess is we will be there before this time next year.

The issue you raise with regards to notice is one of the issues where people have suggested that perhaps this document needs to be more articulate and more expressive. I don't know how detailed we will be with respect to what the notice says. We may go with something as simple as full and fair disclosure. But those are things that really need to be discussed within the association.

And the models that are being discussed here certainly provide any business with ample tools to do a full and fair disclosure without an association, on giving them a legalistic description of what that is supposed to look like.

MR. MEDINE: Thank you for a progress report on IIA's efforts. I want to turn now to --

MS. KRAUSE: In closing, could I just say I think it is absolutely obvious from the last two days that the question is not whether self-regulation can work, but it is a clear demonstration that it is working, that it is flexible, it is timely, it is responsive, and I just want to say that I think it has been a very impressive showing about how it is working.

MR. MEDINE: Thanks for your comments. Turning to Bill Randle, Senior Vice President and Director of Marketing and Strategic Planning at Huntington Bancshares. He is also here on behalf of the Banking Industry Technology Secretariat or BITS.

And I guess the question for Bill is where is the banking industry on some of the issues we have heard about today in terms of self-regulation and enunciation to consumers of information gathering practices and offering consumers some degree of choice in that area?

MR. RANDLE: Thank you, David. First of all, let me

say that historically banks have valued their customers and the very special relationship that they have as someone entrusted with the financial resources of the individual but also the information that goes along with that.

As such, I have worked with several banking organizations in this area over the last two years. The Consumer Bankers Association and the Smart Card Forum, both of which in the last year have issued guidelines on information and privacy.

But more recently, as mentioned, I am working as an advisor to BITS, the Banking Industry Technology Secretariat. First of all, let me explain what BITS really is.

About two years ago the Bankers Roundtable, which is an organization of the top 125 banks in this country, employing about 1 million bankers and representing 70 percent of the assets on deposits of this country, formed a task force on technology.

Frank Votes, the chairman of Huntington, chaired this task force, along with Ed Miller, vice chairman from Chase, who was cochair.

In the fall of last year we established BITS, which is a Banking Industry Technology Secretariat, but more importantly established a Board of Directors made up of 12 individuals. The CEO's of ten large banks that you would

recognize, Citicorp, Chase, Bank of Boston, Huntington, NationsBank, First Union, Norwest, Bank of America, Mellon, BankOne and also representatives from the ABA or the American Bankers Association and the IBWW or Independent Bankers Association make up the 12 member Board of Directors of BITS.

It is important to note that this is a separate board apart from the Bankers Roundtable and is charged primarily with supervising the issues I am about to enunciate. But more recently in April of this year we hired a CEO of BITS, and that individual is Katherine Allen, former exec at Citicorp, formerly head of the Smart Card Forum, and more recently president of the Santa Fe Group.

Now, the objectives of BITS are simply as follows: One, to accelerate the establishment of new electronic payment and product delivery systems through the development of interoperable specifications and standards that will address privacy, security, transaction protocols, and operating rules for electronic product delivery and payment systems.

Two, to create through a certification process for providers of banking products an environment for a safe and secure electronic infrastructure that will enhance bank brands and respect consumer privacy.

Three, to enhance consumer confidence via an acceptance mark. An acceptance mark, somewhat similar to

perhaps some that you have seen, but one that would be related particularly to the payment system, the future payment system of this country, and to evaluate the feasibility of an industry-driven payment certification authentication system and real-time settlement.

Now, these are very broad objectives and they do address the future payment system, I believe, of this country. But on a broader issue, if BITS does its job correctly, and I have every reason to believe that it will, we are addressing not only the payment system of this country but if the job is done correctly, and it should be, I hope, the future payment system on a global basis for all electronic commerce.

If the job is done correctly, I believe that the countries of the rest of the world who are interested in global commerce as much as we are will follow some of the examples that I have just enunciated. It is a very serious project, and that's why the CEO's of the banks I identified are the members who participate on the BITS board.

It has the very highest level of attention within the industry. And you will see some action on this before the end of this year. Thank you.

MR. MEDINE: Thank you. Along those same lines, for those of you who have a continuing interest in privacy issues, on July 17th the FTC will be hosting a workshop on

behalf of the Interagency Task Force on Consumer Electronic Payments to address privacy concerns and the whole area of the developing electronic payment systems.

Thank you very much.

Let me turn to Ronald Goldbrenner, who is sitting in for Linda Goldstein who has had some plane difficulties. Mr. Goldbrenner is general counsel of the Promotion Marketing Association of America and, again, we wanted to get your association's views on how consumers' privacy issues are being dealt with online.

MR. GOLDBRENNER: Thank you very much. I just want to say it is not due to Linda's plane troubles, just due to her sadism because she is sitting in the back of the room, but I want to thank you for inviting us. And I want to commend the Commission on a wonderful program.

I think that what we have seen and heard this morning proves the necessity for this kind of cautious approach where we investigate the issues and see what industry can innovate and develop to meet the problems as they occur. I also thought it was an intriguing offer that the Commission would go out of business if we all adopted the McGraw-Hill program, and I don't know if I am looking forward to that or not.

Bob Pitofsky is my old professor of law and I would hate to see him out of a job. He was a terrific professor.

My organization is in the process of studying these

alternatives. And I think as we have seen today, even though we have a number of central elements identified, there are a great many approaches to deal with it. Trying to mesh the technology, the ability of individuals to protect themselves, and the responsibility of concerns to do it in such a way as to show themselves to be the decent players, is a very difficult and complex task.

And I think the development we have had over the last few years and what we have seen today is indeed the way to do it. I think it proves the superiority of the self-regulatory approach.

We had some questions just today from Commissioner Varney about the fact that if you go into a site rather than hit its first page, you won't get the warnings. You have a lot of problems how many warnings are you going to put up on the page, with the real estate issue that Esther mentioned, and with respect to the query if David Medine, there is a problem similar to caller ID problem, if computers are recording information on you when you first hit the site, should that be disclosed.

The debate there could be likened to whether or not a caller ID had to be provided, whether it was fair and legal. So I think all of these issues need the kind of review and discussion that we have had.

It permits the industry to develop and innovate in

how it is going to meet these needs. The needs of a small business and a large business are different. No business should be required to meet one code. The whole purpose of guidelines and self-regulation is that there needs to be a variety of tools available to businesses to meet their particular needs and to meet the consumers.

Most of all I think we need to consider and understand one of the figures that was in the Harris report that 80 percent of consumers or 79 percent had declined to give information that was requested. I think this shows that Esther's point is very well taken. Most consumers know what they want to give, what they don't want to give, and when they want to do it.

The protections we have are already primarily operating and that is the protection that each individual exercises when he chooses to give this information or not. And I want to thank you again for inviting us.

MR. MEDINE: Thank you. Commissioner Varney.

COMMISSIONER VARNEY: What is your association doing in terms of -- do you have any guidelines for your members on what information they should be collecting for people online and what they should be doing with it and how it should be handled?

MR. GOLDBRENNER: We currently do not have a set of formal guidelines. We do know from the survey we did on

behalf of the FTC and from other information that our members are extremely concerned about this area, and we do have a mandate to go forward and construct guidelines from them. And we are in the process of doing that.

And again I would say that the experience today shows that that's a task.

COMMISSIONER VARNEY: When do you think we could expect to see the guidelines?

MR. GOLDBRENNER: I would be reluctant to give a date, but I would say again that by this time next year we should be able to give you something more concrete.

COMMISSIONER VARNEY: Another year? We have been doing this for two years already. I am a little surprised that it will be another year.

MR. GOLDBRENNER: The PMA has not been involved in this process for that period of time. We have come to it more recently than many of the other member organizations have.

And, frankly, I am reluctant to give a deadline because in my own mind I am not sure that I would want to adopt guidelines. I think so. I think we all seek to provide these protections and to give our members a road map of how they might do that.

Whether that is in the form of our own guidelines or reference to somebody else's or a construction of checklist

of things you might do, I am not really sure and I would rather not commit.

COMMISSIONER VARNEY: Do you know how many members you have that are online and that run promotions and sweepstakes and prizes online right now, by any chance?

MR. GOLDBRENNER: I can't give you exact numbers, but since our association has as its members many of the most prominent marketers in the U.S., I would say a great many of them.

COMMISSIONER VARNEY: Hundreds or dozens? How many people are we talking about?

MR. GOLDBRENNER: Any number I gave you would really not be accurate. I don't have the database to support any guess.

COMMISSIONER VARNEY: On an anecdotal basis is it your impression that your members who are online and who are doing promotions online are currently collecting personally-identifiable information without consumers knowledge or consent?

MR. GOLDBRENNER: Again, I only have the data from the survey, and that is too small a number to represent the group entirely, but I think that when a consumer is asked to give basic data, and I think most of them are, in terms of name, address, et cetera, that's an obvious signal that the other side is collecting data.

COMMISSIONER VARNEY: But not necessarily so obvious what they are doing with it.

MR. GOLDBRENNER: Yes. I think that is a different question and I think there probably the majority of companies are not disclosing what they are doing with data.

COMMISSIONER VARNEY: David.

MR. MEDINE: Thank you very much. Last, but really not least, is Peter Harter who has been with us for now a couple of years, helping us work through some of these privacy issues, Global Policy Counsel for Netscape.

And I wanted to indicate Netscape will be presenting its open profiling standard this afternoon, but I wanted to touch a little bit on the whole issue that we have touched on before. This is not so much what Netscape is doing, as to how firms operating on the Web use cookies. And I want to get a sense of whether firms need to do a better job of disclosing the cookies.

MR. HARTER: I am very happy to be here. This is our third year. For the record, I am not an elf, but I can say how the cookie is crumbling and its effect on products, at least in our product.

Today Netscape is releasing its manufacturing version 4.0 of our product, the Communicator version of the software, the client software, which includes a browser E-mail and other components. And as a software it is more complex.

Our engineer, Lou Montulli, who has been with the company from the inception, helped found Netscape and has been very concerned about privacy and annoyed about the intensity of cookie questions we have had to digest over time. This is, I think, commerce and Marc had a few cookie jokes last year.

In all seriousness, Lou Montulli and others care deeply about privacy and on their own when engineers put features on the feature list for designing the next version of product many months in advance, they had to fight it out with other features that are in demand that don't make it into the product and having to put off for another version for release.

Fortunately they forged ahead. Let me describe how cookies have changed in our products over time.

In Navigator 1.0 and 2.0 and the various 2.0 11 versions and different versions and iterations in between, the cookie preferences could not be set by the user, and the default in those versions of the client software from Netscape was to accept all cookies. In Navigator 3.0, which I spoke about last year here at the FTC Workshop on Consumer Privacy, we announced that 3.0 allowed the user to select a preference that would have an alarm go off to indicate a cookie is being put by a server from a Website on to your client machine. And Netscape 3.0 defaults to accept all

cookies without a warning unless you set the preference to indicate otherwise to you.

In Version 4.0 the user sees the following cookie choices. One, you can choose to accept all cookies. Two, you can accept only cookies that get sent back to the originating server or domain-specific cookies. And I will touch upon that in a minute in more detail, why it is important.

Third, you can disable all cookies, or fourth, warn me before a cookie. Again, 4.0 defaults to accept all cookies unless the user goes into the preference file, which is only a few clicks away. It is not some arcane command integral to the control of the software. It has user interface controls and preferences, no more complex than manipulating an average word processor, I would say.

Now, in terms of people who can't navigate a word processor -- we don't currently manufacture a word processor at this time.

Anyway, what we have done is not only try to improve our cookies used in our product, we also try to make it an open standard. We are not a proprietary software, we are an open standards company. That's probably to us more important than satisfying some privacy concerns because we would not exist but for open standards. That's at our core.

While there is some controversy about what is an open

standard in the process of technical standards bodies and open standards in the press and marketing, nuances and egos involved, if we see beyond that we can see the request for comment 2109 submitted to the Internet Engineering Task Force a few months ago by Netscape and Bellcor that we have submitted these specifications, these choices that a consumer can make in 4.0 to the IETF so all manufacturers of client software that implement cookies in their client software can comment on this standard.

And once the IETF formalizes this request for comments into actual Internet draft specification, since we are an open standards company, we will change our product accordingly to comply with the standard. That process takes anywhere from six months to, well, sometimes requests for comments keep on getting commented on in the IETF process, so we will have no control over that as a company. We release it to the standards body, and hopefully it will go from there in a good way.

MR. MEDINE: Thank you. The only question I have, using Netscape and Navigator 3.0, I set my settings so that I could see when cookies were being placed and the problem that I had was I could see a cookie was going to be placed, how long it would last, but couldn't see what it did.

Will there be any progress on that side so I can have a more educated judgment to whether I will allow the

placement of a particular cookie?

MR. HARTER: That is called opaqueness. You look at a cookie file, although it is supposed to be a text file, it is a jumble. The server places the cookie file on your machine. It is really quite disorganized in that there are no fields of information specifying name, address, gender, so forth, and later this afternoon we will discuss the open profile standard.

Putting that kind of preference of personal data information on to a client side doesn't enable the Website to organize information efficiently, nor does it allow the user or consumer to control information that's there. To resolve both those concerns on both the Website business side and the consumer privacy side, open profile standard addresses that, basically loading the cookie with a lot of information about preferences of the user may be in some perspectives a misuse of the cookie, it wasn't intended to carry all that data.

Cookies are very small, supposed to be temporary, according to the original standard specified, and they've burdened them, making them a receptacle for permanent preference data, which may be overloading that poor little cookie.

MR. MEDINE: Commissioner Steiger.

COMMISSIONER STEIGER: Will this adaptation or change in our ability to deal with cookies have any impact on the

ability of the user to book mark? Is there any relationship?

MR. HARTER: In terms of -- there are some projects, PGP's Cookie-cutter, which allows you to organize on a user interface. You can pull up client software, which sites are going to accept cookies and which won't, organize those different cookies from the different sites.

How scalable it is and how often a consumer will go in there to really carefully organize all their cookies, people probably don't have the time to organize their bills and mail at their desk. Are they going to go and meticulously organize cookie files in the computer? People's desktops and their computer screens, the desk top is pretty messy to begin with. They are going to go -- that's a user behavior, user experience issue, which we deal with in terms of designing software, but our product was trying to keep it simple and give the user these four choices in our product.

If users are willing to take on more sophisticated choices, certainly they can already use products, the PGP's Cookie-cutter, which is a plug-in and interacts with our product. If it is a user demand, considered for a future version, I would suppose, for our product.

COMMISSIONER STEIGER: Thank you.

COMMISSIONER VARNEY: Since we are on the record here, I want to clarify a couple things. There was a

proposal to the Internet Engineering Task Force to basically switch the cookie's default; is that right? What is the -- how do you identify that proposal? It is not 2109, is it?

MR. HARTER: That's request for Comment 2109 submitted by Lou Montulli and an engineer from Bellcor a few months back. It has been submitted. It has been talked about at the IETF meeting I am aware of in Austin, Texas a month and a half ago, and now a technical specification document, generally between 50 and 100 pages long of engineering specifications for how to implement these proposed standards, that is being drafted and will be proposed in the next cycle of the IETF process.

COMMISSIONER VARNEY: Okay. I thought that there was a proposal that would change the default standard for cookies to a negative, that you would not automatically be able to -- it would switch the default. Right now a cookie can get dropped on a hard drive unless you go in and disable, right?

MR. HARTER: Right.

COMMISSIONER VARNEY: I thought the proposal was to switch that around.

MR. HARTER: Not that I am aware of. I have read through the RFC, and I don't recall that being proposed, that all client software would automatically reject cookies unless the user opts to receive cookies, but I might be wrong on that.

COMMISSIONER VARNEY: Does anybody else have information on that?

MS. LEMMEY: Yes.

COMMISSIONER VARNEY: Tara, can you speak into the microphone since it is for the record?

MS. LEMMEY: The RFC from RFP 2109, as it was originally proposed, only accepts cookies on top level domains and not from secondary companies; is that correct?

MR. HARTER: That's correct.

MS. LEMMEY: Which would indicate if you were at CNN.com a cookie from CNN can be dropped because there is implied consent that you are there and they have the ability to do that. Cookies from other third parties that you are not aware of dropping them would be rejected, which is how the proposal was originally written.

MR. MEDINE: These would be companies that might be advertising on a CNN site and so they would be on your screen and the question is should they be allowed, since you didn't choose to do business with them, particularly?

MS. LEMMEY: The issue came up because if a third party is going across, when a cookie creates a state environment -- tell me if you guys understand this or not -- when it creates a state environment it creates a relationship between you and the server.

The cookie and the server create a relationship and

you really need to have those relationships in order to effect commerce or have business.

Third parties, when the engineers wrote it, they wanted you to know who you were getting it from. And they realized there was a loophole in it that allowed third parties to move with you from multiple sites so that different people, if a person dropped a cookie from a server and they were dropping it at all the sites you followed, they can actually follow you from site to site to site and actually have a stream for where you went.

That's a loophole that the RFC, I think, was an effort to shut down, and right now the debate is on whether or not that will be shut down, although I understand Netscape said they weren't going to support the RFC.

MR. HARTER: Our position is we are not in favor of allowing third-party domains to pass through. Basically the user couldn't tell if I go to CNN or Outbounders and a cookie is being passed through from the promoter of the ad banner, advertising firms that handle putting up ad banners in multiple sites also want to collect data about who passes over their banners and aggregate that data and report it to advertising for Chrysler or whatever company sees the ad, it is their advertising agency or aggregator.

And certainly if they can have a cookie that follows you around and enables you to see a cookie from "cnnnews.com"

and a variety of other news sites and sees that you have seen all the different Chrysler ads at different sites during that period of time, they can create some user demographics and surfing behavior data about that particular user. And that's the concern. And that was probably the most controversial issue asked about cookies and this RFC at the Austin meeting.

MR. MEDINE: To clarify, Netscape's position is those third parties should not be able to place a cookie?

MR. HARTER: Right.

COMMISSIONER VARNEY: You do support the RFC?

MR. HARTER: I talked to Lou Montulli a couple of times, and it is very hard to see where it fits in the IETF. I don't want to get into the middle.

MS. LEMMEY: I think it would be moved to the W3C and not the IETF any more.

MR. HARTER: That I have heard too. Maybe Tim Berners-Lee could discuss that.

COMMISSIONER VARNEY: This, I think, is a really important issue because I think it is going to directly impact some of our thinking here. The current state is that any third party non-top level domain can drop a cookie, can go around with you, right?

MS. LEMMEY: Yes.

COMMISSIONER VARNEY: There is a proposal that was at

the Internet Engineering Task Force to change the architecture underlying the Internet to prohibit that, right?

MS. LEMMEY: Yes.

COMMISSIONER VARNEY: That proposal now, we think, is at the W3. Tim Berners-Lee will be here this afternoon, so we can ask him, right?

MS. LEMMEY: Yes.

MR. HARTER: Correct.

COMMISSIONER VARNEY: We are not clear on who supports it and who doesn't support it because we are not clear on precisely what it says.

MR. HARTER: We have committed to our product and we will reject those third parties. We know what we are doing in the product. As I said, for the standards process, we don't have control over that, what happens there.

MS. LEMMEY: The standard has been submitted. Comments are coming in on it. I believe that it is moved to different organizations and there have been split decisions as folks who were using cookies at third parties are really starting to understand the implications on their business and sites are starting to understand the implications on their business.

MR. MEDINE: I want to thank this panel for very interesting views on self-regulation and where it stands

today. We are going to take a break.

Before getting up, we need to keep the center aisle clear for a few moments to bring in a few more chairs. Stay in your places for a few minutes. We will resume in ten minutes with the next roundtable discussion.

Thank you.

(A brief recess was taken.)

ROUNDTABLE 1: PERSPECTIVES ON SELF-REGULATION

"Privacy advocates, consumer groups and government representatives discuss self-regulatory efforts."

JERRY BERMAN, Executive Director, Center for Democracy and Technology

PAULA BRUENING, Attorney Advisor, Office of Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce

LESLIE L. BYRNE, Director, U.S. Office of Consumer Affairs

MARY CULNAN, Commissioner, President's Commission on Critical Infrastructure Protection

JULIE DeFALCO, National Consumer Coalition

JEAN ANN FOX, Director of Consumer Protection, Consumer Federation of America

JEFFREY FOX, Consumers Union

JANLORI GOLDMAN, Visiting Scholar, Georgetown University Law Center

EVAN HENDRICKS, Editor/Publisher, Privacy Times .

MAYA BERNSTEIN, Information Policy and Technology Branch, Office of Management and Budget

MICHAEL R. NELSON, Director, Technology Policy, Office of Plans and Policy, Federal Communications Commission

MARC ROTENBERG, Director, Electronic Privacy Information Center

SHIRLEY SARNA, Assistant Attorney General, New York Department of Law, National Association of Attorneys General

RUSS SMITH

***

MR. MEDINE: We have assembled a panel of consumer advocates, consumers and government agencies to give some feedback on what we have heard today in terms of self-regulatory efforts.

Are they proceeding in the right direction? Are they adequate? Are governmental steps needed to intervene? And if we can get more of our panelists up here, that would be great.

In the interest of keeping going, let me announce we are going to take the session until about 1:20, break for lunch at that time. So we are going to have a much later break for lunch because we had so much more to say this morning and still resume close to 2:00 o'clock this afternoon.

I want to start with Paula Bruening from the NTIA to talk about self-regulation if you want to speak in the microphone. You are an attorney advisor in the Office of Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce.

MS. BRUENING: Thank you. I am here to report on NTIA's report on privacy and self-regulation in the

information age. This report was the result of a call issued by NTIA, and as such the report doesn't make policy on self-regulation, but what it does is assemble papers by experts from various disciplines -- and many of you are actually here today -- on issues surrounding implementation of self-regulatory regimes to protect information privacy.

It also reflects the experience of companies as they move to adopt self-regulation. NTIA was prompted by several reasons to undertake this inquiry, but what was probably most significant was that it was the realization that it is really not enough simply to refer to self-regulation as the answer to concerns about privacy, and that to make self-regulation work and to make it meaningful, it is important to think about the concept analytically and ask different questions such as how self-regulatory regimes work in market economies?

What elements, if any, are prerequisite to self-regulation in the industry? What are the existing models for a self-regulatory regime? What kind of enforcement mechanisms are available? How are disputes resolved?

So the authors represented in this volume address these and other questions. We would have liked to have had more representation by privacy advocates in this volume, and we invite the privacy advocacy community to participate with

NTIA in this ongoing discussion of self-regulation.

We see this document as a model and example of tools and mechanisms to further the debate on self-regulation as an option to protecting privacy in the information age. Copies of the document are going to be available here later today. It is also going to be made available online.

We hope you will avail yourself of it and that you will find it useful. Thank you.

MR. MEDINE: Thank you very much. We appreciate your coming here and announcing the release of this and the materials you will be releasing will be very helpful as we think through the issue of self-regulation.

I would like to have this be an open discussion among the panel members and again pose the question what you heard this morning and whether you are encouraged about industry self-regulatory efforts, what you have heard that is discouraging, what issues the industry is not addressing or is addressing, and are there major industry players or industry segments that were not represented here today that should have been here talking about privacy policies?

I am going to really open the floor up to free-flowing discussion. Anyone who would like to volunteer to start is certainly welcome. Russ Smith, who is here as a publisher of the consumer-info.org Website and proponent of private rights of action afforded to consumers to resolve

claims of privacy violations by industry.

MR. SMITH: Yes. I would like to discuss self-regulation, and I would like to find out where it exists. I have not been able to find it over the last few years.

I have submitted complaints to numerous industry groups, including the Direct Marketing Association's Ethics Council, and I get no response whatsoever.

In fact, they work hard to put consumers off, and hopefully they will drop off after a period of time. They recently submitted a report of this council, for this hearing, and none of my complaints are in this report. And I don't know what happened to them. I can't get an answer.

And, in fact, DMA will not even tell me the members companies they are representing at this hearing. And it is just completely unacceptable from a consumer standpoint.

There is, the example I want to use is the Telephone Consumer Protection Act, which is the telemarketing law enforced by the FCC. This law requires telemarketers to have a written do-not-call policy and I challenge any consumer, when telemarketers call you, to get this policy that's required by law. It is not even voluntary.

In addition, telemarketers are required to give their telephone number.

MR. MEDINE: I appreciate information on the

telemarketers, but I would like to focus on the online issues if we can because that's really our focus today.

Do you have any indication of failure to comply with any self-regulatory efforts in an online context?

MR. SMITH: My point is that the same companies who I have all this data on for the last two years are moving into the online community, and, yes, I have gone through this process with online industry groups, such as Cyber-Promotions and a new organization called IEMMC, and I have gone through the whole process just like I went through with the DMA of opt-out and filing complaints, and I get no response except for more junk E-mails, which contain pyramid schemes and pornographic material sent to me constantly.

In fact, about two hours before I came to this hearing yesterday I received another one.

COMMISSIONER VARNEY: What did you think of the McGraw-Hill presentation of what they were going to do?

MR. SMITH: Well, it sounded good until they told me they were working with the DMA. And that puts up a red flag and said, I am sorry, but I can't believe anything they tell me at this point.

Maybe they are doing something, I have not heard any complaints specifically about that company, but the numerous other companies that have policies, they make up a policy, they send someone to this hearing, and then the marketing

people never see this policy and never implement it and maybe they will put it up with yellow text on a white background and you can't read it.

MR. MEDINE: Janlori Goldman, expert in privacy and technology issues, and also has been tremendously helpful to the Commission as we have tried to wind our way through these issues.

MS. GOLDMAN: I want to congratulate the Commission to get started because I think that when we talk about self-regulation, what we see is that it doesn't happen in a vacuum. It happens because this agency has held two years, going on three years now, of hearings where, as Commissioner Varney has done, it asked the question: What are you doing and how long is it going to take you to do it? And how is it working and, you know, who do we need to be talking to who we are not? And I think not only this effort but the first as well has had a large impact on what we talk about self-regulation and whether it works and how well it works.

My few comments really focus on the fact that self-regulation is a part of the process when we talk about privacy policy. It is not a fix. It is not the whole story. But it is an absolutely critical part of the process.

We were looking at kind of market-based solutions that as Esther Dyson said are not just about what the industry is willing to do to give people choice and to give

people notice but what individuals are able to do as part of that process to say what they want their choices to be and take some action.

Some of the important things, though, about self-regulation are also some of its limits. The importance obviously is that it gives the industry an opportunity and consumers an opportunity to develop workable, responsive solutions to problems that have already been well-documented. It allows them to some extent to say with competition we will bind each other, we will bind ourselves and bind each other so that we are not stepping out on a limb and possibly losing business.

The other thing it does, I think, is to help in the public relations department by saying we are doing this on good faith, we are doing it voluntarily, which is also very helpful, where there has been some anger and backlash from consumers.

And I think very importantly it proves to policymakers that it is doable because you hear so often we won't be able to do that, that's going to hurt our industry and take away from potential revenue or existing revenue so you see it is doable and possibly use it as a model. And it educates the industry in that regard to say this is something not only we came to reluctantly, we wouldn't have come to on our own, but now we are doing it and it doesn't hurt as much

as we thought it would.

And I think in that way it encourages much more open and honest participation on the part of consumers to say we now know what is going on. We can make certain choices and we will be less reluctant to part. The limits, though, I think are pretty obvious.

It only in the sense binds the good guys and the good guys are the people sitting in this room, for the most part. They have said we want to do the right thing, we are trying to do the right thing, we hear the complaints, we know a certain percentage of people are giving us inaccurate information, withholding information, not even coming to our site, they are not going to buy things, so there are some real business reasons for going forward, but there are a number of companies and organizations who have no public presence, who don't have a good name to lose, and so those are the folks who in essence are not looking at this as either an ethical or business issue.

And the enforcement issue, which has been talked about a great deal. There is no way to have a remedy, an individual remedy, in this regard. And while it may be good to say, well, we say we are doing the right thing and the FTC can now come in and say there have been false and misleading statements, that still makes it very, very difficult, I think, for individuals to enforce.

The only other comment that I want to make is a comment that was made earlier about whether or not privacy is considered an important issue in the public. And I think it is not a good idea to rate privacy along with other concerns that the public may have, such as their physical safety, such as the budget, such as, you know, a number of other issues where it is kind of put in there. That's not the context that's helpful for us.

Most people only understand privacy when there has been an impact. And then they will say I don't want my employer to see my medical record. I don't want as a condition of me surfing the Web to have information gathered about me and created in a profile, but to rate it along with other things, I think you need to put it in a privacy-related context and say how have we handled this issue across the board and how should it be a priority?

In a book that came out very recently by Janna Malamud-Smith, she talks about private matters. And she is a psychoanalyst who says that having privacy in our lives and being able to control what people know about us and under what circumstances is what allows us to develop ourselves and our character and our identity.

And those are very tough things to measure and tough things to quantify in this kind of a setting, but that is the real consequence of not doing what people in this room say

they are going to do and not making sure that across the board that happens as well.

COMMISSIONER VARNEY: David, I think what really strikes me about what you said is something we grapple with quite a bit, that self-regulation tends to capture the good guys that are doing the right thing to begin with. Is it your view that we ought to consider regulating for precisely that reason, that there is a lot of activity out there by parties that are invisible that may or may not violate existing law, might not be fraudulent, it might not be deceptive? What do you think?

MS. GOLDMAN: I think, as I said, what self-regulation does and why it is such an important part of the process, the policymaking process, whether you decide to make the policy or not make it, it gives you an opportunity to create a record of what is doable, what works.

How the industry on its own -- and I say on its own with some measure of understanding that on its own involves the FTC saying what are you doing and the media stories on the front page over the last couple of years.

But take it that it is on its own. This is what they are able and willing to do as a first step out in order to maintain their good public name and in order to maintain their customer base and public confidence and trust.

COMMISSIONER VARNEY: You are fairly familiar with us

as an organization and you know about Section 5, which is our authority to prosecute deceptive and other fraudulent acts and practices in commerce and trade.

Do you think we ought to start examining a fairness standard by which we would consider prosecuting behavior on information collection online?

MS. GOLDMAN: I think that what the FTC's authority does in some ways is put some of those who are voluntarily engaged in the self-regulation process in a bit of a bind. Probably a good bind because, as they all say, we are going to say what we are doing, we are going to give people choice, and if we don't do it, you can come and get us.

But for those bad actors, they are not saying anything about what their information practices are, they are not giving any kind of notice, and so it seems to me that either the FTC's jurisdiction and authority should be expanded, not just to look at people who are making misrepresentations but who are acting in a way which would be considered to be unfair.

COMMISSIONER VARNEY: Our jurisdiction may not need to be expanded to do that. We do have authority in unfairness. I guess I am asking whether or not you believe that as we see these standards emerging, should they become for us a point of reference as to what is fair and what is unfair?

MS. GOLDMAN: Absolutely. I think basic fairness standards that people have talked about, the notice and choice standards are, should not only be industry standards, should be national policy and international policy. That should be our starting point.

MR. MEDINE: Shirley Sarna is chief of the Bureau of Consumer Protection in the New York State Attorney General's Office, here as a representative of the Consumer Protection Committee of the National Association of Attorneys General.

MS. SARNA: I am actually quite astonished because everything that Janlori said is in the scratchings that I was going to say. I too went back and kind of reviewed the bidding of what occurred this morning and coming at it from a slightly different point of view because I am an enforcer.

I do agree there is a lot moving this market towards self-regulation, often the threat of legislation is a prime mover, but in this case economic self-interest dovetails completely with that threat of legislation or regulation and I think that provides a lot of incentive to experiment in self-regulation, and that's really issue No. 2.

We have often heard in our federal system that the states are the laboratories for policies and in this case what we are really seeing in many ways of those in the market are what are the laboratories for what works and doesn't work.

And I think that no matter where this process ends, the opportunity to explore options and to test them out, I think, is an invaluable contribution to the entire process.

But there are clearly shortcomings, as Janlori says. One of the very obvious ones is who is it that's participating in all of this. And it is likely from our experience, from my experience as a regulator, that those who are stepping up to the plate and at the very least thinking about this, massaging the issue, making a commitment to principles, and then very importantly making sure that all elements of the corporation are aware and committed and participating, you have segmented the market and what is very likely, and we heard that today, the smaller companies, the new entrants, those likely to have less of a stake are less likely to participate in the process. And from our experience segmenting the market in that way is not a very useful way to proceed.

Also, where there are difficulties waiting for the market to self-correct in some circumstances I think works better than others. In an area like privacy where some of what we are talking about, as I said earlier, I think is normative expectation, I think it is more challenging to think about the market being able to shape the information specifically enough to translate into a clear economic indicator for a company.

On the enforcement side, I can't underscore enough the enforcement difficulties. We in New York State don't have unfairness jurisdiction, but we do have deception. From a deception point of view, where there is a representation about policy procedures in place and obviously where the conduct of the company falls short of that undertaking, I think I am very comfortable in being able to shape a law enforcement action and actually in New York it was a matter that Eric Wenger shepherded that for us.

A company, to whom I give enormous credit, Juno, represented that its privacy policy was that we are not going to -- give us this information, we are not going to use it or make it available to third parties. Yet in their agreement there was a specific reservation that said that this might be available to third parties.

When we brought it to their attention, quite candidly in a law enforcement posture, they were aghast and very quickly and well beyond whatever our expectations were corrected that to make a very strong privacy statement.

The tricky issue is, and it dovetails right into the failure to address that middle market, a failure to disclose under these circumstances would be a very difficult if not impossible case to bring. So short of a bottom line easily recognized standard applicable to all, I think that we run the possibility of having uneven obligations and uneven

guidelines.

I leave it to your headache to kind of parse through and compare and contrast, but that is yet another.

So I want to ask a provocative question, not one that I necessarily have an answer to, but I just want to ask the question. What is unacceptable at someplace down the road with something, a standard that is recognizable, that there has some consensus behind, because that's really what we are seeing in these guidelines, and that really makes the market equally competitive to all the actors in that market and puts on that market an equal obligation to deal with what I think many of us have felt for some time, and what the social science research confirms for us is an important consumer value? So I would be very interested in hearing the other side of that.

MR. MEDINE: Maybe Jerry Berman, who is the Executive Director for the Center for Democracy and Technology and a veteran in the field, will answer that.

MR. BERMAN: Mostly legislative battles. I agree with Janlori in terms of that self-regulation only takes us so far. There are bad actors, people fall out and you have the good guys in here, but it is also an experimental way to find out what the rules might be.

I have no problem with ultimately writing a standard into law when we have a consensus about what that standard

should be. In every area of consumer law dealing with privacy we have reached some consensus where you at least have 51 percent of the votes and that includes more than privacy items, it has to include industry and their representatives.

On the Internet we are dealing with a new global medium, and it is very different. And it is difficult to map legislative solutions and the European solution in particular on to the Internet. We don't know what the rules should be. We don't know what the -- Commissioner Varney asked about the fairness rule. We don't know what it is yet.

The problem with leading with a proposal, getting Congress rolling up here with a legislative proposal at this point is that they are liable to start with the wrong standard. And what you do is you turn the good guys away from the self-regulatory efforts that they are undertaking and you turn them into a defensive operation in the foxhole and they are dealing with a bad bill, call it Communications Decency Act II for Privacy.

So instead of bringing empowerment tools to the market, which could have happened in the content area with much more, much faster, it slowed down, while people spend millions of dollars defending the First Amendment in court. That can happen in privacy. It is a hot button issue. It lends itself to an awful lot of discretion and complexity and

there are other values that need to be -- I think that the self-regulatory moves the industry has taken are not enough, but they should be commended for it and not banged on the head for taking them.

We should build on them. They are setting a standard. No one in this room, I believe, could really say that they know how to write the privacy standard of fairness for the Internet.

No. 2, is this is a great meeting for empowering users. Self-regulation and government intervention are all based on the fact that consumers can't act for themselves and there is a market failure. For children and maybe in the lookup services where there is no relationship with customers, that may be true. But in the transaction world of interactive media, there is the possibility of having a regime in the infrastructure which allows consumers to state their preferences, Web operators to state what their policies are, and to exercise choice and not even have opt-in/opt-out.

So why opt for opt-out when you might be able to erase the distinction through efforts of technologists in the industry? So what I am saying is that self-regulation isn't all of it, but you just can't take, say, that's great, let's move to Congress and start legislating.

MR. MEDINE: Mary Culnan, who was nodding during

that, we will find out what she was nodding about, is a Commissioner on the President's Commission on Critical Infrastructure Protection and from Georgetown University.

How do we pat the good guys on the back and encourage them to engage in self-regulation while bringing into the Net the bad guys?

MS. CULNAN: Which is a good question. Today I am not representing the views of the Commission on which I serve. This is actually more of my business school hat on today, but the Commission is interested in some of the same issues.

So I want to digress a little bit from your question, but I think I am hopefully going to answer it. Really one of the things that's come out of this hearing today is, in fact, that it is making a business case for privacy, which I think is really the big issue. We heard this in the survey results. We heard this in the McGraw-Hill presentation, heard it from the DMA and from others.

This theme of public confidence or public trust keeps coming up. And this is really the reason for why companies need to put privacy protections in place because it is good for business. What does this mean? If consumers trust you, if they have confidence in a company, it means they are willing to assume the risks of disclosing their personal information because they believe whoever this third party is,

the Website owner and other company can be trusted to act in their best interests, when they can't go behind the Website and see what is really going on as we heard someone say earlier.

So for organizations to build this kind of confidence or trust, they have to develop the kinds of mechanisms that can serve as a substitute for firsthand knowledge on the part of consumers, the kind of knowledge you get when you are in a one-to-one relationship with somebody you know, you learn over time whether you can trust them or not.

So there are really two things that you can do to build this confidence. You can say what you do and you can do what you say.

So what does this mean? Saying what you do means you are transparent about your processes, your practices. You tell people what you are going to do with the information that you are collecting, how it is going to be used, what rights they have with you.

We heard a lot about this this morning and also in the surveys, over and over, no matter what kind of a survey it is, people are reluctant or unwilling to disclose if they aren't told what is going to happen to the information.

Then under the do what you say, this is where you really need some kind of standards or internal reviews or audits or the TRUSTe seal or something that says to people,

okay, I can believe you because there is some process in place to assure that, in fact, you are behaving the way you have said that you are going to behave, so the Underwriter Laboratory seal or the equivalent.

In my own research I found this also, using some data that Alan Westin collected a couple years ago, that if you tell consumers that you are going to observe fair information practices, the privacy concerns associated with profiling for direct marketing purposes evaporate. It doesn't say, didn't look at the question of: Well, did they do what they say, but basically disclosing, people are saying fine, this is fair to me, I will disclose my information to you, which is really pretty astonishing.

And it says every business out there should be willing to at least disclose their practices, assuming that the people feel them to be fair because it is in their interests to do so.

MR. MEDINE: The question is how do we make that happen?

MS. CULNAN: How do you make that happen? We have heard, there has been a lot of progress made this morning, I think, and I think this is really due in large part to the FTC's efforts. And I want to congratulate you again on doing this and thank you for having me here to do this, but it used to be people would come in and hold up their policy and every

one would say that's fine and now somebody says, as Janlori pointed out, what are you doing, how much, how often, how many people are doing it?

I think one of the things is to sort of see how this works. I thought Jerry was very eloquent on this and to see what works. The one thing with the Web is anybody can go out and verify. You don't have to depend on the companies to do anything.

So that's one thing. There are plenty of opportunities for research and this can be done with some effort, but it basically doesn't require a lot of money as some other kinds of studies do.

MR. MEDINE: I have to ask people, we have a short amount of time.

MS. CULNAN: I will wrap up quickly. The things that can be done, companies can do on their own if they don't want to do TRUSTe or something like that, they can put on the Web page, we audit ourselves, we have internal procedures, come clean with those, and I think wait and see what happens.

And basically see if this becomes standard business practice and what problems remain and what consensus evolves. This happened with fair credit reporting, so when the FCRA was finally amended the companies involved had pretty much adopted the practices already on their own and it wasn't a big problem, but I agree, I think if we regulate too

soon we are in problems. If we don't regulate at some point and there is still bad apples, then that's a problem that something needs to be done.

MR. MEDINE: Esther Dyson, you have been introduced already.

MS. DYSON: I will be brief. I want to go a little farther from just talking about TRUSTe and representing that particular point of view and say we really need to start thinking about these issues in a different way. What I would like to do is propose an answer for Russ Smith, and it is the concept of the Direct Marketed Association, rather than the people who are doing the marketing, the people who are being marketed to.

We have all been talking about how the Web changes the balance of power, et cetera, et cetera, et cetera, so I would like to just take you through how I see that could actually happen. And it is not automatic, but this is what I hope the FTC and everybody here will foster.

First of all, yes, every consumer can now go and he can look for the TRUSTe marks or Direct Marking Association stuff if he believes it or whatever, but that's really difficult. It requires not just an informed consumer but as somebody said a consumer who has a lot of time and not much better to do.

He can use a P3 thing, he can set up his browser with

all kinds of defaults and hedges and conditions and look for Websites or vendors who correspond to his preferences. That too is probably -- may or may not work. People may lie and so forth and so on.

What I think is really going to happen, and I am surprised that AOL is not here, this is now going to become a marketing thing for ISP's and other Internet service providers. Come to my ISP, I have a list of people that I automatically block. They cannot send E-mail to you. Much like a content filter.

ISP's will be known for having not just porn free sites but offensive commercial stuff sites. It will, in the end, I believe it is going to be policed in some form or other by the ISP's who will trade among themselves who the bad actors are, ISP's who don't control people who send stuff from their services will eventually be black-listed by the other ISP's.

This will create a situation you might say where the Net will be Balkanized because not everybody can send to everybody else, but if it is done on a distributed decentralized voluntary basis, I think the best way to get rid of these bad guys is not by trying to create a single standard that's going to be inflexible, hard to police, et cetera, but by leaving it up to the decentralized forces not of the individual consumers who don't have the time but to

their ISP's who will be their representatives.

MR. MEDINE: They will be here tomorrow, by the way, to talk about unsolicited E-mail. Michael Nelson is the Director of Technology Policy in the Office of Plans and Policy at the Federal Communications Commission, but more importantly a new father. Congratulations.

MR. NELSON: Thank you very much, David. I am going to try in two minutes to build on what Esther was just saying and also to address the question you asked, which is who else should be involved in this discussion.

Over the last four years, both the FCC and prior to that at the White House Science Office I have given hundreds of speeches on the information highway. And one of the speeches I give is called the eight P's of cyber policy.

And the top three issues on the list, the real show stopper issues are privacy, piracy, and pornography. And I guess I would urge you as you look at the privacy concerns to make sure you are looking at what these other issues can tell you. These are linked issues.

Efforts to protect children from pornography, efforts to stop the distribution of copyrighted material that is illegally copied are in many ways parallel to what we are doing here on privacy.

They involve some interesting jurisdictional concerns. They involve -- many of the solutions involve

labeling, and many of the third parties, so I think we should make sure we are looking at the parallels in other areas.

I learned in Washington long ago that if you have a policy initiative, you never succeed unless you have a good bumper sticker and you have a good model.

And we are searching for models in this area of privacy protection. And there are a number of them out there from these other areas. There are also a number of interesting developments overseas. And I think there should be an effort to learn from the mistakes and successes of what is going on in Europe and the developing world. There are some very interesting things going on.

Canada has been a real leader in this area. The UK has set up some interesting new approaches involving self-regulation. Probably their most successful one has been in the area of adult material.

They have set up a hotline where parents and users of the Internet can report cases of abuse of this system and can report cases where their children have run across adult material. This kind of online hotline works very well. The technology is very efficient for that.

And it is that kind of self-policing as well as self-regulation that is a very powerful, powerful combination.

The other group that I hope you will involve a bit

more will be the technologists. Since I am one, I guess I am biased, but I am a technological optimist. I think we have a lot of opportunities here for new technology to provide new solutions and it would be good to get people like Tim Berners-Lee who is coming, but other people of his ilk to talk about not only what technology is being developed but also where the technology is taking us.

This discussion was very different three years ago because we hadn't seen cookies. We hadn't seen -- the Web was in its infancy. In two years, three years, things are going to be completely different again and the issues we talk about will be very different.

And we need to be projecting forward to thinking about what it will be like when it is as easy to send money on the Internet, as easy as sending an E-mail message. That will have interesting implications for privacy. It will also have interesting implications for our ability to get paid for private information.

Part of the solution, I think, in this whole game is better information and better ways to get reimbursed for sharing your information.

MR. MEDINE: We will be focusing on technological issues this afternoon and reconvening this group again. Jean Ann Fox is the Director of Consumer Protection for the Consumer Federation of America, and also vice president of

the Board of Directors of Consumers Union.

What is your take on where we go from here?

MS. FOX: Well, I believe that self-regulatory efforts and voluntary guidelines are very positive and useful, but not sufficient. There are always bad actors that don't comply with the best efforts of the leaders in the industry, and for that reason I believe the Federal Trade Commission needs to have enforceable guidelines to be sure that consumers are treated fairly in the new marketplace in cyber space.

It is Consumer Federation of America's position that consumers should have sovereignty over their personal transaction information, that consumers should be able to control the disclosure of that information used by other parties. You can call that opt-in, maybe we can think of a less fighting word to apply to it, but the technology is available, I believe, to make it possible for consumers to be presented with the choice of that they have to choose to allow you to use information that can trace back to yourself.

That shifts the burden from consumers to protect their privacy to marketers to persuade you that it is in your interest and worth your while to allow them to collect information about the things that you look at.

I think one of the reasons that this is a cause of

anxiety and concern for consumers is because you can't see it happening. If you use the same kind of data collection practices in old-fashioned shopping where we went to the mall and we looked at things, the equivalent to what can be done on the Internet would be someone following around behind you looking at which billboards you looked at, which subway placards you read, which ads in the magazine you looked at, how long you gazed at the shelf in the supermarket and tabulating that data to be tied together with what is on your frequent shopper card at the supermarket or the information off your check when you pay for it, your purchase, and then selling that information to someone else.

If this happened in physical space, you would say: Get away from me and don't do that. When it happens in cyber space, most consumers don't know that's going on. Since I am the least sophisticated computer user in the room and only know what my children have taught me about using the Web, I feel that I am probably typical of a lot of people and we don't know what is going on and how to protect our interests. And we think there need to be some real rules that can be enforced to make people feel comfortable.

If you only relied on enlightened self-interest, you could close down half of the Federal Government. Enlightened self-interest would admit that no cars would ever have been manufactured that weren't safe or that had poor fuel

mileage. Enlightened self-interest only goes so far. And you need to have a basic set of standards in order for the companies who want to do the right thing to not be at a competitive disadvantage when they provide consumers with real protections.

All of the voluntary guidelines that I have seen announced or described today, though, all have the failing and only allow for consumers to opt-out of providing information. I think things would be much more supportable if they shifted the balance and had consumers opt-in.

Thank you.

MR. MEDINE: Thanks. Let me ask Julie DeFalco, a policy analyst with the Competitive Enterprise Institute and National Consumer Coalition, do we need enforceable consumers standards?

MS. DeFALCO: Actually I was going to read down a list of stuff so I don't repeat what other people have said. First, to say self-regulation is kind of a misnomer. What you are really talking about is a guided, setting a goal that's maybe arbitrary but the government sets what other advocates are setting. It is not a free market in the conventional sense.

There is also a heavy presumption today that any government regulation that would happen in the Internet will work better than whatever is going on now. That's an

unfounded assumption. There is simply no basis that that would happen.

In fact, most of the evidence shows that when government goes beyond its mission of setting the rules of the road and to deciding the composition of the traffic, as Richard Epstein put it, regulation restricts consumers choices, it doesn't expand them.

Finally, there is a presumption that privacy is an absolute right when actually what it is is a preference and everyone has different preferences. If you are surfing the Web, it is like you are walking down a street, and I wouldn't think that Ms. Fox would disagree it is okay for someone to stand on the side of the street and record what you are doing and tell the person sitting next to them that you are wearing a red jacket.

And even if that did bother you, I don't really think that you have any recourse because what you are saying in this term of preferences is you are really controlling the speech of other people. That's what downstream control means.

Finally, the best way to comment the very clear variation in these preferences is to allow the development of different solutions. I think that it has only been a couple of years and people have only just started to develop these privacy policies and it is kind of silly to expect all of a

sudden there is going to be this complete set of standards that are going to be developed. It is going to be something that takes a while. And I would suggest that the best thing for consumers and for everybody is for the FTC to kind of hang out and wait. Thanks.

MR. MEDINE: Evan Hendricks, I take it you concur with those comments?

(Laughter.)

MR. HENDRICKS: That's the kind of schlock I have been listening to for the last 20 years.

MS. DeFALCO: Thanks.

MR. HENDRICKS: Let's wait a little bit longer? No, we are here because we are trying to find the best way to protect privacy. One reason we have to be here and we currently have an inadequate system of protecting privacy and trying to decide what is the best way to protect privacy and I wish I had more time, given the shortness of the hour to say the nice things I have to say about the policies that came forth today because I think each one of those efforts will do something to help protect some people's privacy and I welcome those efforts, but the theme of today is inadequacy.

We are a country of 240 million people. There is no way that those efforts are going to address the privacy concerns of the people of this country.

I am inadequate to protect the privacy of this

country. The FTC is inadequate. All of us together can do a lot more, but it needs to be a national effort to adequately protect privacy.

Organizational policy, self-regulation, you have to look at the example of the Freedom of Information Act. This is a good law. Some agencies do better than others at implementing the law to give it its real meaning because they have good organizational policies to implement the FOIA, so it is common sense that an organizational policy by itself is inadequate. It is common sense that a law that's not enforced or administered is inadequate. You have to have the whole nine yards.

Now, the answer to your question is yes, we need enforceable standards. I think the reasons are quite compelling. There are too many serious examples of the failure of voluntary self-compliance in this country and Russ Smith hopefully will get a chance to talk about some examples on his Web page, but we broke the story about AOL, which was wrapped in the knuckles by Congressman Markey for selling its list without notice.

And now they have buried their notice in the terms of service agreement and they are selling lists, not only selling the lists, and all the members I have talked to are not aware this practice was going on, but they are also going to, once you are an AOL member, they go to an outside

database and check your income level. They check how many kids you have in the house, what kind of place you live in. They are selling lists of kids between the ages of 0 and 5, between 6 and 11, and between 12 and 17, and there is no notice going to AOL members that this is happening.

I think if you are talking about a fairness standard, if you don't have the authority to do an informed consent standard, it seems to me you certainly have authority of a fairness standard where all organizations are required to tell what information they collect, what they plan to do with it, and give people choices in relation to that information.

There are also, you know, Martha Landesberg asked the question about 25 or one-third of the DMA members observed the DMA's privacy guidelines and the mail preference service. As part of the record I want to make sure we have this page from Paul Schwartz and Joel Reidenberg's book on page 309 where they say about the same percentage. And they say that, "Members of the privacy task force even ignore the DMA guidelines. The DMA privacy task force declined all requests to discuss actual information practices in response to the survey conducted for this book. The DMA also does not represent every company in the industry. These practices show basically a lack of a true commitment to making their program a real program."

Publishers Clearinghouse was the chairman of the

Privacy Task Force and they had to settle with the state attorney general about mailing list practices. And they were even thought to ignore some of the DMA guidelines.

I am not satisfied with some of the responses to the transgressions by Metromail, which we don't have time to detail here, but that showed a lack of enforcement.

MR. MEDINE: In the interest of time, I think we get your message.

MR. HENDRICKS: One thing is DMA, as I understand it, won't release its own membership list. How are we supposed to audit what is going on with their practices of their members?

MR. MEDINE: We are certainly happy to take further written comments here, but I think the message is clear.

MR. HENDRICKS: Can I say one more thing?

MR. MEDINE: Sure.

MR. HENDRICKS: We stood here all morning too, and you didn't control the time of the earlier panels. There is a real irony here. The Internet is welcome or look forward to its commercial potential, you know, that this is going to be a great thing for commerce. But the irony is that it is not living up to its commercial potential, and one of the reasons is concerns about privacy.

I think that industry should see the light on this and realize that the voluntary efforts by themselves are not

enough and that we should all work together to establish the legal standards that would give consumers the rights that they need so they finally have consumer confidence so it can live up to the legal standards.

That's why like the relationship with the auto example, the auto industry was cruising fine just like our information industries have a technology and have competitive advantage now, and then the '60s came and then we had a gas crisis, and then market share was taken over by smarter foreign companies that made cars more fuel efficient. If the auto industry was saved from itself by appropriate federal standards mandating fuel efficiency, that would have been something that would have been good for the industry and good for all American consumers, and the same way I think this industry is failing to see the writing on the wall, the same way the auto industry did, and I think just as they come forward and say we don't need legal rights for people because we know what is best for you, here is our voluntary compliance policy, I am saying to industry, you don't know what is best for you. You need to be saved from yourself by fair industry standards and legal rights for individuals because that will help you keep your competitive advantage and not fall off the table the way the auto industry did.

MR. MEDINE: We are more than happy --

MS. BERNSTEIN: That's why we are taking seat belts

out of cars.

MR. MEDINE: If any of you have concluding remarks, we would be happy.

MR. FOX: I will be brief. I know this afternoon is really the time for technology, but since you had the cookie man here, I can't help but comment. You asked before what major players might not be here, a niche player known as Microsoft appears to be completely absent from these hearings.

COMMISSIONER VARNEY: They are rather reluctant to enter this building, for other reasons.

MR. FOX: Maybe they could find someone from another division. They have a Chinese wall.

I think a couple years ago Netscape was the de facto standard and the dominant product but certainly Microsoft is right there with Netscape now. Some people think that they are going to, you know, and they own the operating system which poses other potential privacy issues, but the thing I want to point out to people is that cookie thing seems like it is kind of exotic techi-type discussion, but it is extremely important because these two companies hold what is essentially the keys to the kingdom.

Anybody, all of us that want to go on the Web have to go through one of their two products. And it is kind of like they have cornered the market on access to the Web. And I

have a serious question at this point about who their true customers are, whether they are really the nominal customers, the people that get essentially free browsers or are their customers really the publishers and people on the Web?

And so these issues, those, the public has a vested interest in those two products. They are not just another WordPerfect or Quicken or something, they are crucial products. And I think we have to follow very closely; whether they decide to adopt a standard or not, has a profound impact on consumers' ability to control their information.

MR. BERMAN: For the record, Microsoft and Netscape are both participating in the technology demonstration this afternoon. To say they are not here when they are not at the table to do anything, I mean, doesn't advance us down the road to either privacy regulation or good government regulation.

MS. MAYA BERNSTEIN: Maya Bernstein, I am not Bruce McConnell. I apologize for Bruce not being here today. He had a meeting with the director, something about the budget deal.

I do want to say, I know most of you in the room have seen this options paper that we put out for the Information Policy Committee in April, and one of the options we talked about was self-regulation. Obviously we are not going to go

to a completely self-regulatory system. We don't have one now. Nobody is talking about repealing the Fair Credit Reporting Act.

And I think there is general consensus that there seems to be need for comprehensive medical records, legislation, perhaps children's legislation or other vulnerable populations.

It also doesn't seem to be in the cards for this administration that we are going to create some kind of very strong regulatory admission or agency of the government. That just doesn't seem to be the way that this administration, this government is moving right now.

We are cutting budgets, balancing the budget, getting rid of agencies and cutting, but we are getting pressure from consumers, from Europeans to do something. And so I just want to say that as one of the editors of the option paper and another one, Becky Burr, was in the room that I am going to be one of the people to read your comments, so I am hoping you will make detailed and interesting comments for us to read.

Also I do want to say that we are very happy to hear the creative ideas that have come out here. Clearly you have all thought about this in preparation for these hearings, so you will have no trouble turning in comments on time on June 27th.

I do want to say we have no plans right now to extend the deadline after June 27th and so we are looking forward to hearing those comments and hearing your thoughts about self-regulation so that we can present to the public, present to the Europeans, we can know better how to make the case for part of the marketing that can be benefitted by self-regulation.

MR. MEDINE: Thank you very much. Leslie Byrne, final words?

MS. BYRNE: Having sat through this morning's panel, I guess I will save my comments until next year.

(Laughter.)

MS. BYRNE: It seems like it is always on the horizon and always in the future, how we are going to address this. And I don't want to get deterred about the issue of the Internet and privacy. Janlori talked about medical record privacy, she talked about children, and the fact is that these are all coming together as one issue. It is not Internet. It is not medical record. It is the issue of privacy, regardless of what the medium is that we look at.

And I think Evan's comments had some validity in that this issue is getting hotter by the minute. And while I applaud the efforts at self-regulation, the fact is that consumer demand is propelling these industries to do something. And the real question is whether they do

something concrete or they do something for appearance sake.

That is the issue here. I am not convinced that self-regulatory schemes do much in terms of enforcement or anything other than give appearance of doing something to hold the wolves from the door. So while I hope that there is some merit to self-regulatory schemes, and I hope that it is never just one more year, just one more year, the fact is without an umbrella of privacy principles we are coming up with different standards for privacy for medical records, for credit, for all the rest of it, we are coming up with 50 different states' interpretations of privacy, and I think it would behoove the industry to look at how we can have a common standard that won't use up screen real estate, which is a term I just love. I thought that was the best term I picked up today, screen real estate.

That when we do something on the Internet, we know that we are going to have notice, that we are going to have access, that we are going to have choice, that we are going to have the information that we need as consumers to make intelligent decisions. And whether that's medical records or the Internet, it won't matter because we all have those same rights.

MR. MEDINE: Thank you very much all of you for those remarks. And this group will be convening again at the end of the day for a critique. We will pick up the next session

at 2:15.

(Whereupon, at 1:35 p.m., a lunch recess was taken.)

AFTERNOON SESSION

(2:15 p.m.)

PANEL III: INFORMATION PRACTICES ON THE WORLD WIDE WEB

"Commercial Web sites' current information practices."

YALE R. BROWN, President and Chief Executive Officer, Intelligent Interactions Corp.

CHRIS EVANS, President and Chief Executive Officer, Accipter, Inc.

SHELLEY HARMS, Executive Director - Policy, Nynex Corp., representing Bell Atlantic Corp. and Nynex Corp.

ERIC J. JOHNSON, Professor of Marketing, Operations, and Information Management, The Wharton School, University of Pennsylvania

TARA LEMMEY, Chief Executive Officer, Narrowline

MARTIN NISENHOLTZ, President, New York Times Electronic Media Company, Coalition for Advertising Supported Information and Entertainment

KEVIN RYAN, Chief Financial Officer, DoubleClick

ARTHUR B. SACKLER, Vice President, Law and Public Policy, Time Warner, Inc.

***

MR. MEDINE: I think we are ready to resume. We are a little behind schedule, but we have lots to talk about, so we will do the best we can.

The first panel this afternoon is going to focus on

information practices on the World Wide Web with particular emphasis on technologies that make information collection and targeted online marketing possible, and about the mechanisms available to consumers to control how their personal information is collected and used online.

Finally we are going to ask panelists to consider whether actual practices should be dictated by technology, or just because information can be collected, should Websites do so?

The first panel member we will look to is Yale Brown, cofounder and president of Intelligent Interactions Corporation of Alexandria, Virginia and a former vice president of Oracle Corporation's Emerging Technologies Group.

MS. LANDESBERG: Thank you for being here, Mr. Brown. I wanted to ask to begin with Adfinity allows Websites to create databases of personal information through online registration forms and to overlay the data collected with other information from other databases.

MR. BROWN: Correct.

MS. LANDESBERG: Can you tell us what kinds of information your clients are actually collecting online this way?

MR. BROWN: Yes. It has been our focus to limit the amount of information that a consumer has to provide for that

collection process, so basically we are looking for an identity, name, address, age, and that's about it, basically identify who you are so that we can use existing databases, existing sources of data to provide an additional level of detail for marketing purposes.

Our focus is direct marketing, so we subscribe to all the principles of the Direct Marketing Association and are focusing on allowing an opt-out procedure, we allow a person to say I do not wish to participate in this and still get the benefits of visiting the site.

MS. LANDESBERG: Thank you. What kinds of disclosures, if any, are built into the Adfinity software?

MR. BROWN: From a disclosure standpoint we work with our clients so that on the registration page itself we explain what the information is going to be used for. We provide them the ability to say I do not wish to and a check box, for example, on the registration page.

If they check that box, we put a permanent code in their subscriber file that says never show any targeted information to this person and never use it for any overlays.

MS. LANDESBERG: What disclosures do your clients provide users regarding the tying of their Website databases with off-line databases?

MR. BROWN: I think it varies from client to client

since that's outside our prerogative, that's how they manage their relationship with the end subscriber or end user, but in general they make, explain that this is information that they are asking for for marketing purposes and they make all of the additional information optional so that the viewer, subscriber, does not have to provide, if they should not wish to.

MS. LANDESBERG: Is there a limit to the number of off-line databases that Websites can tie to their registration data using Adfinity?

MR. BROWN: No, there is not. There is virtually unlimited databases.

MR. MEDINE: Maybe just to get a more concrete sense, could you walk us through from a consumer perspective how Adfinity works so we can put in perspective the collection practices that you allow to take place and subsequent use of that information?

MR. BROWN: Certainly. If I was going to go into a site, it is the perfect example of taking the direct marketing model that exists today and direct mail and promotions and moving it to the electronic environment.

What we have done is you would go in to a site, the site would ask you to register, a registration screen would come up. They would ask you to put your name, address, age, Zip code and explain what the information was used for and

allow you to opt-out. Once you did that, you would be given access to any information or content that you wished to receive at the site.

On a subsequent visit you would either be asked to log in or we would use a digital signature. We would, in the background, what I mean by preprocessing offline, merge that data, your identity data, with other databases at an aggregated level and bring that information in and be able to send more relevant targeted advertisements or promotions.

From a response standpoint we do not track you through the course of your session in the environment. What we do is measure your response to a particular promotion.

For example, if it is an airline promotion for you to take a trip, the only thing that we track or respond to is did you click through, did you respond in an affirmative or negative in response to that advertisement or promotion. So there is no other information we collect.

MR. MEDINE: Just to clarify, are you gathering individually-identifiable information? You say it is in aggregate form. Is it identifiable just to the point you know I have clicked through and you aggregate me based on other demographic information or do you maintain a file on me that would allow someone to market another trip directly to me?

MR. BROWN: We do maintain an individual file on

you. That's the file that also allows us to give you the option to opt-out. Without that individual level we couldn't differentiate you from anyone else and allow you to opt-out.

COMMISSIONER VARNEY: What is in the file?

MR. BROWN: Subscriber name, ID, name, address, and age.

COMMISSIONER VARNEY: How did you get that?

MR. BROWN: We asked you for it.

COMMISSIONER VARNEY: I gave it to you?

MR. BROWN: Yes.

COMMISSIONER VARNEY: No other way you are going to get it?

MR. BROWN: No, ma'am.

MR. MEDINE: What other types of databases do you use to enhance that information?

MR. BROWN: We don't provide the databases but we work with major database vendors who are in the direct marketing field. We have built what we call API's, application programming interfaces, which allow us to bring their data in and merge it. This is at the request of our customers. We do not own or retain any ownership of the data ourselves.

MR. MEDINE: What would be an example of the kind of database you might gather information from to enhance the subscription information?

MR. BROWN: There might be census data, there might be data from vendors such as R.L. Polk or Metromail, Database America, those sorts of publicly available databases.

MR. MEDINE: Who are your customers?

MR. BROWN: Our customers are generally publishers, merchandising companies, catalogue companies, people who are doing online reservations or transaction systems online and games and entertainment companies.

MR. MEDINE: How do they get in touch with the consumer after you have provided that information to them?

MR. BROWN: I am sorry.

MR. MEDINE: How do they contact the consumer? Do they contact an individual consumer with offers?

MR. BROWN: The consumer must enter the site. There is no ability to spam or take this information and shove it down somebody's E-mail box. You have a contract of sorts, a social contract between the consumer and the content provider, which says in order for me to receive this information, I have to enter your site. I have to come in.

And then those promotions or advertisements will be delivered to me along with the content or the games and entertainment or the transaction I wish to fulfill.

MR. MEDINE: Does this primarily apply to repeat visitors to sites?

MR. BROWN: Absolutely.

MR. MEDINE: 100 percent of who you are targeting with advertisements, are people who registered, you had a chance to enhance their demographic information with demographic data, and so you can better target particular ads for them on their next visit to the site?

MR. BROWN: Absolutely. It is for people who have a regular relationship and it is important to point that out. We believe that there is a relationship that's established between the site provider, the content provider, and the viewer and it is not designed to hit one time. It is the relationship that's established in return for me giving you my identity. I am receiving value for that and I am going to have this ongoing relationship. The same way that the advertiser also has a relationship with that person.

If they are using their own internal databases, if I am an airline and I want the use my frequent flyer database to make you an offer, that database, that relationship is one that we have established over time.

We don't, we being the advertiser or the site, it is of no -- there is no value for us to endanger that relationship. We want to maintain and enhance it.

MR. MEDINE: If I go to another site that you also have a contract with, is there any way of carrying over my information from one site to another?

MR. BROWN: We don't do that.

MS. LANDESBERG: Our next questions are for Chris Evans.

MR. MEDINE: Chief executive officer of Accipiter and co-founder of Da Vinci Systems and the founder of DDWWW Hotlinks.com, an Internet content site for the client server industry.

MS. LANDESBERG: Accipiter's product is called Ad Manager and you license this software that allows Websites to build databases of personal information using cookies and registration information and to sell ad space on the basis that those ads can be targeted on the basis of the database that the Website creates.

MR. EVANS: Let me amend that a little bit. The software does not allow the site to build that database as much as it allows the site to leverage a database which it has built. To the extent that a site has built a database of information from individuals, we can leverage that information to target certain ads and personalized advertising messages back to individuals.

MS. LANDESBERG: Okay. What kinds of personal information are the clients who use your software collecting?

MR. EVANS: Really for the most part I would say, and as a bit of background, our clients, many of them run in the top 20 Websites and everything down to very small sites that

are sort of regional magazine kinds of properties up to major search engines.

And as much as sites like to talk about being able to build that information up and being able to target against it, practically they are not very far down the road right now. There is some registration, we have a high tech site that has a voluntary registration procedure where you can personalize your site by filling out a form and get some personalized information, but really for the most part these sites, the discussions we are having are really out, a bit out into the future of how do we tie these things together and leverage them less so and what are you doing today.

MS. LANDESBERG: Are the advertisements that get placed with the aid of your software capable of collecting personal information themselves? Do they set cookies on users' hard drives?

MR. EVANS: There is a difference between collecting personal information and setting a cookie, but generally what an ad will do is it will establish a numbered ID for a person the first time they are seen on the site.

What we can do with that numbered ID, the primary use of that numbered ID is not show you the same ad over and over and over again, but to be able to show you, if we have already shown you this ad, we want to show you a different ad.

So for that kind of purpose, to be able to establish an individual trail and be able to show you a sequence of ads or be able to not repeat ads, we will use that information. Now, in that data -- so there is a data table that for each unique visitor to a site there is an ID number. And basically the extension of that is for a site to be able to plug additional information into that data table. Should that information exist, like gender or marital status or region of the country or whatever, that information could be used to personalize advertising.

MR. MEDINE: And is that identification also accomplished through the use of a cookie as well?

MR. EVANS: Well, the identification, us knowing from one person that comes in versus another is done via a cookie. And I think that there is overall sort of a discussion of cookie and sort of one observation today, there is sort of good technology, bad technology discussions that I don't think the lines are that clear.

For example, in the case of cookies, my observation looking at say my own cookie file, after spending a year and a half on the Web, is that primarily the information consists of some identification number, something that allows me to establish one person from another.

And in talking to sites and people that want to use our software, what we found is that for the most part the

information that they are using it for is really to get some sense of reach versus frequency; that is, to know what percent of the people coming to my site are regular people who visit weekly versus what percent are people that I have never seen before, and other fairly benign things.

I think overall one of the things that there is a distinction between explicit information, I am not seeing being drawn here, I guess, is explicit information, where I live, how old are my kids, anything that's, you know, sort of explicit, identifies me as a person in real space versus implicit information, what sites do I frequent, how often do I frequent this site, have I seen this ad before, where in the site do I go.

That in and of itself is not tied, unless the person offers explicit information, isn't really tied -- you can't tie it to a particular individual. I think there may be -- there are privacy issues on both cases.

COMMISSIONER VARNEY: Chris, would your guess, the percentage of information that you have identified or described as benign, you know, all the information that's tracked on a cookie, you said it is not tied to real space identifiable information unless you have offered it.

Well, what is going on out there? I mean, how much of the information is tied? How much is not?

MR. EVANS: Realistically I see very little of it. I

mean, companies would like to do a lot with it but when you get down to the core of it, they are dealing with, you know, dynamic HTML and they are dealing with sites that are growing by 100 percent a quarter and just trying to keep the right hardware and software in the system is stretching their true technical resources an awful lot.

COMMISSIONER VARNEY: It is your impression that those places that are employing cookies for information collection purposes are not for the most part including personally-identifiable information?

MR. EVANS: In my experience. That's not to say it is not technically possible and that there aren't sites that are, but as a practical note in my experience I don't see it very often right now.

MR. MEDINE: Using your system, you do talk about gathering information on a consumer based on their identification number. Is that information gathered at the Website as opposed to a cookie?

MR. EVANS: Yeah. As a practical matter it doesn't make a whole lot of sense to put personal information into a cookie. It is kind of like the Steven Wright joke about having the world's largest shell collection scattered around the beaches all over the world.

If you were to take, you know, a database of a million customers, you could have a million customer database

and keep it on a million hard drives scattered all over the world. What makes more sense is to have a common database and really have a key field, some identifier associated with that data kept on a cookie.

MR. MEDINE: And you talked about making sure that consumers don't see the advertisement twice, one reason for having an identifier. Using your system, is that true across the Websites; that is, if you show a consumer a particular car ad, will the cookie that you place for that particular Website also allow you to look as the consumer goes to another Website and say, uh-huh, that consumer has seen that car ad, I will show then them a different car ad on a different Website but both are used to develop their advertising?

MR. EVANS: Good question. Generally not, if the site is the purchaser of the software, the licensee of the software, then it is the site who is writing that information in.

Now, it is possible, and there are cases where you could be serving ads into several different sites and, in fact, there is another panelist, Kevin Ryan, who can speak a lot more to that. Our software could be used to do the same thing. However, I think there is a distinction of, you know, are two different domains necessarily two different organizations? We have one customer, CNET who has CNET.com,

Shareware.com, Games.com, and they have made a branding decision to make a domain name part of the product.

To go in and say basically different domains equals different organizations and thou shalt not cross information, there is one case that I know of practically where what you would be doing is sort of bull's-eyeing an organization where they really just have one enterprise, where they had different sites and they probably should be able to share that information between sites.

MR. MEDINE: By the same token if they don't share domain names, you don't know if you are dealing with a different part of the organization or a third party?

MR. EVANS: In the basic nature of cookies, if someone is on Shareware.com, you look like a different person than if you are on CNET.com. There are, if you have two sites, if you have two domains that are cooperating with each other, it is technically feasible for them to communicate about that information, but it can't be done without sort of a lot of effort on both sides, both domain's part.

MR. MEDINE: What kind of disclosures do consumers get, if any, about the information practices of firms that use your software?

MR. EVANS: Once again, because from an information gathering standpoint it varies from site to site, and we are not so much involved in that, in the collection of that

information, so it is not something I can really speak to expertly.

COMMISSIONER VARNEY: Do you know, Chris? Do your clients give disclosures?

MR. EVANS: I can think of really a couple of sites that do registration, and I can't honestly remember how the disclosure policies are set up and where they stand.

COMMISSIONER VARNEY: Would it be appropriate for you after these hearings to spend some time working with our staff and looking at, without raising proprietary information, obviously, but looking at a couple of different sites and seeing if there are disclosures?

MR. EVANS: Yeah. I will be happy to do that.

COMMISSIONER VARNEY: Thank you.

MR. MEDINE: We would be happy to hear from you about that. Maybe we will turn to DoubleClick, since you raised the issue of how you use cookies in terms of exposures of ads.

MR. EVANS: Can I make one or two more comments while we are on this? One, there was a comment about watching where each individual goes and this. Our personal experience is that when looking at that and the possibility of tracking individuals as they go from page to page and trying to correlate that data is that that data becomes incredibly unwieldy to the point that even though it is technologically

feasible, no customer would be willing to make sort of the information, the investment in all the high speed equipment they would need in order to practically do something with that.

What we found is that we actually aggregate that data on the fly and so we know how many people come through this page group versus that page group on a given day, but by the time that data is stored, it has been aggregated, you know, your participation in that is one unit of a number of 423,000 number.

I guess the other thing that is something I am trying to sort out, and you all kind of spoke to this, is I think from an information collection standpoint, sites really try to build relationships with customers. The first step may very well be to determine is this person a regular at my site, before I bother to solicit any information from them or trouble them at all.

I honestly feel looking at sort of how much information is involved and the cost potentially of asking someone a question, does it make sense to say: Well, if somebody visited us once a week for four weeks, then perhaps we can offer them some incentive to ask questions. What I think, what I am curious about is in general whether identifying somebody, determining whether somebody, before they provided explicit information, can be considered a

regular or not and doing that amount of tracking constitutes a privacy limitation.

MR. MEDINE: On your first point about the amount of information involved, it sounds a little like going from the period of paper files to electronic and that is it was very cumbersome to put together paper files until the electronic era arrived, and then it was easy to merge this data.

I am wondering if this issue of the amount of data and click-stream is just a technical issue and we will be back here in a year because everybody is tracking click-stream because it has become economic to do so.

MR. EVANS: I am not sure a year. We can look at the technology curve and say it is possible. Just to make a statement of what is practically going on and what is likely, people wonder whether everyone is watching over their shoulder at every site they go to.

My personal observation is most of these companies would not be willing to make the technology investment to do that. Even if they did, I am not sure they would know what to do with the information once they had it.

MR. MEDINE: Kevin Ryan is Chief Financial Officer of DoubleClick. Your views on how DoubleClick uses cookies to deal with this.

MR. RYAN: What we do is our business is selling and delivering ads for different Websites and we put them

together into a network and use the technology to deliver targeted ads. A fundamental element of that is anonymity.

We do not collect any names or E-mail addresses on people. The cookie is a smart part of the use there. And I agree with most of what Chris said in terms of the cookie really essentially now on the Internet space is used to control frequency.

That's partly because consumers have said that they do not like to see the same ad over and over and over again, and advertisers don't want them to see the same ad over and over again either, because they don't pay any attention to it. So the cookie can be used to track the frequency and it can be used to track frequency across different Websites in reference to a point David made.

That's beneficial for both consumers and advertisers for the same reason. Again, it is completely anonymous, though, which I think is the real -- we don't have anyone's name. Everyone is registered as a number. We are keeping it that way.

MR. MEDINE: Let's go back to the anonymity question. If a consumer registers at a site, does that matter in terms of the degree of anonymity?

MR. RYAN: We don't use any registration information.

MR. MEDINE: Your sole concern in using cookies is to

prevent multiple exposure to a particular ad?

MR. RYAN: Yes.

MR. MEDINE: And do you get any other information about the consumer, what site they were on?

MR. RYAN: Right now we don't use the registration information to do anything. The basis of us has been to really -- a good example would be an individual site has maybe .5 percent Swedish users. An individual site could not sell that space to a Swedish advertiser.

By creating a network we can lump it together and anybody who comes in from Sweden can receive an ad in Swedish, and that is beneficial to the Website.

MR. MEDINE: To clarify further, if you have cookies that sit on a person's computer for percent multiple Websites, would that allow you to know what Websites they had been to, since you are essentially developing a common cookie?

MR. RYAN: We say the person. We don't know name or address. We do track -- we can tell that No. 1265984 has been on one Website and another Website.

MR. MEDINE: You have the ability to track essentially where they have been, but you don't know who they are?

MR. RYAN: We don't know who they are. We have to track, by the way, we have to track which ads are delivered

for advertisers because we have to track that click-through because people are buying ads either based on the number of impressions or sometimes on the click-through.

For counting purposes, we do need to have a record of that to show we have delivered to the advertiser what the advertiser wanted.

MR. MEDINE: Only a matter of choice, you could combine registration information with that consumer's identity to their cookie to create a profile of where that consumer had been if you chose to. You have chosen not to; is that correct?

MR. RYAN: Yeah. At this point we are not using it.

MR. MEDINE: The technical ability is there, basically in your current system to add on a registration?

MR. RYAN: Someone else, an individual site that has registration information, they can choose to link that to a cookie and then attach that to the registration information. We don't do that.

COMMISSIONER VARNEY: Who does that?

MR. RYAN: Right now, as Chris said, I don't think very many individual sites are using -- I am not aware of any that are being able to deliver ads to registered users because individual sites aren't always big enough to be able to segment that information.

COMMISSIONER VARNEY: David, I have a question of

several of the panelists. You have a Website, right, corporate Website?

MR. RYAN: Yes.

COMMISSIONER VARNEY: Do you have a privacy policy?

MR. RYAN: Absolutely.

COMMISSIONER VARNEY: What is it?

MR. RYAN: It is listed on the Website, which talks about everything I talked about, anonymity, talks about the opt-out. We take privacy very, very seriously. It is crucial to our success that customers and clients and sites feel comfortable.

We have an opt-out cookie as well that we talk about in there that says that if people, even though they are anonymous, if people want to not have the cookie tracking frequency, they can do that. And therefore we no longer have ability to do that.

We encourage the Websites in our network to refer to our privacy policy. And our privacy policy is going to be audited by a Big 6 firm to give more confirmation of what we are stating. A lot of it is explanation, really. There has been a lot of misinformation about cookies and so we are trying to clarify that.

COMMISSIONER VARNEY: Can I ask that question of Chris and Yale very quickly? Do you both have Websites and do you have privacy policies and what are they?

MR. BROWN: We have a corporate Website, but our Website has no functionality in it other than information dissemination. And, again, in concert with what Kevin was saying, we have retained Arthur Andersen to review our privacy policies and our security functions on our software.

COMMISSIONER VARNEY: You do have a privacy policy?

MR. BROWN: It is in formation. It is not published on the Website.

COMMISSIONER VARNEY: How about you, Chris?

MR. EVANS: We do not. We have a Website. There is not a privacy policy on it, but because we are not really interacting directly with the customer. One of the things we are trying to sort through is to what extent, our people don't really see us directly, they see us through the lens of the site, so the sites have privacy policies. We are trying to sort through what degree should we be coaching them or providing them hints.

But we don't have something sort of finalized on that level.

COMMISSIONER VARNEY: Do you collect information about individuals who visit your Website?

MR. EVANS: When somebody comes in and asks for a demo, we do ask them for information. And I am embarrassed to say I don't think we tell them anything about what that is. That is a fairly small number and business to business,

but point taken that we should provide that.

COMMISSIONER VARNEY: Great. Thanks.

MR. MEDINE: Any additional questions? Kevin, earlier today we heard a mini-debate on the issue of third party's ability to place cookies. I take it if there were a standard set that did not allow that, that would put you out of business?

MR. RYAN: The cookie, out of what we do, the cookie is not used very much. A lot of the targeting we do is really without a cookie. The Swedish targeting I was talking about does not use a cookie.

MR. MEDINE: How do you target if you don't use a cookie?

MR. RYAN: We can recognize, any site can recognize someone coming in as to what country they are coming from. So we just pick that up and say if this person is from Sweden, we deliver a Swedish ad.

But I think the third-party cookie, there is no particular reason why third party, trusted third parties of publishers should be treated differently. The reason we do business with a lot of the very big blue chip companies is because they do trust us on this. And we are an out-source sales channel.

So it is perfectly normal that if you use another company as a sales organization, they have information about

customers and that's a choice that the company makes.

MR. MEDINE: The logic is if I trust a Website, I should also trust their judgment in advertisers as well?

MR. RYAN: In the same way that if you think, many parallels to that, if I work for a company that uses an outside payroll company, that means that someone else in another company does know my salary, but they have trusted that ADP or any other company that doesn't violate that or accounting firms, law firms. I mean, there are sales channels, so I think this is not unusual.

COMMISSIONER VARNEY: I think the difference, the possible difference in the analogy is when I go to a Website, I don't necessarily have any idea that there is an advertisement on the site and that there is information being collected about me, whether or not it is personally-identifiable.

Frankly I am less troubled if it is not personally-identifiable, but when I go to work, I know that I am going to get a paycheck and I know that the paycheck is going to get processed. There are some elements of notice that I think are present in the analogies that you have made that aren't necessarily present when you are kind of surfing through the Web looking at different sites.

MR. RYAN: To me it goes back to the issue of we don't know your name and don't know your E-mail address and

can't send you E-mails, can't do anything there. So I don't really think something there has been violated at all. We are a partner there.

I think there are a lot of examples, though, in business, the business where services are out-sourced and a consumer doesn't necessarily know some of the information is --

COMMISSIONER VARNEY: Would you feel differently if you did have personally-identifiable information? Would you have a different answer?

MR. RYAN: I don't think so because then it gets back to disclosure. We encourage, as I said, to all the sites and have been a leader ourselves in disclosing what information is being used for and where it is. And we encourage all sites to do that.

To the extent sites are collecting personal information, I think it is beneficial to everyone that they do disclose what it is going to be used for.

MS. LANDESBERG: If I might, how and when does the consumer get that disclosure? If I go to site X, which is in the DoubleClick network, am I told that? Does it disclose to me by clicking --

MR. RYAN: Talking about registration information?

MS. LANDESBERG: Is there a disclosure that the ad is part of the DoubleClick network and that by clicking through,

even though you can't identify me personally, you may track me to the next ad in a DoubleClick area?

MR. RYAN: If you put your cursor over the ad, DoubleClick will appear at the bottom. We can't dictate to a Website editorial content as to what they want to put on there. We are happy if people put our name all over the place, but that's a choice the Website should use.

MR. MEDINE: The consumer doesn't know a cookie is being placed by you on their computer, which would allow you the next time you visit a site, would target them, prevent them from seeing a repeat ad?

MR. RYAN: Now you are making reference to nothing to do with us, making a reference to how a browser works and how a cookie is embedded through there in Netscape and Microsoft.

MR. MEDINE: And a lack of disclosure to the consumer that it is taking place?

MR. RYAN: You are talking about how browsers work.

MR. MEDINE: We are going to place a cookie in a disclosure or not, a site can say, and the way your system operates there is no disclosure to the consumer that a cookie will be placed by you on their computer.

MR. RYAN: Or any site.

MR. MEDINE: Maybe we could turn to Tara Lemmey, who does similar work but has slightly different views on some of these subjects, Chief Executive Officer and Founder of

Narrowline Internet Company.

What are your thoughts on these questions of placing cookies, disclosing them, tracking people?

COMMISSIONER VARNEY: What does your company do and how is it different from the other companies we have heard?

MS. LEMMEY: Our company is a transaction system, buying and selling of Internet-based advertising. We work with various companies, including McGraw-Hill, whose privacy policies you heard earlier, to allow their sites to sell directly to buyers.

We don't touch any of the information, we have no access to the information, we have no ability to have access to the information. We early on hired Coopers & Lybrand to do an audit on us and an assurance audit so that every policy that we set up from the company from the ground up had to do with significant controls, not only over data but over information being transmitted.

We actually do deliver advertising. We do not use cookies at all anywhere. We have privacy policies that guarantee complete anonymity to anyone who is receiving an ad from us.

There are other ways to deal with the frequency issue which does not require a cookie. I am responsible for ad delivery, ad cost at an enormous number of sites, including across sites for gays and lesbians, across sites who

understand lookup service, across sites that understand what your news preferences are, across sites that understand what your food and cooking preferences are.

And it is very, very critical to not only me but the companies I am delivering ads for that no one can track that information across each other for competitive advantage purposes, if nothing else.

McGraw-Hill chose to work with us because of our privacy policies. They have subscriber-based information. They do not share it from publication to publication. Our Research Department has worked with them. We do do demographic and psychographic affinity-based profiling with complete anonymity to any one of the subscribers who use it.

And what we basically have done is create privacy walls and partitions between -- there are some important relationships, I think Chris talked a little bit about some of them, one is between the viewer and the site. When you go to a site you have an implied contract that you and the site have a relationship. And if a site wants to give someone a cookie, that's up to the site and the viewer to deal with that issue themselves.

At least that's our point of view on it. We don't deliver anything and we don't have any disclosure on knowing what that is because that puts me into a precarious position of if someone wants to know where other people have been, I

would have the information to tell them. And I have chosen not to have that information at all, so I can never be asked for it by anyone.

That implied relationship we think is very valuable from a competitive advantage perspective. If I am a major content site my most important relationship is between me and my viewer. Just like American Express understands that the relationship between their card holder and them is the most important relationship. To turn over that information is compromising your user base.

That is sort of an outside of it. There are a lot of issues that you guys started to raise, which I think are not covered that have to do with third parties. One is the use of clear gifs. We are talking right now about advertising, third parties delivering ads, that the ad showed up, it is possible to deliver a cookie with a clear gif, which is an image that has no image in it, so you don't even know the image is there. It is a phantom piece of information that comes down which may be delivering a cookie with it or may be able to track a cookie that's already placed.

By us not having cookies at all, it gives us no ability to deal with clear gifs. It gives us no ability to have phantom tracking across anything. And that's a practice that you do see coming into play in the industry, the use of clear gifs.

There are also a couple of other things going on here. We talked a little bit before, you guys in the last session talked about something that I would really like to refer back to for a second which is this notion of disclosure at all levels of the site.

One of the things that we do is when we actually serve anything, we serve our information with it so that the viewer can actually see and click through and see what our privacy policy is, not only on our site but everyplace an ad is delivered.

We are working with a company called Deluxe Internet, which is building sort of a browser-based product which is called a contextualizer. And when they travel with a user, they can actually identify meta-tags within the site and what we are trying to do is work with them on the TRUSTe Committee to identify with trust marks everything that's happening down to the page level or down to the video stream or audio stream level in that environment because this Internet is not hierarchal, you don't come in at a page level, you come in more geodesically, on the side levels.

More often than not you are moving in a geodesic environment from place to place, not top down, so you really do not have identifiers at that level.

Our proposal is that the site gets the same level of mark that their third party does. If the third party is

tracking information, you have to disclose that a third party is tracking it as well, all the way down to whatever page level it is happening at.

That's really fairly critical because certain sites that we work with have, we click, there is information that's being delivered by advertising, and then there is purchasing. So sometimes in the same site you can just be viewing and sometimes you can be purchasing. You will have very different marks and awareness and privacy policies for the purchase pages than you will for the content pages.

So to say that a site has one mark across the board doesn't necessarily make sense and you really need to know what those are at very different levels of your travels in this unbound media environment we deal with on the Internet. So that's probably more than you need to know, but does that answer the question?

MR. MEDINE: I think so.

(Laughter)

MR. MEDINE: That's very helpful. I want to shift around a little bit because I think there is a lot of interplay in the discussion and turn to Martin Nisenholtz, the president of the New York Times Electronic Media Company and manager of the New York Times Website.

He is here to talk about his Website policies. And I will disclose he will have to leave here in 15 minutes, so I

want to hear how The New York Times Website operates in the context of the discussion we have heard now about tracking and cookies and information.

MR. NISENHOLTZ: Sure. Well, first of all, as I think a number of people have noted, this is a very dynamic environment that we live in. And it is so dynamic that it changes day to day.

In fact, we covered the EPIC study in Cyber Times on Monday, and we realized that we ourselves hadn't been disclosing a privacy policy off the home page, we moved to do that. And I think as of today, this morning, it might be this afternoon, but I think it was this morning we off the home page of the New York Times on the Web now have something that says privacy information and --

MR. MEDINE: Self-regulation at work.

MR. NISENHOLTZ: Well, in a way. And our privacy policy might be a stretch, but certainly policy information is now easily accessible.

But, you know, to bring this to a level of practicality, and I think it is important to make this point, we have now put this privacy policy on the home page of the New York Times on the Web. And we get about 4,000 new people a day who come in. And if roughly 1 percent of those people, which is a very low number when you do anything on the Internet, people will click on almost anything, so if

1 percent of those people click on the privacy information and actually go beyond reading it and ask us to do something as a result of it, it will generate roughly 40 inquiries a day to our customer service operation, which on an average case-by-case basis costs us around $5 a hit to manage.

We are happy to do that. We believe that it is very important to make this explicit and to make sure our users understand what we are doing and, in fact, to be able to change the information or get information from us about what we are doing on the Internet, but there is a cost to do that.

And the only point I want to make is that when you aggregate up that cost, it means that we probably won't have a reporter covering these hearings because the cost is about $70,000 just to make that change, we estimate. We hope it is lower, in fact, as we automate it more and more. We think it will be lower, it may be higher if it goes from 1 percent to 2 percent, but there is an inevitable cost to anything that you do online.

Sort of as a corollary to that, and I think people need to be sensitive to this as well, the New York Times is making an investment in this business. We have fewer than 50 people working on the Website operation. And there are people, just like you, who have jobs and want to keep those jobs. And there is no guarantee that these are going to turn

into businesses.

So we are talking about a very nascent state here. We are talking about a state that is not yet for the most part proved in the marketplace. We are struggling every day to sell advertising in an environment where advertisers, quite frankly, still don't know quite what this does for them.

That's not true of all advertisers, but if you look at the environment in general it is safe to say the advertising community is still struggling itself to figure out why they should invest in this new arena. So my only point in telling you both that we now have an explicit privacy policy on the home page, to describe the potential cost of that, and then as a corollary the tradeoffs is to make the point that none of this is free and that all of it is subject to a lot of instability over the next couple of years.

Now, in terms of the explicit policy that we do have, and obviously now I am sure you are a user of our Website and will click on the privacy information button, we do ask users to register for The New York Times on the Web. We obviously make it clear when you register that you are registering, and we also have opt-out at the end of the registration form, so if you don't want to hear from us or advertisers ever again, you can do that, but we ask people to register really for

three reasons.

One is -- and this gets at one of the points made in the EPIC study, and I think it is important for us to air this -- that anonymity is not always good online. We don't want to create an environment, unless we bring the interactive features of the Website down, which we are happy to do, if that's ultimately what we have to do, but we don't want an environment online where people can come on to The New York Times on the Web and in an anonymous fashion say whatever they want, pornographic, libelous in a totally uncontrolled way. That's our policy. That's our view in terms of what we would like to see happen in terms of the general level of discourse on our Website.

We have hundreds now of forum topics that people participate in. Is the level of discourse always at the highest? No, it is not. And you wouldn't expect that because it is public discourse. But I think that the fact that people have to register for our site, they don't have to provide a name but they do have to give us their E-mail address, does go some way in ensuring that the level of discourse on the New York Times Website -- not that the users of our Website would necessarily do otherwise -- but that the level of discourse is held to a higher standard. That's No. 1.

No. 2, we are in a nascent business. We need to

understand at some level what people are using and what they aren't using, just as a product development guide for our own efforts. If we don't somehow do that, we are kind of at a loss to know which parts of the Website to invest more in and, therefore, to build up and which parts to potentially not invest in.

We have done a number of things that quite frankly for those users who have followed us are not, you know, going to light the world on fire in terms of business. The Bosnia project that we did last year was a good example of that.

We put that up for a Pulitzer Prize. It was the first Web journalism to be put up for a Pulitzer Prize last year. And as a result of that there is now a committee at the Pulitzers examining whether online journalism is something that should be recognized as having that level or that standard.

So I am not here to say that everything has to meet a test of the marketplace in such a Darwinian way that we are not going to pursue something if it is not totally profitable, but we do have to have some kind of product development process and information is key to that.

Then, finally, in an aggregate context, and we don't reveal any information to third parties, we don't even collect names, but in an aggregate context, yes, we believe that the Internet is a fundamentally different medium than,

say, television, which is a mass medium.

The Internet is only going to work as an advertising forum if the advertisers see it as a more efficient vehicle than mass marketing. Otherwise why would they invest in it? It doesn't have the same reach as television or for that matter print.

It is by definition from what I have been told by our advertisers a more direct marketing channel. Therefore, it has to be used in that way for it to make economic sense. Those are the three reasons that we do what we do, and I hope that at least addresses some of your questions.

MR. MEDINE: That's helpful. Do you have policies about secondary use of identifying information? That is, will you sell E-mail addresses or other identifying information?

MR. NISENHOLTZ: We will not sell E-mail addresses or anything like that.

CHAIRMAN PITOFSKY: You do use a cookie to put the person's identification or password on?

MR. NISENHOLTZ: They don't have to. We give them the option when they register whether they want to continue to put their ID and password in or either on. In other words, you can just put your ID in and preserve your password or put both in, but we have to store the information in the cookie in order to provide that convenience to the user. But

that is right, yes.

MR. MEDINE: Maybe we could turn to another Website operator, Arthur Sackler, Vice President at Time Warner, which supports over 190 Websites.

Can you talk a little bit about your company's policies about disclosing privacy practices by the company and some of the other issues we have been talking about?

MR. SACKLER: Sure. I will be happy to. One of the things that we have decided to do over the past couple of years as we have learned more and more concerns that consumers have had about privacy is to go slow. We were among those who were criticized last year for some of the things that we were collecting on surveys, et cetera, and we have simply stopped that, as far as we know.

I mean, we are doing what amounts to an audit, an inventory, site by site, page by page, on those 190 and growing sites in order to figure out exactly what we are doing and to put up our policies and notices as appropriate.

Now, as far as policies go, at this point it is a question of both yes and no. We have both a decentralized structure and that huge number of Websites. And a number of our Websites already have policies up. The rest of them, we are focusing on a corporate set of privacy goals, which will involve notice and choice and an opportunity to know what if anything is being done with the information.

And as those goals are developed, each of our Websites will be able to take those goals and adapt them for use in their own business context.

Now, one of the things that I think more directly addresses some of your questions is what is it that we collect and why do we collect it? Because of the large number of sites, we were asked to only focus on a couple of them.

One is Pathfinder, which is a gateway site maintained by our publishing subsidiary, Time, Inc., and the other is Warner Brothers Online, which is maintained, of course, by our studio.

In both we collect click-stream data in the aggregate. We do do what we call session cookies in Pathfinder, which exists only for the duration of the particular visit to Pathfinder. We don't do any cookies on Warner Brothers Online.

We do general notices of our privacy policies from the opening page of both sites and at each point of data collection. We specify what the uses of the data will be and, by the way, on those uses, we don't -- we don't pass any information at all on to any third parties from either site, and as far as I know, from any of our other sites, but I can't say definitively that there aren't some somewhere that might still be doing some of that.

Why do we collect the information? It is much like the gentleman from The New York Times was saying. We have to better understand what uses, who is using, rather, what parts of our offerings and how much. Unlike what he was saying, we are looking a little bit to the broadcast television model.

We don't want to charge subscribers to come to our sites and use the services that we have there. We want to have them advertiser supported. This is a business. We are in business to make money. In order to appeal to the advertisers, we have to be able to show them who is visiting or really how many people are visiting -- not the who.

We are not doing this in a personally-identifiable way. This is in the aggregate. And we have to get that raw traffic information in order to get back to the advertisers and let them know how many people are viewing their ads, then figure out from that what is the cost per thousand, et cetera.

We then want to refine our sites in order to better target our offerings to whoever might want to come on the site. So for all those reasons we are collecting information.

We do collect a little bit of personally-identifiable information. That is for things like delivering newsletters or for Warner Brothers Online or delivering Web cards, if you have ever seen that. We have happy birthday cards. We have

Batman cards. Come and take a look. It is good stuff, especially if you forgotten a birthday card for somebody, send this over the Net, it is great, last minute.

So we do collect that information for all those reasons. Then, again, I would like to agree with the gentleman from The Times, when on Pathfinder, individuals want to go to our chat rooms or our bulletin boards, we do ask that they register. We do ask for a fair amount of personally-identifiable information.

We want to know to some degree who is there if we ever need to find out for some sort of reason that would relate to doing something or communicating in some way that we think would be totally inappropriate or maybe even unlawful.

We also ask people to register if they are going to Pathfinder Personal Edition, which is a deluxe version of Pathfinder, offers some rather specialized services.

So all of that, though, is voluntary. No one needs to register for anything in order to browse either Pathfinder or Warner Brothers Online. So people do know from that point what our policies are, where that information is going, what it is going to be used for, and it is all voluntary. They don't have to do it.

COMMISSIONER VARNEY: Can I ask a couple questions? Do you transfer the data within the company?

MR. SACKLER: No. As a matter of fact, within Pathfinder, within Warner Brothers Online, doesn't go to the parent.

COMMISSIONER VARNEY: You may not know this, it is a little technical. When I send the Batman birthday card, do you capture and keep the information on the person I am sending it to?

MR. SACKLER: I don't think we do, but I would have to check to make sure.

MR. MEDINE: Following up on the first question, you have a corporate policy or do you think you will have corporate policy about sharing information across Websites? That is between Pathfinder and Warner Brothers and CNET to gather information?

MR. SACKLER: We haven't addressed that because no one in the company has expressed any interest in doing it.

MR. MEDINE: Turning to your neighbor there, just on the Website mode here for a moment, we have Shelly Harms, the Executive Director of Policy and Government Affairs for Nynex. She is representing both Nynex and Bell Atlantic today.

If you could talk about your company's Website policy.

MS. HARMS: Yes, thank you very much. I would love

to be here representing the new Bell Atlantic, but that has been delayed a little bit.

COMMISSIONER VARNEY: Not our fault.

MS. HARMS: It is not.

MR. MEDINE: Not our department.

MS. HARMS: I was involved in developing and implementing Nynex's current privacy policy, which has been in place for three years. And right now I am involved in developing the new Bell Atlantic privacy policy. And I will be involved in implementing that once the merger closes.

We are here for two reasons. One is to listen and learn because we are in transition, not only from separate companies to one company, but also from our traditional lines of business to new lines of business in the online world, and I found today extremely illuminating.

The second reason is because we thought it would be useful for you to hear from a company that has a strong tradition of privacy how we are trying to adapt to the online world. I will go briefly through our current practices online.

Right now the only personally-identifiable information we collect is through a voluntary means. For example, on our Nynex home page we do allow people to apply for a job with Nynex and they know they are sending their resume to us. We then use that information for the purpose

of evaluating the job application. We don't retain it. It is only for that purpose, and it is voluntarily supplied.

Similarly, Bell Atlantic Internet Solutions, which is our new online service provider, gathers information, name, address and a means to build a customer for purposes of providing the service only. We do some general tracking of what people are doing when they are on our Website, but that is not identified as to who is doing it. So we use it only for purposes of improving the Website at this point.

We would like to obtain more information, for example, Big Yellow, which is our electronic directory service would like to use information about a customer's interests in order to better match an advertiser customer of Big Yellow with willing buyers.

Bell Atlantic Internet Solutions would like to have more information about the customer's preferences in order to make the Website -- or not the Website -- the online service that we are providing more convenient for the user.

So I want to turn to the privacy policy that's going to govern what we will do when we start collecting that kind of information. And it is the privacy policy I am going to talk about, evolved from what we do now in our traditional telephone business.

We both have, Bell Atlantic and Nynex, both have

strong policy. We filed those with the FTC last month. This morning I filed as a supplement, I filed the planned new Bell Atlantic privacy policy. It is virtually finished. And it will be formally announced once the merger closes.

I want to say something. This is sort of a response to something this morning. In developing these policies, we found the work of the Interactive Services Association and other industry groups very useful. And we, in fact, participate in some of those efforts.

However, we didn't adopt that wholesale. And we felt it was very important to customize our policy for our business. We talked to some of our customers. We talked to consumer groups in our area. And we felt it was important to develop our own.

And it differs from -- you will see it differs from the McGraw-Hill policy, and it should, because we are in completely different businesses. We have different relationships with our customers. So that's a short way or long way of saying that we think this should be allowed to evolve and be flexible, depending on the various businesses involved.

We found when we did this our existing policies actually applied pretty well to the online world because what we had was broad principles that applied to all our lines of business already. It included that we must inform our

customers of the information we collect about them and their options to control its use.

It included that we must provide opportunities to control how we use that. It included we must enable customers to control whether we disclose that information to third parties. It included that we must consider privacy in developing new services.

All those apply equally well to online, the online world as they do to the traditional, more traditional lines of business.

We added some things too in the text, sort of underlining our black letter principles to try to deal with some online issues. We added the commitment to provide a Website disclosure. You won't see it there yet, but we are hoping you will on day one of the merger.

We added the idea of not sending E-mails, if they are not wanted. I think that we may have to examine that again in light of some of things I am learning today, but I think that the idea that -- our idea that we are doing this could be a competitive disadvantage because other companies might not be doing it, that's not the way we look at this at all. This is an advantage.

And we have, I think that the trust level we have been able to build in the telephone area is something we really want to carry over. And we think that that will be a

huge advantage to do the right thing on privacy in the online world.

Just to tell you where we are in the process, the principles that we filed this morning are our black letter policy. They are going to guide us in implementing them. It is similar to what we implemented in Nynex over the past three years.

Our first projects for implementation are going to be drafting a brochure for the telephone companies to bring that up-to-date, but also to draft the Website disclosures. Other projects include conforming practices over the new company. You can imagine the kind of things we are doing.

It is also going to include getting out to all employees what the policy is, training for employees, projects like that.

I want to close on a note on government's role here. I think that this workshop has been just tremendous because I think it has galvanized the industry. And I think that a lot of the things you are seeing today would not necessarily have happened, at least not today, not by today, if it hadn't been for this.

So what I am saying is, you know, continue to do this because it is enormously useful. The only other thing I would suggest is that I would be interested to know -- I am echoing Esther Dyson -- what the government's policy is on

collecting information when I am hitting your Website.

COMMISSIONER VARNEY: Actually we did deal with that. There are Government Records Acts. And when we had our last privacy workshop last year we created a list serv for people to participate in ongoing discussions of the issues that were raised and we had to -- I think, Bruce is here in the green shirt behind the camera -- he was working on the Website for us and all of our general counsel, everybody, we had to figure out what information we were required to retain for government records purposes, what we could do with it, and we did, we disclosed it.

It is one of the things we talk about wherever we go, is all government agencies, who now all have Websites, figuring out what information they are collecting and what they are doing with it. And, in fact, I think it is in the most recent privacy paper that came out of OMB.

MS. HARMS: That's interesting, great.

COMMISSIONER VARNEY: I think we are trying to practice what we are preaching.

MR. MEDINE: I would like to turn to our last Website representative, which is Linda Goldstein, who may or may not operate a Website themselves, representing the Promotion Marketing Association of America; she traded places with Ronald Goldbrenner earlier today.

I understand the organization has conducted a survey

of Websites, and we would be interested to hear the results of that.

MS. GOLDSTEIN: It has been very interesting sitting here listening to the comments made by the specific Website owners, many of whom are members of PMAA, and I think that the experiences that they have discussed here this afternoon really were reflected in the survey that we conducted.

I would like to begin by saying that from the perspective of the PMAA, its members that use the Website, use Websites, use it really as part of an overall integrated marketing program. Many companies are rushing in increasing numbers to develop and improve their Websites, but in terms of perhaps where the industry is and how effectively some of the policies have been implemented, at least our discussions with our members indicate it is not due to a lack of sensitivity to the privacy concerns, but typically in a large Fortune 500 company you may find as few as three to five people who are responsible for the entire Website operations of the company. And, quite frankly, they are overwhelmed and kind of learning as they are going along.

And in many respects they have their hands full just trying to deal with the business aspects. And sessions like this are good because they increase the sensitivity of companies to ensuring that where they are philosophically actually is implemented on the site.

What we learned from our survey, which I need to caveat by saying that we did send the survey and the survey is on record in our written comments, we did send the survey to all of our members. Unfortunately as with any voluntary message, the response back -- perhaps we should have hired a direct marketing professional to help us get a better response rate, but the response rate was not as high as we would have expected, but I think the results are directionally informative.

In terms of the purpose of the Website to our members, clearly the sentiment that others have expressed here is reflected in our membership. Our members use the Website principally to help build brand loyalty and strengthen their relationships with their customers.

The Website is part of a broader integrated marketing campaign. And they look to the Web much as they do other direct response vehicles as a way of interacting more directly with the consumer and of delivering more targeted advertising and promotional offers to the consumer.

Of those that responded to our survey, only about half actually collect any information at all. Of those that do, none of them release that information to outside third parties.

Now, I will tell you that sitting here we have seen a lot of other issues come up that quite frankly we didn't

address in our initial survey. And I think this has been helpful in terms of helping us perhaps refine our survey as we go out and try to expand on that information, so I don't know for example among the members that have multiple divisions, to what extent the information may be shared across those divisions, but we do know universally that our members do not share the information with any outside third parties, only a small minority of members that responded collect any click-stream data, and it is aggregate click-stream data being utilized solely for the purpose of measuring traffic to the site, not for any other purpose.

None of our members who responded send unsolicited E-mail. Virtually all of our members are aware of the industry guidelines, whether they use the DMA guidelines or Casey guidelines. They are all aware of them.

Again, I would say about 75 percent of those who responded that have a Website have developed their own internal policies. Only one of the members who responded indicated that they actually do put the notice of the policy on the home page. Others may have it as part of an overall legal page or may not have it at all.

However, the few companies that do collect anything more than simply name and address -- and there were only, I believe, two or three of us among the respondents -- those companies did indicate that they do provide at the point of

data entry some disclosure. The fact as to how that material might be used and as well as an opt-out provision, and I think what that tells us is, again, the importance of maintaining flexibility.

That at least from our members perspective, the type of disclosure that they feel may be necessary if they are simply collecting name and address may be different from what they may feel is necessary if they are going beyond to collect more sensitive proprietary data.

And I think overall the sentiment that has been expressed to us in terms of our members' usage is that, again, the primary objective of this medium is to help build brand loyalty. And while the policies may not be fully developed and articulated on the sites yet, philosophically they are highly committed to not taking any action that would undermine a consumer's confidence or loyalty in the brand or in the company.

MR. MEDINE: Thank you. I want to close the session on information practices with Eric Johnson, who is a professor of marketing operations and information management at the Wharton School of the University of Pennsylvania and director of the Wharton Forum on Electronic Commerce.

You have done some study in this area, and I am happy to hear what you have learned about current practices and what your concerns may be about future practices.

MR. JOHNSON: Our major interest was implicit data collection, not kinds of things you know, the keyword you type. I will argue there is a market test where that information is valuable. Do people buy keywords? The answer is yes. Implicit information certainly has that --

MR. MEDINE: Explain.

MR. JOHNSON: Type the world automobile. Is the ad that's placed in the next screen customized as a function of that? The answer is yes. And those keywords are sold. So implicit data, there is a market test for it.

In fact, I want to argue that I think this kind of data can be a very good thing, both for consumers and firms, and we don't know how to use it yet. My analogy would be think about supermarket scanner data and your analogy to no one quite knows what to do with it, supermarket scanners in 1980. Now not only is it an efficient industry now because people collect that data.

Just an analogy, we have stores now you walk into, the equivalent of having a video camera on your head, you don't know who it is, but you know what people are looking at it. A quick place where that might be useful. Let's take Edmonds, the direct person, site that provides information about cars. I can get what is called from marketers an invoke set. Is that valuable? I would argue that could be quite valuable.

In fact, we know from lots of research done at Wharton and other places that there is a very high correlation between the amount someone spends looking at sites and preference. That, I think, would be very useful, on one hand. The scary part is you might predict what someone will choose before they choose it.

On the other hand, you might be able to help them find alternatives on what they like. I think there is real value for firms, but we did a survey looking not, a random survey, basically talked to some experts trying to sell products to help people analyze click-screen data. And we would say: Gee, 2 to 5 percent is the number I would guess who are looking at click-stream data. Most of that is to redesign the site to make it easier for the consumer.

Windham Hill reorganized their site because of alphabetical lists, people who have groups in A were getting many more hits than names with Z. So it is useful, but that's not an individual level site.

The question is not what is happening now, in my perspective, but what is happening five years from now. I think it is more Internet years than real years here.

MR. MEDINE: Where do you see things heading?

MR. JOHNSON: The issue is what consumers know. I think it is informed consumers who benefit, can benefit from the analysis of the click-stream data. And the question is

basically I am afraid this is sort of -- I am trained as a cognitive psychologist, but I am afraid what consumers think about is based on perception.

For them it is not the fine people on these panels, but spammers they get confused with. I have gotten a spam. Based on your browsing answer, we thought the following pornographic site would be of interest to you. I swear there was no reason for them to have thought that. But, you know, my guess is the average consumer might get very worried in receiving that kind of spam notice.

I think if there is careful informed consent on the part of consumers in place, that it would be a very valuable tool.

COMMISSIONER VARNEY: Eric, I'm not sure if you have any information on this. Do you know, would you hazard a guess or do you have any information about what is being collected online today that's personally-identifiable without knowledge and consent?

MR. JOHNSON: Certainly by definition most analysis of click-stream, which is done at the aggregate level is done without knowledge and consent. I mean --

COMMISSIONER VARNEY: Also not identifiable.

MR. JOHNSON: Usually not identifiable. Technically the presence of a cookie makes that as a single site identifiable over time in many ways we have talked about.

COMMISSIONER VARNEY: Right.

MR. MEDINE: I know Kevin wanted to address this issue of marketing to consumers and the degree to which consumers are concerned about that practice.

MR. RYAN: Just one thing, I wanted to give a perspective to this. We think making customers feel comfortable about privacy is very important, but we have delivered $3 billion in ads over the last year. And out of that, and we are well-known in the Internet space in the advertising space on the Internet, we have received, I would guess, maybe 25 or so E-mails, people having questions about privacy.

We put a privacy button on our home page to make sure we answer all those questions. Very few people choose to go there, even though they are passing through and see the button. We provide the opt-out method for people. Very few people choose that. And we shouldn't forget that customers really do -- people on the Internet have chosen to have advertising-supported Websites over subscription Websites.

They are not going to be able to get free content forever, so they have to choose one of the two and they are choosing this. Between them we give them a choice between targeted information and untargeted. Guys into sports would rather see a sports ad than a perfume ad, so there is $600

million of advertising that's again generated this year alone in the second year, based on using information as intelligently with as much disclosure as we can overall.

And we should take that into consideration before trying to restrict anything in that direction.

MR. MEDINE: Yes.

MR. SACKLER: David, before we go, I brought along copies of our Website pages and policies and there are more copies outside. And these are the black and white hard copy versions. We will have some color versions for the record.

MR. MEDINE: We appreciate that. I want to thank this panel for enlightening us about the current state of technology as a tool for gathering information about consumers.

We are going to take a 15-minute break and turn to technology as a tool for addressing online privacy, which will have a major announcement at that point.

(A brief recess was taken.)

PANEL IV: TECHNOLOGY AS A TOOL FOR ADDRESSING ONLINE PRIVACY

"A review of available technology and current development efforts."

TIM BERNERS-LEE, Director, World Wide Web Consortium (W3C)

JASON CATLETT, Chief Executive Officer, Junkbusters Corp.

PETER HARTER, Global Policy Counsel, Netscape Communications Corp.

SAUL KLEIN, Vice President, Marketing, Firefly Network, Inc.

DEIRDRE MULLIGAN, Staff Counsel, Center for Democracy and Technology, Internet Privacy Working Group (IPWG)

MARC ROTENBERG, Director, Electronic Privacy Information Center

***

MR. MEDINE: Thank you for returning. This session is a session on technology as a tool for addressing online privacy. The question is are there ways to empower consumers to protect privacy themselves online.

And we are going to start off with a number of discussions and demonstrations. The first by Deirdre Mulligan, who you have heard from previously, from the Center for Democracy and Technology, will talk about IPWG and what that all means.

MS. MULLIGAN: I would like to step up here.

MR. MEDINE: Sure.

MS. MULLIGAN: It is a pleasure to be here today, especially during the technology piece of this because I think it is very important, especially as we look at the Internet, that we make sure that policy and technology are really wedded together.

Interactive communications media, I think, really give us both risks and opportunities in the privacy arena. And during the Federal Trade Commission's hearing last year and in the record that came out of that, there were four key elements that many, many participants realized had to be addressed if we were to have an effective regime for privacy on the Internet.

And those were notice to individuals of information practices; choice, meaning individuals needed to be able to make decisions about the flow of personal information; access, meaning individuals had to be able to gain access to information held about them by third parties; and security, meaning that there is no privacy without security.

At the conclusion of the workshop last year a number of us put our heads together and decided that in order to craft a framework for privacy that addressed these concerns it was going to -- we were going to have to engage in a cooperative effort that built upon the expertise in the

policy area, the technology area, and the business community.

Out of that formed the Internet Privacy Working Group, which is a cross-section of industry and consumer and privacy organizations working to develop a framework for addressing privacy concerns in the online environment.

What IPWG, Internet Privacy Working Group, has been doing is develop a language for users to communicate privacy preferences and Websites to communicate their information practices. The work of IPWG has not been done in a vacuum. It is meant to contribute to the World Wide Web Consortium Platform for Privacy Preferences, which you will see shortly and which is really the meat of the technology.

The P3 project is an attempt, I believe the first attempt, to actually implement the concepts of notice and choice into the framework of the Internet. And I think because of this it actually has a profound effect to kind of shift the way in which we have thought about self-regulation in this environment.

I want to say at the front end that the Internet Privacy Working Group and the larger P3 project at W3C only address a limited set of privacy issues. They do not address, for example, access issues. They do not address oversight and enforcement issues.

However, I think that within the context of these other issues, within the context of self-regulatory efforts

and other efforts that are being undertaken, such as TRUSTe, that this is a definite step forward.

The IPWG vocabulary in the P3 project will enhance individual privacy in three ways. They will enable individuals and parents -- I want to emphasize we did pay very close attention to the very independent needs of children on the Internet -- to exercise control over the collection, use, and disclosure of their or their children's information through a set of individually chosen preferences.

This would happen on the browser side. It also will enhance privacy by providing a common language for use by Website operators in notifying users of an information practice in a standard, easily understood format. This is particularly important because there is a diversity of players on the Internet.

The Center for Democracy and Technology, as well as Microsoft, have to be able to express our privacy practices in a way that is going to be meaningful and simple for people on the other end.

Probably most importantly it is going to enable users and Website operators to communicate and in some instances find mutually agreeable terms regarding the handling of personal information. It is not going to force individuals to disclose information, nor is it going to force Websites to deal with people on terms they don't want to, but it is going

to facilitate a dialogue.

There are a few things I want to just emphasize about the vocabulary, if you could put the screen on.

IPWG really focused on creating what I like to call a flexible and robust vocabulary. If you look down the left-hand margin, it is broken into two sections; uses and disclosures. And it talks about use in, you know, the uses for system administration, the uses to support the transaction, the uses for research or product development, and it goes through a whole variety of uses that a Website might make of information.

Similarly, it goes through a whole set of reasons that a Website might make disclosure of information. And we tried to set those out in fairly understandable language so that if you were a Website operator you would be able to look at this and say this is what my Website does.

I would say this is similar to the effort that DMA went through in developing their practice specification. Across the top you have information that puts this in context. Is it physical contact information? Is it your name and address? Is it cyberspace contact information, your E-mail address? And you can see the rest, computer information, navigation and click-stream data, preference and demographic data.

A Website would fill each one of these out, either

for the entire Website or per page. A Website might have a general information set of practices, and they might have a page where they collect data because you register. They might have separate practices at that page. And to facilitate the individual decision-making, you would want to have that granular ability to flag where practices vary.

The vocabulary developed by IPWG, I think, is important in thinking about how to effectively craft a solution for Internet privacy. The P3 platform, the P3 project of W3C, it builds upon the medium's interactivity.

This is really a different medium than our traditional paper-based world. There is the capacity for real-time decision-making and communication. And I think that is not something we should -- it is something we should really explore because unlike the paper-based world where we have had this tug about opt-in and opt-out, this real-time communication, I think, can dilute some of the transaction costs that have forced us into that rather contentious battle.

Similarly, it can enable this in a seamless manner, so unlike a Fair Credit Reporting Act form where I have to go and read the form whenever I want to find out what some of these practices are, I can actually configure these in my browser on the front end and know that I can surf the Net

securely.

I think most importantly when we look at self-regulation or we look at legislation, both of them have problems in mapping on to the Internet. For the same reasons that we have said national legislation may not be effective because of its inability to be exported as individuals step across our country's boundaries, self-regulation has some of those same problems.

DMA, ISA, and other entities, eTRUST, may take very good steps, but their effectiveness is also limited to their members. They may not be nation members, but they are still members.

By building something into the infrastructure that actually addresses some of these privacy issues on the front end, we can build in a base line that establishes a communication as notice and consent model to be used flexibly around the globe. And I am going to turn it over to Tim Berners-Lee.

MR. BERNERS-LEE: Thanks, Deirdre. On behalf of the World Wide Web Consortium and 180-odd member companies and other organizations across the globe, thank you for inviting us.

I would like to, in the next few minutes, try to provide you what P3 for privacy purposes is and a little bit of how it works in particular from the user perspective. So

we have a few slides and a demonstration which is a working mockup.

I would like to thank various people who have worked with us on this to help make the demonstration possible. I mention at the bottom of the slide, AT&T, CDT, DMA, IBM, Microsoft, and the Princeton Review actually have a Website with a privacy policy. And we have used this in the demonstration today.

The basis of P3 is that there is on the user's side, there is a user and a publisher. On the user side, there is a right to a choice as to how the user's private information is used. That choice is made in an informed way.

On the side of the publisher of the information, the person running the Website or person on behalf or on whose behalf the Website is run, makes a commitment as to how the personal information is used.

P3 consists -- will produce technical protocols which will allow the user's browser and the server, the Web server programs, to communicate across the Internet to make sure that those two commitments via each site have been made and understood. It makes a match between the two.

The P3 technology is used for expressing assertions about privacy and negotiating them. It doesn't, as Deirdre mentioned, address enforcement. There is a limit to what technology can do. It does provide hooks.

In some cases it is possible to do some enforcement, to actually provide technology to stop people getting information which they are not authorized to use; otherwise to use the market to use the strong market forces which drive people to assert a good reputation by establishing trust with users, by having verified the good policies, and clearly the third leg of those possibilities is regulation.

To clarify our relationship with IPWG, W3C is focused on the technology and IPWG is focused on the vocabulary. The strength of the platform, there are three layers to it. The platform from W3C is the protocols which allow two computers to talk about privacy. When they talk they need a vocabulary with defined terms. IPWG is focusing on that.

And when a statement is made, for example, when a user decides what they would or would not like, that profile-setting is done in terms of the vocabulary and then is sent across using the protocols. And it is important that globally those protocols are consistent so that the computers, clients themselves all over the Web, all over the world have the same protocols.

It is useful if there are global vocabularies so people in different countries can, for example, talk about privacy, but it is possible also to have several vocabularies. And it is obviously crazy to imagine at the top level that everybody's personal preferences would be the

same.

W3C and IPWG also worked together to marshal the resources which will be able to be used to get the technology actually produced. So the situation at the moment, I should clarify, is that we have been talking about privacy for a long time.

Four months ago the Consortium put together a proposal for specific action. We called it P3. One month ago, on the 15th of May, the review period by our members finished, so it is now a formal project within W3C. We are very happy, in fact, that the work we do builds on experience from the IPWG's world of labeling material for parental selection, and protocol we call PEP for negotiation.

It is built on some interesting work, but, on the other hand, we expect that the P3 work will not be specifically linked to specific Web technologies. It will work with anything because it will not be bound specifically to, for example, HTML pages or gif images or things, HTTP. We hope it will be a general framework, and work with future technologies as well.

We will give you a quick demonstration. One of the ways in which we expect this to work is that rather than a user reading and defining all the fine print about what exactly they would or would not like their information to say, where they would like it to be distributed and what they

would like done with it, that there will be certain settings, profiles which will be pre-prepared, perhaps by well-known bodies which have the user's trust and which will be downloadable.

Let's look at the list of settings which have been prepared by IPWG. Let's look at a list for children. Notice it is quite reasonable to have different sets of profiles for children and for adults.

For example, when you are setting a profile for a child, you may want to disable the ability to give out credit card numbers. We can look at one of these, pick it up just by short description, but if you are more interested, you can look back in detail, more detailed example, more detailed text, cumulative text, natural language about it.

We can also dump down to this table which defines it specifically in terms of, in this case, the IPWG vocabulary, so if you remember Deirdre's slide, which was a matrix of things you could or could not do with data, this is the matrix, if you use this profile, of things you think is reasonable and you are prepared to be able to do with your data.

Let's go back now to the list of profiles and if we can have a look at one for adults.

These are summarized partly so they will fit on the screen so you can read them. If we look at the third one,

this is one which has been prepared for example so that a site is allowed to share personally-identifiable information but only so long as the user is allowed to review that decision.

Now, that is an overview of the privacy profiles that you might pick up from a Website that you trust because it is supplying you with some suggestive settings for your browser. And you can pick them up in the browser. And let's imagine that now we have done that, and let's go browse away.

We have -- this is the material from the Princeton Review, used with permission. As we go around we have loaded a particular profile so as we route, each time we click, the P3 software is ensuring that the commitment being made by the publisher matches those we require as we browse.

Where we are a student browsing for information about possible colleges, and there is a service at the bottom that we may want to sign up for. There is a button that says sign me up, for those of you at the back. When you press that, we go to a form, uh-oh, a form is going to ask us for information which is going to be used in a way that we haven't so far accepted. We haven't given our consent to this.

So now you imagine that this would be put up as a dialogue box by your browser. So suddenly a dialogue box pops out with a number of buttons. One of the options we

have got is to go and look at the state of the site that might want to explain about its policy.

Let's follow that link to the person. Fortunately, we have a site here which actually does have, by coincidence, something to say about its policy. It may say all sorts of things and explain why it wants that data.

Under this point we may decide it is totally intolerable and stop browsing, click cancel, and surf somewhere else or we may go back to that dialogue box and decide on a number of options in particular. One of the options, unless we are a child browsing under parental control, we have let's just override this for now, these guys for this session, let's override it and give them whatever they want. I will take the risk.

There is also a button which allows us to, for this, to adopt this policy for this site. So we click on that. That tells the browser, yes, go get the settings, the profile settings which they have suggested. There is a button also which we won't look at now, leave for another time, which allows you to go and look at what those settings are.

Suppose we actually press the accept policy. So now from now on when we go back to that site the browser will use that policy. There is the application form. The browser is letting us see it. And on the application form it bears the information.

Now, you may have heard of the OPS proposal to the World Wide Web Consortium made by Firefly and Verisign on Monday. That concerns not only the privacy question but also the automatic provision of information.

If you can imagine that something that might happen here is that information has actually been filled in for you on the form because this information which you have said you are happy to have it automatically disclosed.

So we have now accessed information which we wouldn't have before. The system would have stopped us accessing.

There is one more thing I would like to show you, and that is some software being written which is running in the browser which allows you to actually delve in at any time to see the details of the profile that you have picked up.

So you can pick up a profile with a particular brand name, someone you trust, pick it up for your mother or school or whoever, but you also might go in there and change the elements of that matrix.

Can we bring that up, Joseph?

UNIDENTIFED SPEAKER: It is coming.

MR. BERNERS-LEE: We have lots of things running on the machine. We have a server running on the machine.

Let's give you a few points to take away. You notice that although you have to start off with computer protocols which allow two machines to start talking about privacy,

those really have to be adopted across the Web.

From then on you can have a number of different vocabularies. They can be done by industry groups. They can be done -- IPWG is doing one, very nice to have a global one, but you can have many, with negotiation use special ones and you can have very many different sets of recommended settings in terms of those vocabularies. You don't need to register them centrally. This is sort of an architecture which worked very well in the Web before.

It would be very nice to have a common agreement internationally on the vocabulary. It would help understand what a foreign site needs when it challenges you to allow certain use of information.

What we haven't talked about is what happens when you go to a site and it doesn't say anything in P3 language. And we can't, technology alone cannot -- P3 cannot address what happens when P3 isn't used.

Let's go over -- we will get back to that. The Consortium is working to evolve this technology in response to, I think, three pressures. There is the market demands. Our members need to go forward for market reasons. They are very aware, they click into this area, of the policy questions which we fold in. And we have technical requirements we fold in together so the W3C is the meeting place for all those elements.

If we can quickly before our time is up sneak back and show you what the browser interface may look like here, if you played with it. Going into various bits of software with your computer before, you will be familiar with these tabs across the top and the option boxes that you use for setting a lot of references, particularly users used to setting preferences on a computer, so it is fairly familiar.

In fact, what this is doing is looking at a particular setting. I would imagine that when you are browsing the Web the particular settings you are using would be identified by an icon you can see very visibly or perhaps by something else, such as the color of the window, the border of your browser or something like that, so as a user you can be very aware of which person you are using, of which mode you are working privacy-wise; how much information you are giving away, so you don't accidentally make the mistake.

When you are going behind that icon, that particular setting, you can if you want to go into the matrix and go back to Deirdre's slide again. It is being able to go in if necessary, check or uncheck one of the boxes so that personally I can decide that for my own personal reasons I really don't want information about whatever it is about my machine used for helping the market research on their products.

That concludes our demonstration.

MR. MEDINE: Thank you very much. We have a couple of questions we would like to ask. Commissioner Varney.

COMMISSIONER VARNEY: Yes. That was terrific, Tim. The first question I have is what happens in your example when you go to the Princeton site and by the time you got the message that they don't adhere to your -- they are on a different privacy platform than you have expressed a preference for, how much information have they captured about you potentially before you cancel and jump out?

MR. BERNERS-LEE: Well, as I say, the system works by assurances made in either direction. Clearly when you make a first request to a Website, your request may go out with no assurances. So this is equivalent to the situation where P3 is not being used.

So there is no assurance which is made by the user. And at that point the thing that is done by the server is as though nothing has been agreed to, no negotiation. The server can respond and come back and say: Whoa, I would like to do -- I would like you to accept that we are going to track your address, will you please come back to me, having accepted this privacy profile, here is a suggestion, here is Y, and here is what it is. And here is where you can download it, et cetera, but, yes, an interesting moment before this happened.

MR. MEDINE: Can I clarify that? What is it a site

can gather in that moment about you, if anything? The moment when you first basically make contact but before you have a chance to have an exchange of preferences expressed, can they gather your domain name?

MR. BERNERS-LEE: Typically, a lot of people go through proxies, and one of the ways is through proxy, which will actually mask who you are among a certain set of users, so it varies. They can capture your IP address, that can sometimes be turned into a domain name. Sometimes that will track with you and sometimes won't.

In fact, that's quite a complicated question. There is not a lot of information, and I am not the expert on how you do that.

COMMISSIONER VARNEY: The question of what happens when you go to a publisher of a site that isn't a P3 participant, would you get a flag right away or could you set your preferences that I only want to go to sites that are P3 speakers?

MR. BERNERS-LEE: Clearly those are both possible.

COMMISSIONER VARNEY: Maybe we will hear more about this from Peter. The relationship between the OPS proposal and the P3, it sounds like at least in part what this could be is that the OPS standard would allow you at your choice to fill out a variety of personal information and then any time you choose to transmit it, it is already in place and can

go.

I guess my question for both of you or maybe more for Peter is can your choice on OPS be zero information?

MR. BERNERS-LEE: I would like to say one thing. I don't want to second-guess the working group situation. OPS has been submitted to a working group. We started the working group. We are explaining to you what the target or goals of the working group are and base assumptions, but we can't say exactly what the paper, policies of the finished product will be. That's the proviso I put down there.

MR. HARTER: Actually, I think Saul Klein from Firefly could answer that question better than I could.

MR. KLEIN: Within the OPS standard, there is a default setting. I never want to share any information with any site I come into contact with. So it is very much up to the end user. I never want to share, ask me if I want to share, or I will always share. And you can actually -- and hopefully we will be able to demonstrate this.

COMMISSIONER VARNEY: Okay. Thank you, Tim.

MR. MEDINE: A question for Tim. Just to make explicit what you have been saying, for this process to work there has to be essentially a self-regulatory effort on the part of Websites to adopt this, not only the protocol but essentially the commitment through the language to honor requests by consumers?

MR. BERNERS-LEE: This works by negotiation. So it isn't that everyone has to -- all the sites have to do it, but a user can insist that anywhere that they visit does.

MR. MEDINE: And once they do do it, they have to abide by what they say or we get into deceptive trade practices and so forth. The question for Deirdre, following up with Commissioner Varney's question, the language, IPWG language, does not have an option of I don't want to go to any sites that don't protect my privacy; is that correct?

MS. MULLIGAN: It has an "I want to be close to anonymous." As Tim was saying, when you go to a Website your IP address, I mean, potentially could be linked back to you through some means.

However, the commitment could be that, you know, that the site is saying that they are not going to be collecting information for any purpose other than kind of system administration.

MS. LANDESBERG: I guess my question is can I set a preference -- it seems as though IPWG did not elect to include a preference for someone who may want to block or be denied access to sites that don't have a posted privacy policy.

MS. MULLIGAN: Actually IPWG thinks that's a very important thing, especially in the children's area, that people would be able to say, similar to the platform for

content selection, if you look at the browser you can say: Don't go to sites that don't state what their policy is.

But I think what Tim was probably trying to say -- if I misspeak, please correct me -- that the specification itself doesn't do that. That's something that happens at the browser end.

W3C, I think, plays a role in making model recommendations as to what interfaces might look like and IPWG has a very strong feeling about what that interface should look like. For example, in the children's area, you know, there should be a button and the default, I guess if you were talking about a default, would be that there is no kind of negotiation with children; the idea being children can't consent.

Similarly, that you can choose to go to all Websites regardless of whether or not they have a policy statement, or you can choose to only go to Websites that are participating in this P3 specification. And that that is really a primary piece of this.

MR. MEDINE: Again, just to clarify, is that option available for adults under the current scheme?

MS. MULLIGAN: Absolutely. I mean, what you are looking at is a vocabulary, and it is a draft, but in our discussions, while it is not evident up here, that was clearly something that is being discussed.

MR. MEDINE: You should have a choice to visit non-P3 sites?

MS. MULLIGAN: Yes.

COMMISSIONER VARNEY: Hopefully the technology will work if you are a Website publisher or host, if someone brushes by your site and doesn't land because you don't have the P3 vocabulary, you will know how many people you are missing because you are not participating.

MS. MULLIGAN: It is actually something that Jeff Fox from Consumers Union brought up the point, and I think it is a very relevant point, that it is very useful for businesses to know why they are losing business. If it is because of a lack of privacy practices, that it would be very useful to be able to have that communication occur.

And it is certainly something that I think I am interested in having. I am not sure whether or not the specification can support that, but I agree with you. And I am sure there are other people in IPWG who think that would be a useful thing to do.

COMMISSIONER VARNEY: Thank you.

MR. MEDINE: Thank you very much for the very useful demonstration.

I want to turn now to Marc Rotenberg to talk about a subject we haven't spent much time on to date, but essentially the ultimate form of privacy can be anonymity.

And Marc will address that question. He is with the Electronic Privacy Information Center.

MR. ROTENBERG: Thank you, David. My presentation is going to be a little bit different from Tim's. This is more descriptive than prescriptive. It is based on survey research that we did last week looking at 100 of the top sites on the Internet.

And we came up with some very interesting findings, but I just want to briefly introduce the survey approach, the next slide.

First of all, as I am sure you are all aware, the privacy issue is obviously important and the GVU poll this morning, as well as the other polls that were released, underscore this point. And we are hearing a great deal about many different approaches, self-regulatory and technical.

We were interested in simply going out on the Internet and seeing what the current privacy practices and policies were in June of 1997. These things are changing quickly, changing daily, in fact.

We picked June 5th, last week. We used the list of Internet sites reported by 100hot.com, which is a fairly reliable listing of popular Websites. You might have chosen another.

We decided not to look at issues related to security encryption or spam, although they are obviously there on

Internet privacy. We looked at essentially seven issues at each site. We asked, first, was personally-identifiable information collected? Then, is there a privacy notice or policy that's readily available?

To some extent we tried to assess if this was a good policy. We wanted to see, for example, were there restrictions on secondary use? Did users get access to their own information? Sometimes it is called a user profile. Was it possible to be anonymous at the site? And, finally, were cookies enabled?

On the first question where we looked at 100 sites, we found that approximately half collect personally-identifiable information. If you are wondering what do we mean by PII, we thought name and address were personally-identifiable. We thought E-mail was personally-identifiable, but we did not treat the TCPIP address as if it were personally-identifiable, although there are techniques, of course, in some circumstances to make a link to an individual. We were for the most part trying to use common sense applications of some of the key terms.

Not surprisingly, you will see requests for personally-identifiable information where there is online registration, surveys, user profiles. If you do purchasing online, if you are buying books, for example, most likely the Website will want to know your mailing address, so they can

ship that information or that product to you.

But also what was interesting is that many of the sites that do not collect personally-identifiable information are some of the key sites providing news and information to the online community.

For example, on our list we found, among others, CNN, TV Guide, Washington Post, Weather Channel seemed to be doing quite well without any personally-identifiable information from their site users.

One of the issues we identified in the study, which is available on our Web page, is the issue of database matching. It is a question I know Commissioner Varney has raised a couple of times about her relationship between the transaction record and mailing lists and so forth. It has traditionally been one of the key issues in the computer privacy realm.

We would suggest that for people who want to go back and continue to look at these issues, the next question would be for those sites that collect personally-identifiable information, is that information linked to another database? And AOL is one of the companies recently where some questions have been raised about that.

Of our 100 sites, 17 had privacy statements or notices, but we found it was often difficult to find these statements. So we tried a series of different techniques.

We used the "find" command in the browser software, we went looking at the FAQ page. You can understand, of course, in describing what a person is doing and not what a crawler might have done, trying to find those terms at the site, but we think as a matter that's how to experience Internet.

We found some privacy policies after registration. We didn't think that was a very good idea. It has to be there before you sign on. And eight of our sites had restrictions on secondary use, which is to say some explicit statement about a limitation where information would be used.

How good is a privacy policy? And I would be the first to concede there are many different ways to do privacy policies, but as a general matter, I think the threshold for any privacy policy is really there are some responsibilities for the organization collecting information and there are some rights for the person who provides the data.

We were interested, for example, in whether the sites told the users why the information was collected and how it would be used. One site which we have generally thought was pretty good, and we still think is pretty good, although I think Commissioner Varney is likely to raise some questions about the privacy policy, is Amazon.com, which tells you on the one hand they will not rent or sell your information and

then tells you to send them E-mail to be really sure that they won't rent or sell the information in the future. We thought that was a little bit too ambiguous.

Time/Pathfinder, they have a fairly good policy and we know it is on their home page.

Access to one's data or, to speak more broadly, access to one user's profile is one of the critical tests of privacy policies. You find it in virtually every U.S. privacy law from the Fair Credit Reporting Act to Video Privacy Protection Act. It is in international guidelines. It is not the same thing as access to a policy or statement. It means literally one can see the information that has been collected about the individual that is held by the organization.

Oftentimes it is described as transparency. We found virtually none of the sites provided any real means to provide access to one's own data. The one exception, which is notable here, is Firefly.

By the way, in going through this presentation I should make a note, EPIC receives no support from any of these organizations we survey. I am going to say good things about some companies and maybe some bad things about some companies. We are not being supported by any of them. This may be why.

(Laughter)

MR. ROTENBERG: What is interesting, of course, about Firefly is they allow individuals to create their own profile, to access their profile, and to revise their profile. From a traditional sort of privacy principle, that's really getting very close to the bull's-eye, anonymity. This is really one of the big issues, we think one of the core issues. I will say more about it in a moment.

Not surprisingly, if you think about it, virtually all Websites allow you to access the home page on an anonymous basis, taking for the moment my stipulation TCPIP addressing still doesn't really provide a link to a unique user.

This is essentially the storefront, the shop window. More interesting still is that the majority of sites in our sample allowed users to visit and use services without disclosing any personally-identifiable information.

I think if you take apart a Website you will be surprised how much information you can typically receive without ever saying who you are. News services, as I noted before, routinely base the provision of service on the fact that the user doesn't disclose personal data.

We thought this was a critical indicator of how privacy is currently today protected on the Internet as opposed to some sort of futuristic proposal, and obviously

expressed some support for this.

The cookie topic is very controversial. As I said, we are trying here to be more descriptive than prescriptive. We were interested simply in how many sites had enabled cookies. We didn't go to all the pages, so we don't know if we caught all of them. At least of our 100, we found 24.

Oftentimes cookies are used for registration, simply to store a password on a user's system, but they can be used for advertising purposes as well. What was significant to us was that there was no notice to the user about the use of cookies.

You can go digging in your system preference file and look at your cookies, in some of the browsers you can enable a message which comes up, but for the most part I would say for most users it is really hard to track how cookies are being used. For this reason we thought the browser standards actually played a critical role.

Here are the conclusions. Although privacy is a top concern on the Internet, few sites today actually have privacy policies or real privacy practices. I think this is a critical point to understand just how important it is to develop some safeguards.

In the absence of privacy policies, there is really no assurance that when you provide personal information at a Website, it may not be misused.

And so we went straight to the heart of the central question. Does notice and consent work today? A lot of people say the government should only step in if there is market failure. We found a bigger problem. There is simply no market. There is no market failure. There is no market.

There is no way today in June of 1997 for people who are on the Internet to express a preference to protect their privacy through any type of relationship expressed on the Website. We also found that the use of cookies is not made clear to users, but again anonymity seems to play a very important role in protecting online privacy.

So our recommendations follow from this. We think there should be a privacy policy that's easy to find. We think it should be a good policy. We want individuals to be able to get access to their own user profile.

We think that cookies transactions should be more transparent, so that people know what is going on and, of course, that anonymity should be encouraged, but until these things are done, our conclusion truly is "surfer beware."

I want to add two quick sort of epilogues here. Very interesting, after the survey came out we got this nice message from Steve Jenkins, who is the Webmaster of Windows 95.com. And he wrote to us after he saw the survey. You can read it. He says: "We had previously been unaware of these concerns. Thank you for bringing them to the attention of

surfers across the Net. And we have created a privacy policy statement and posted it on our site. We are currently in the process of putting a link to our privacy policy statement on every page. Again, we thank you for helping us better our site." So we were very pleased by that response.

Then there was the news story yesterday which appeared, a fellow writing for the news, Chris Stamper, Netly News, "Infoseek is watching you. Next time you go looking for information from a search engine, remember that the search engine may be looking back, at least if you use Infoseek."

We are left with the point that even as we may be establishing progress through privacy safeguards and policies on the Internet, there is a host of issues still out there that arise very quickly that some writer will bring to your attention as well.

Thank you.

COMMISSIONER VARNEY: I have one question. You surveyed 100 sites, right? 49 of them had privacy policies, mostly hard to find?

MR. ROTENBERG: 49 collected personal information. 24 had policies.

COMMISSIONER VARNEY: Do you think that that extrapolates across the Web or is it different because you really are dealing at the top 100?

MR. ROTENBERG: I have no idea. My suspicion would be among the larger sites for these issues are more likely to arise, it is more likely that you will see a policy statement.

COMMISSIONER VARNEY: That's what I am getting at. It would not be accurate to project that maybe 24 percent of Websites had policy statements?

MR. ROTENBERG: I don't think so. I think it overstates it.

COMMISSIONER VARNEY: Privacy is much much lower. Thanks.

MR. MEDINE: We will now turn to Saul Klein, who spoke a moment ago, Vice President of Marketing for Firefly Network and to Peter Harter, who is from Netscape, we heard from before.

MR. KLEIN: I am going to talk from over here, if I can. I think this works. Great.

I would like to thank the Commission very much for inviting us to come along to talk at these hearings. Firefly/Netscape today are going to be talking about personalization with privacy and discussing a framework for a personalized network.

So let me just go straight into what we are going to be doing is talking about some of the issues at stake, talking in a bit more detail about the open profiling

standard and also demonstrating the Firefly Passport, which is actually a working version of some of the features of consent and profile management as described by Marc, and then giving a brief demonstration as to what the Passport would look like in an OPS world.

So what is at stake? Just in the top line figures here, there are millions of people online. There are hundreds of thousands of Websites. And figures suggest that next year alone we should be expecting 55 million additional interested adults in the U.S., nonusers of the Internet.

The number of host sites coming on to the Internet grew by 70 percent last year. What we have here are hundreds and hundreds of thousands of sites, millions of people, and no way, as the Commissioner has just pointed out, for people to actually protect their information or establish trusted relationships between sites and users.

So with all this explosive growth, what is slowing things down? Well, obviously something we are all here to discuss and have talked about and Marc just talked about is there is no widespread framework for privacy on the Internet.

And when we think about the different constituencies and how that affects things, well, we know that people feel uncomfortable and see little value in exchanging information.

If we are going to talk about a personalized network where people can find the information that they want, the

businesses can do business on the Internet and people need to feel comfortable and need to be in control of how they exchange information.

Secondly, businesses have no widespread framework for relationship building, which means that electronic commerce is stalling, the growth of advertising on the Internet is not being delivered to content sites and for young Internet companies -- and Firefly is a young Internet company -- to innovate on the Internet you need to be able to make money, but you want to be able to make money within a framework where you are building trust because that's what the Web promised.

There are some interesting figures which hopefully people have had access to produced by BCG and eTRUST, which actually go to speak to these points. I think Peter will be discussing those.

If you are software developers, one of the strengths of the U.S. economy and increasingly the U.K. and Israeli economy and many other economies is software developers. These software developers have no standard platform for even building privacy into their applications.

So this is a great scenario that there are hundreds and thousands of Websites out there, there are millions of people, but there is no framework to succeed. So I will hand it over to Peter to talk a bit about how we are trying to

address that.

MR. HARTER: I thought I would come down and do it Jerry Springer-style.

But, again, it is great to be participating in the hearings on the second panel. And at an appropriate time, this is a footnote I have, an update on the cookie question left over from this morning. I made some calls back to Mountain View and we have a detailed answer for that.

And as Saul was saying, there is a market need based on consumer concerns. A lot of people have already said a lot of things about surveys of the concerns consumers have.

And here are some data points we want to share with you this afternoon. As you can see, 70 percent of consumers are concerned about privacy. If that many people are concerned about it, well, as I said last year, privacy is a snake or an opportunity. I think it could be perceived as a snake because it is going to come and bite you with bad PR, perhaps, at the company with your customer base or it is an opportunity to do something. And Netscape and Firefly deem this to be an opportunity.

We also have seen that almost 50 percent, 42 percent refuse to give any kind of information. This is a block to E-commerce. Some commentary in the press to date about the open profiling standard has said that the Internet is not about just exchange of information for the purposes of

E-commerce, it is about just being able to browse freely and anonymously.

That point has a lot of credibility to it. I would think governments and companies and jobs are at stake here in terms of having this global information infrastructure. We have seen in this town, at least since 1982, a big thrust in the NII and GII and European Commission and Information Society and this information for this country, I think E-commerce has equal status, if not more important status, than that, very credible point of that.

E-commerce is very important and there is a need to get around this blockage. If consumers are afraid of using personal data on the Internet, they are refusing to give up necessary registration information for the conduct of electronic commerce, something should be done about it.

The final data point you can see up here is 34 percent of consumers give inaccurate registration. Well, having no information is a bad thing. Having inaccurate information is even worse, I would say.

You can't really run a business on having inaccurate data. And that's a pretty simple straightforward point. We have seen the opportunity is as much as $6 billion over the next few years. And although Andy Grove last week in D.C. said the Internet time works at a clock speed three times faster in speed and government is three times slower in

speed. I heard that on audio and it came in every 30 seconds. And the technology doesn't quite keep up with the rhetoric.

We here in Washington, even though it might be coming somewhat south of Netscape in Sunnyvale, whether it is $6 billion, $16 billion, or only $600 million, these figures are hard to predict because so much changes month to month, quarter to quarter, year to year. And $6 billion is something worth doing something about.

So the next slide, Saul.

We have really good news today. A few weeks ago Firefly, Netscape, and Verisign had submitted the OPS to the P3 Working Group of the World Wide Web Consortium. Today at noon we announced with Microsoft, both Netscape, Microsoft, and over 100 companies now support the open profiling standard.

Some of you may have seen a recent article in U.S.A. Today that there is a petition on the Internet requesting that Netscape and Microsoft try and adopt open standards. And I did reference this morning that there is a lot of jostling about what is open standards.

Well, I think the issue of privacy is so important to competitors on the Internet marketplace that we have come together in cooperation with support and good leadership of the experts at the W3C over the past few weeks to craft

support for the OPS.

And as Tim Berners-Lee referenced, we can't say much now about the details of the OPS because we have given it over to the open standards process. And we are, although we authored the proposal, it is now part of an open standards process. And it is going to change because there will be input from many people. And it will be part of the W3C process for getting this specification and turn it into a standard that industry can implement and the consumers will benefit from.

A few points about OPS that I think will remain strong, that it is designed as a standard to enable personalized electronic commerce. What that means, this is very laborious for the consumer, fill out name, address, Zip code, credit card information. When you go buy things from merchants like Amazon.com or when you subscribe to online newspapers like New York Times. Heretofore things like cookies were used to store the information.

When I log on to read the New York Times, I see at the bottom of the screen, welcome, and they give my user name. That is stored in the cookie. When I go through the registration page of the New York Times, they tell me that is what they are going to do in order to have me automatically log in, so I don't have to type my user name and password in every time, but that's not the best place to keep personal

data.

The OPS profiles is a better place to put the data for a number of reasons. One of which is that data is under the user's control because not only does it make the profile gathering activity for Websites more efficient, because they have a common framework as opposed to doing it ad hoc in their own way with cookies, which is opaque if not invisible to the average consumer, but the profiles remain encrypted on your hard disk.

Now, what are the implications for U.S. export controls? I won't comment on this this afternoon, but I do think that user control profiles that are defined fields, you can enter information you want to disclose and there are levels of profiles, and the fact that it is encrypted on your machine means that you have a lot more control of personal data as it gets shared with servers out on the Internet.

As I mentioned, over 100 leading companies in all sectors from advertising to hardware, to services, to publishing, and the public policy advocacy groups like EFF and OPS clearly demonstrates that it is trying to do its best efforts towards self-regulation.

MR. KLEIN: I am going to move on to a demonstration of the Firefly Passport as it is today. The Firefly Passport, which you see on the right-hand side here, is as Marc was describing a means for an individual on the Internet

to control how their information is stored and exchanged.

Currently this works through a server side application. And these profiles are stored with Firefly, but what I want to show people is some of the things that you can do with your Passport, so obviously it is personally identifying you.

What I can do is I can go in and I can have a look at my profile. So what I have here is my member name. I can choose that to be obviously whatever I like. It can be a screen name. It can be my real name, my E-mail address, optionally my first and last name.

Firefly doesn't actually require first or last name. As Marc made the point you can actually do very, very successful personalization and community building without actually having to personally identify anyone.

The other thing Passport allows me to do is to make that information private or public. As I go to interact with other people who have Firefly Passports or sites that accept Firefly Passports and some of the sites accepting Firefly Passports include My Yahoo. Yahoo is a customer of ours, Barnes & Noble, Ziff Davis, AOL, Greenhouse Networks, et cetera. So that's how I can manage my profile.

Let me show you how this works when I actually go to a Website. I can use my Passport to actually see some of the sites that accept the Firefly Passport. So, for example,

here is a site called Film Finder, which is a movie site. It recognizes me using the state maintenance aspect of cookies, which was described before. All it is doing there is saying this is a user name. It is not using cookies to target advertising or do anything else because you are in full control of your profile.

What you have here is obviously a link to the Firefly privacy policy and an eTRUST or now TRUSTe mark. Firefly is one of the early members of eTRUST and on the Steering Committee. And we are delighted that that is actually launched now and going out into a wider marketplace.

So the other thing is just in terms of having information accessible. Your privacy policy is actually a link from your Passport. Nearly 3 million people on the Internet today are using this.

Now, let's go into the OPS world and have a look at how the Firefly Passport would work in the OPS environment. Obviously from Firefly's point of view, as I say, we're a small, young company, for us to be able to work together with both Netscape and Microsoft to advance these standards and have them adopted and within the framework of the W3C where organizations from all around the world can contribute to this is very exciting.

So this is -- I am going to try and exit this briefly so we can get a better view.

This is going to be the Passport or at least a demonstration of the Firefly Passport within the OPS world. And this little window, which hopefully is going to open up in a moment, I don't have a proxy server running on this, but it still doesn't seem to be running too quickly, may mail is opening. Here we go.

This is, if you like, an OPS version of the Passport. What you have here is a Java application, which actually sits on the end user's machine and allows the end user to control their information actually on their desktop.

Again, recognizable, it is running within my Netscape client here, which obviously supports JAVA. And what is happening is I have two views. I have a personal view of my profile, and I have a community view of my profile. So let's have a look at how I could edit my personal information.

What this is going to do is bring up, if you like, and obviously the work being done by Gateway within the context of the P3 working group is incredibly valuable here. What you have here is the ability -- and I don't know how well people can see this -- to be able to set permissions against a variety of anonymous information.

So, for example, my member name, which is in this case "Cape", I can say always show this information, ask me if you want to share this information, or never share it. And I can do the same thing for Zip code, country, industry,

gender, et cetera.

The other nice thing about OPS is it is an extensible data model. It is built on the V-card open standard, so my contact information, which you will notice is separate from my anonymous information, can have home and work information.

And, again, I can see permissions all the way through. I can have currency. I can have interest. The value here, obviously, is if I have a trusted relationship with Barnes & Noble, I don't want to give them my credit card every time I go to the store, so I can just say okay, just show them my American Express card and I can expedite the ease of that transaction.

From a community viewpoint, if you like, what the personal view is, how do I see the rest of the world? The community viewpoint is, you know, how do I want to present myself to the rest of the world? We look at the community view. What we see here is my community viewer for places that I go on the Internet. For example, Netscape, a site called Launch, Yahoo, people who are part of my community and interests that I have.

What I can do here is I can use my community viewer to actually go to one of these sites. You go, this is a site called Launch, which is a site for -- which provides music information. And this window which you have just seen pop up there is a request for information.

This site, which I haven't visited before, is saying Launch requests your ZIP code and your music interests. It has a statement. It is saying Launch will use your Zip code and music interests solely to provide local concert information. And I can then say always allow this exchange with Launch, allow this exchange only once, or don't allow this exchange.

And what we can see here is that there is a framework for a trusted third party, be that Coopers & Lybrand, who has audited Firefly's privacy policy for a year now, or an eTRUST or a Better Business Bureau, et cetera, to actually display that Launch is a trusted site. I can say, okay, fine, that's great, I would now like to go in. Let's see what the site experience would be like.

So I go into the concert area. It recognizes me. I have given my Zip code information, so it knows that I live in Boston and some of the bands that I like. And it is telling me that -- I don't know why it is telling me Marvin Gaye is playing in Boston, but it is telling me that --

MR. ROTENBERG: It is an old version.

MR. KLEIN: Bands that I like are actually going to be in that area. This is a good model to have a look at how the end user benefits, how the business benefits the Website, in this case Launch, and also the artists, the acts, the labels benefit as well. So this really is a win/win

situation.

The other thing I can do, which is very, very important and people talk a lot about it, how do I actually ensure that the transactions happening between myself and an Internet site are being logged. If I want to view my personal information, what I can do here is in a similar model, if you like, to a credit card statement, look at the interactions that have happened between myself and Websites.

So, for example, I can go and say on this particular date I used this service. I can see whether that's a trusted service or not. So, for example, I can go to Launch, I can read the statement they made, they will use my information for X, Y, Z. I can go to the IBM site. And they are saying your occupation and industry information will be used to direct you to different IBM products and services.

So not only are there business-to-consumer applications here but obviously great business-to-business applications.

And, again, I can see that they have a trusted third party; whereas Cirque Du Soleil, which wanted my Zip code and E-mail to give me news of local performances, doesn't. I have a choice in those situations to say, okay, I will give them this information once or maybe I won't give it to them at all or et cetera, but here is an explicit model for

actually implementing some of these technologies and public policy practices that we have discussed today.

So on that note I guess we will sit down.

COMMISSIONER VARNEY: It looks like what you have got creates tremendous convenience for consumers and businesses, and also provides Firefly with an enormous amount of personal information. You probably have more personal information than anybody on the Net.

MR. KLEIN: Well, I mean, that's a very fair point. To look at what Marc was saying, there are definitely opportunities for businesses to collect and manage information. And that's regardless of whether you are on the Internet or whether you are off the Internet.

And to me that's a lesson online, online question. As a business you have an information relationship with someone who you can trust, someone who respects your privacy and someone who gives you a good service.

So from that point of view I would like to think that, you know, even though we are a small company, we are sort of trying to do that well and do that in a way where people can trust us, but now in working with Netscape and working with Microsoft and with the contacts of the W3C really opening up that ability to anyone, and I think we have seen from the support of OPS and some of the studies, the BCG study, the GVU study and also our own experience of 3 million

Passport holders and some Websites with large businesses like Barnes & Noble and Yahoo, that this is a model that people want to follow.

COMMISSIONER VARNEY: Do you track information about your Passport holders, keep track of where they go, what they do, what they buy?

MR. KLEIN: We don't use cookies to track people.

COMMISSIONER VARNEY: Well, you don't need to.

MR. KLEIN: Because the model here is informed consent. What we do is we give the end user a tool to control their information.

COMMISSIONER VARNEY: I am asking about their control of your use of their information. I come to you, I sign up, I am a Firefly Passport person. I buy books, buy wine. You now have an enormous amount of information about me. What do you do with it?

MR. KLEIN: What we do with the portion, say yourself as a Passport holder would collect within your Passport, is like any other business. You as an individual can choose whether you want to share that information with Firefly in the OPS model or not.

If we add value to you as an individual because you are sharing information with us and we are saying here are places, for example, where, you know, you can buy books that you might like or go and find news that you might like and we

are never going to share that information with a third party without your explicit consent, which we say in the Firefly privacy policy, all of our customers subscribe to the Firefly privacy policy as well, so really what we have tried to do within the abilities of any company in this, as Marc pointed out, there are not that many organizations doing this.

COMMISSIONER VARNEY: You have 3 million Passport holders, right? So you have 3 million names, presumably.

MR. KLEIN: We don't have names. We don't believe that it is necessary to collect name or address.

COMMISSIONER VARNEY: You don't have their name or street address?

MR. KLEIN: If people choose to give us the information, they are doing it within the context of informed consent and with the explicit understanding, which is attested to by Coopers & Lybrand and eTRUST, that we are responsible in terms of our uses of data and information.

One of the interesting things about that statement model which we just demonstrated is that what that allows someone like Coopers & Lybrand to do is actually go and look at a business like ourselves, transactional, data transaction logs, if you like, and say --

COMMISSIONER VARNEY: Let me ask you something. If you have 3 million Passport holders, how many names and addresses do you think you have, percentage-wise?

MR. KLEIN: I would say probably less than 15 percent. Because for our business it is not necessary.

COMMISSIONER VARNEY: Okay. Of the 3 million Passport holders that you have, how many do you have informed consent from to share their information with third parties, however we define that information?

MR. KLEIN: First of all, we never share anyone's information with third parties. What we say in our privacy policy is, one, any information you share with us will not be shared with any third party without your explicit consent, informed consent.

No. 2, the information which you share with Firefly will only be used for offering personalized service, and for providing personalized advertising if it is going to be used in any form, it will only be used in aggregate form and with no identifying information.

And, No. 3, if you want to cancel your account, click cancel at Firefly.com and we will take it out.

COMMISSIONER VARNEY: Okay. Now, when you join with Netscape and Microsoft for the OPS standard, and I realize it is now in the Open Standards Committee so we can't talk about what it is ultimately going to look like, how does it really change what you already do?

MR. KLEIN: Well, there are a couple of things that change. One is that currently the way Firefly Passport works

is, as I mentioned before, it stores profile information on the server side in a product we call the Firefly Passport.

By working with the major platform vendors, Netscape and Microsoft, we can ensure that that profile information can also be stored within client side and on someone's machine. And that information can then be, you know, encrypted on the end user's machine. So there are a couple of things.

One is that extending the Passport on to the client side, outside of just pure JAVA script, which is what I showed people in the first version. The second is, quite frankly, to have the support, the unprecedented support of Netscape, Firefly, Microsoft, over 100-plus organizations to be working within the context of W3C and the P3 working group means that from our point of view this doesn't work unless the marketplace grows.

MR. MEDINE: I have one OPS question. As I understand it, OPS basically allows consumers to consent to the release of personal information to a Website. The question I have is what assurances do the consumers have about the subsequent use of that information by that Website?

MR. KLEIN: In terms of the assurances, what OPS has striven to do, as Tim mentioned, in terms of what technology companies, I guess, are capable of doing, it is a tactical

framework in which public policy and business practices can set and you can actually have responsible measures put into place, both on the client and the server side, to say that Coopers & Lybrand is monitoring this site, we have an eTRUST mark, and this is a brand that I trust, IBM, Guinness, et cetera, for example, and I know that they are not going to do anything with my information.

To Marc's point, privacy policy is all well and good, unless you have someone with teeth like a Coopers & Lybrand backing up what you are saying and unless you actually give the end user control to access their information, then, you know, from a technology point of view, at least, we feel that's what OPS is striving to do, is to create a framework for a personalized network with privacy.

MR. MEDINE: To clarify, OPS isn't a technical standard, but it still totally depends on the Website's agreement to abide by any given set of privacy policies.

And a further question is will there be anything built into OPS to disclose to the consumer at the time they release the information to the Website, what the Website's policies are concerning secondary use?

MR. KLEIN: Absolutely. If we turn the clock back to the demonstration I gave, what I went to the site Launch, the box popped up saying this is what the site wants. Do you consent to this? I saw the eTRUST mark there, and having

done that, that transaction is then logged into my statement.

MR. MEDINE: I assume that's because the site chose to put its mark there. But by the same token it can simply say I want your information, period, and then you give it to them not knowing how they intend to use the information for subsequent use.

MR. KLEIN: There is a huge education issue here, both in terms of businesses and consumers. And our belief is that working with the major platform companies, having widespread support from OPS, we have obviously seen that even in a short span of time, the last two or three weeks, this has become a major talking point.

And we have seen major, major companies adopt some of these goals.

MR. HARTER: We mentioned from the Launch idea it is great to have. Going forward, once there is a standard promulgated, implementation of it by Websites is going to be an educational task, equally important, Websites that choose to comply or say they comply with OPS and other software that's technical standards.

Consumer protection and fraud laws that are on the books today will have to be evaluated. Can they be applied or is there some need for modification? I think that's another important topic for discussion. Probably that will

take place after this conference or this hearing.

MR. MEDINE: Could OPS be blended with P3 so you basically program in your privacy preferences and then in those situations where you have previously authorized release, OPS would provide for that release?

MS. MULLIGAN: I want to say two things. One from the very beginning when the Internet Privacy Working Group formed, and that was with participation from W3C, they had a staff person there, we initially decided to put any talk of data transfer, this automatic data transfer aside because we felt that before you talk about any data transfer, you had to talk about what are the behind-the-scene rules.

What is the notice? What are the information practices of the entity? How are they being disclosed? What type of control does the user have on the front end? Then you can start talking about whether or not I want to disclose information, but until you put that framework down, you shouldn't be having that discussion.

I think the good thing is that W3C is the place where this discussion is going to occur. And the underlying framework, the vocabulary and the P3 project, their specification, if the information is being moved about in a cookie, if it is using push technology, if it is in OPS, it doesn't matter that the rules apply to the data elements and so that it would govern it regardless. So I think they can

work together.

MR. BERNERS-LEE: Just to sort of reemphasize that point, OPS is being submitted to P3 and, you know, will be reviewed within the P3 working group of the World Wide Web Consortium.

So in terms of our confluence of efforts here, this is exactly what is going on, which is obviously why the organizations are working closely with the P3 and the IPWG and World Wide Web Consortium to bring this through.

MR. CATLETT: It is making sure the pieces of the puzzle will fit together well.

MR. HARTER: Would it be appropriate to give a footnote about the question this morning?

MR. MEDINE: Certainly.

MR. HARTER: Not only to Commissioner Varney and others raised that during the panel, but also another panelist, Jason from Junkbusters and a reporter from Consumers Reports, whose card I just lost, but I have his article here, it is Jeffrey Fox.

I called back to engineering on Netscape Mountain View to find out what exactly is happening in 4.0 of our product in terms of cookies that come from advertisers or third-party cookies. And as it turns out information I filed in our submitted filing last week and as I reviewed the four changes in cookies, we do give the user a choice to block

cookies from third parties.

There is a dialogue box you can pull down, indicate. If I am going to CNN.com I have a choice to reject cookies that come from other domains.

MR. MEDINE: You have different levels of choice, you can accept all cookies, accept cookies from the main domain you are going to, or reject cookies from third-party domains or reject everything?

MR. HARTER: Accept all, reject all, and then just take the domains I am going to.

MR. MEDINE: Okay.

MS. MULLIGAN: Can I add one more thing? In talking about how P3 would work and how the vocabulary would work that that third party, the person who is responsible for that ad banner, they would have a separate statement of information practices, so right now the problem is transparency, which you noted before, the individual doesn't realize they have opened a session with someone else, because they haven't gotten a notice of that, and that the P3 would respond to that because you would have to know if you were going someplace where there were different information practices, you were dealing with someone else.

MR. MEDINE: I appreciate that. Again, thank you very much for the demonstration. Our final speaker on this panel is Jason Catlett, CEO and founder of Junkbusters.

MR. CATLETT: These few months have seen enormous changes in privacy, and I am very honored to be with you here today. We have seen enormous changes in the past few months and I am very honored to be here with you today because it is clear people in this room and the organizations behind them are having an enormous effect on privacy in the 21st Century.

In 1993 the New York Magazine ran a famous line on the Internet: "Nobody knows you're a dog." In 1997, they not only know he is a dog, they know his name is Fido, they know he likes chasing cats and they know he eats Alpo. And he is wondering whether he should get off the Internet before too many people find out he is a dog.

What should Fido do? What should Fido's family do? Returning to this room, I think the one statement we have wide-spread consensus on today is that it would be a tragic loss of opportunity if people like Fido were to stay away from the Internet in droves because they fear for their privacy.

The main response we have heard today is that the people collecting information should disclose the practices and make them acceptable to the people disclosing that information. And the other main response is that government should intervene to legislate or regulate those practices.

There is a third response, and it comes not from companies or governments, but from people. People want to

ensure anonymity. Alan Westin told us 80 percent of them want it. My talk today is going to show some of those means, and specifically we will look at cookies and how cookies work, and how you can prevent cookies and how to prevent tracking that goes with them.

First, let me just ask how many people in this room have actually seen a cookie? Could you raise your hands if you have seen a cookie? I would say maybe 30, 40 percent of the people. Well, you are in for a tasty treat.

We are first going to look at the way advertisers collect the history of your Web browsing. Technology for doing this is now widespread. So rather than single out one real company, I have marked up a fictitious search called Bassa Vista. It looks like one of the search engines, but this isn't intended to encourage or discourage any particular search engine.

I have chosen this one for its simple and familiar interface. The ad company and some of the ads seen here are also fictitious.

Using a search engine is going to a Web page and typing in whatever words you are interested in, say, for example, privacy. The search engine returns a list of Web pages containing those words. You also get an advertisement. You may have noticed that the advertising is related to the words in your query.

Eric Johnson mentioned this in the previous session with automobiles. And you get something else, a cookie. The browser doesn't tell you that you got a cookie unless you change its configuration, as we are doing now. Most browsers used today won't automatically refuse all cookies.

Instead, each time the Web server serves a cookie to you, you are asked if you want to accept it. And there are sites that send maybe a dozen cookies a page and having to click 12 times is enough to wear down even the most ardent private enthusiast.

I am very glad Netscape has announced the next version will permit no third-party cookies. Let's see how this works now that we have set cookie alerts. Let's search for the word cookie. A dialogue box comes up indicating from Bassa Vista.com, shows you the cookie. And as with most of the billions of cookies served, this one is simply a unique identifying serial number for the transaction.

And if the browser accepts the cookie, then the next time you send a page to that, the requested page through that site, the browser will send the cookie to the Web server along with that page request.

The box also shows you the expiration date of the cookie. And in some cases it is the end of the 20th Century. Cookies can be made to last for years. I have seen one expiring in the year 2030. So this technology allows

advertisers to build up comprehensive long-term profiles of what consumers search for, which ads they click on, and which pages they view. We can reject this cookie by clicking on the cancel line.

Immediately a second dialogue box appears. And this dialogue box indicates that the cookie is coming not from Bassa Vista but from a Web advertiser called Banner Track.com -- also fictitious. This is what we call a third-party cookie. It comes from the advertiser, not from the search engine.

Most people aren't aware that their cookies are being sent by other parties. We are going to reject that cookie too.

Remember when we searched for privacy? The information that was logged into your profile contained the cookie serial number, and it is possible then for the advertiser to know that you are the same person who searched for this query today and another query before.

The profile that can be built up from assembling a time history of a person's searches can be very comprehensive and obtrusive. People who want to protect their privacy without having to constantly cancel cookies can use a program called proxies. One of the ones I am going to discuss today is called the Internet Junkbuster.

To use this, you simply tell your browser to send all

its requests to a proxy server, and it intermediates between the browser and the sites that the pages go to being requested from, and it removes the information that the Junkbuster is being told to police, such as those related to cookies or several other headers that people consider sensitive.

Let's see the cookie crunching in action. We search for the word junkbuster. We no longer get a dial-in box. The window behind the browser tells us that the junkbuster was scanning the headers here for the cookie, found it and crunched it. It didn't pass it on to the browser.

Examining the header information also reveals that the search engine is handing the specifics of your query over to the ad company. For most people simply stopping cookies will thwart tracking, but if your computer uses a static IP address, tracking is easy. Having a set IP address means everything you do on the Internet comes from the Web service, like the Internet address, it is like global caller ID.

The companies that access the Internet via the company's Intranet are usually assigned static IP addresses and the corporate users may not be aware that it makes them easy to track, even without cookies. So what can people who don't want the ad coming to get their search engine do? They have a couple of options. They can turn off the auto load images option, which effectively makes their Web browsing

text only. The ad company won't get to see the query because it won't be asked to serve an ad. It is a graphic. Unfortunately, this option makes it very difficult to navigate some sites. They are designed so that the graphic is needed to get around in.

What is wanted by the consumer here is the ability to block some graphics, while letting others through. This can be done by a filtering proxy, such as the Internet Junkbuster or any of several available on the Web today.

Junkbuster does this with a file called the block file. The block file contains the URL's that the user wants blocked by simply editing that file and adding the words "Bannertrack.com", no ad from Bannertrack will get through again.

The second mechanism is being used by parents for blocking sites they consider unsuitable for viewing by the children. When the page is displayed now, the ad is replaced with a broken icon indicating the browser can't get the URL that was requested. And we can see from the other window that the Internet Junkbuster blocked the URL.

The Internet Junkbuster allows you to block parts of a Website. The same mechanism is available for cookie management, so you can tell some trusted sites -- you can allow some trusted sites to set cookies but not anyone else.

The Internet Junkbuster is free. And several

thousand copies of it have been down-loaded from Junkbuster.com and several sites around the world. A UNIX version of it has been available for about four months. The Windows version is forthcoming, but we have not yet announced it.

Most people who use corporate or campus network browsers, don't have to down-load our software. They simply run through a single computer on the network that is running the software and that serves all users, whether they are using Windows or other operating systems and whether they are using Microsoft Internet Explorer or Netscape or another browser.

Companies and government departments also like our product because it has the same information that threatens consumers' privacy, also poses a threat to corporate confidentiality.

For example, I don't think the FTC staff would be happy if all of the queries that they had used for the past few years were made available in an inappropriate disclosure. The Internet Junkbuster proxies are also provided by ISP's in the United States, Europe and Asia as a free additional service to the customers.

Ms. Dyson's remarks this morning that ISP's will represent the customers at a grass roots level and use this kind of service as a differentiation point, I think, were

absolutely spot on.

The Internet Junkbuster is one of many proxy servers that are used for various goals in the areas of security, privacy, and efficiency on the Web. Just yesterday Lucent Technologies, the communications equipment company that's split off from AT&T, announced a new proxy called the Lucent Personalized Web Assistant or LPWA, which gives surfers a way to register at sites anonymously without having to do a lot of bookkeeping of passwords and so forth and without revealing to the site their real E-mail address.

There is a press release outside if you want to know more. As Saul pointed out today, the personalization is not dependent on identification, so this works with those.

To conclude, I think we can expect proxies such as the Internet Junkbuster to be adopted more and more as consumers take back their privacy by using technical means of assuring their anonymity.

If there is time for questions, I will be happy to answer.

MR. MEDINE: One question is you talk about static ID's, IP addresses. Isn't it the case that those who use commercial online services like AOL don't have static ID's and, therefore, basically if they are going on the Internet through one of these online services, at least it eliminates one of the concerns for tracking because their IP address is

not known?

MR. CATLETT: That's correct. It does not eliminate cookies. You have heard some other means or you can use the Internet Junkbuster if you want to have cookie management, allow some sites cookies but not others.

MR. MEDINE: Thank you. That was an excellent demonstration. You are making concrete the cookie discussion we have had throughout the day. We will take about a ten-minute break and reconvene with our roundtable.

(A brief recess was taken.)

ROUNDTABLE 2: PERSPECTIVES ON TECHNOLOGICAL APPROACHES

"Privacy advocates, consumer groups and government representatives discuss technological efforts."

JERRY BERMAN, Executive Director, Center for Democracy and Technology

LESLIE L. BYRNE, Director, U.S. Office of Consumer Affairs

MARY CULNAN, Commissioner, President's Commission on Critical Infrastructure Protection

JULIE DeFALCO, National Consumer Coalition

JEAN ANN FOX, Director of Consumer Protection, Consumer Federation of America

JEFFREY FOX, Consumers Union

JANLORI GOLDMAN, Visiting Scholar, Georgetown University Law Center

EVAN HENDRICKS, Editor/Publisher, Privacy Times

ERIC WENGER, Assistant Attorney General, New York

***

MR. MEDINE: Thank you very much. Anyone who is on this panel gets a medal for sticking through the whole day.

MS. GOLDMAN: I will take it.

MR. MEDINE: We also appreciate there may be some early departures as well, but we really do appreciate your sticking around to give your thoughts and feedback on what we have heard this afternoon.

This morning we had a chance to critique the state of self-regulation and now we have a chance to comment on the state of technology. So as before I will turn it over to the panel members for their views on what we have heard this afternoon.

Does it answer all privacy questions that anyone has? Should we go home tonight and rest assured that privacy is going to be protected or not?

Jeff.

MR. FOX: I wanted to just comment on the P3 proposal and, of course, I don't want to be a grouch, but I have a criticism to make about it.

First, I want to say that I think it is definitely a move forward. And I think for protecting children it looks as if it will be a far superior technological solution than blocking software, which I will be talking about more on Friday, but the reaction I have is that there was something about this that was -- the P3 system was still biased in some way against the consumer.

And what I thought as I was listening to the talk about negotiation was that if I go to a car dealer and I say, you know, I will give you $20,000 and he says 25, I am not budging, that's not a negotiation. Negotiation involves both sides. And this doesn't sound like that. It sounds like it is a chance to negotiate away your privacy rights.

But from the description of it, it didn't sound as if there was any provision in this for the Website to make a counteroffer. What is wrong with that? I know there are auctions on the Web now. I know someone who has submitted multiple bids where if one bid isn't good enough, another bid will automatically be submitted. I don't see any reason why the Website can't provide for an override of our normal policy, we will swap you an E-mail address if you don't want to give your name or something.

DEIRDRE MULLIGAN: Can I respond to that as the person who is in charge of that?

MR. MEDINE: Since not everyone who presented this afternoon has a chance to come here and respond, I would like this panel to express their concerns and have Deirdre, who is here as a privacy advocate, not as a defender of P3, because I don't think it would be fair to whose who aren't, we would have to add them back on the panel again. Let's try to see that they have a chance to present their thing.

As I have indicated at the beginning of the session, the record will be open through at least July 14th. People will have plenty of opportunity to submit responses on the public record.

MR. FOX: Another point is that, as I mentioned to Deirdre, I think that the system should provide for the consumer to tell the site why they object to the policies or

why they are leaving the site. I don't think we have an equal power relationship here.

We have a large number of isolated individuals and a large fairly well-off sophisticated company. And I think that something -- some provisions need to be made to balance the power equation somewhat more.

Also, as sort of a concern about if more and more basic services become established on the Web where it becomes an essential service, if you want to buy something or do certain kinds of things you have to go on the Web, if some of these privacy policies are put up there on a take-it-or-leave-it basis, people are going to have to buy away their privacy and they are going to feel compelled, especially in the case of children where everybody on the block except Johnny has seen this game. He says: Mommy, you know, I have to see that game. What do you say to your kids? Parents are frequently caving in when the kid has to have something.

So I think there are risks here of forcing, in a sense almost compelling people to negotiate away their privacy rights.

MR. MEDINE: Do you think that's much different from the off-line world? You go to a credit card company, do you have an ability to negotiate your privacy rights in that context or a merchant, do you think, is there maybe online

more opportunity for dialogue rather than less?

MR. FOX: Recently I went to a Sports Authority store to buy something, and they just instituted a digital signature system. And they asked me to sign this LCD kind of thing where they would record my signature for a credit card transaction, and I said I don't really want to do that.

This was the first day they had that system live. And they kind of huddled with the manager. And they came back and processed it the normal way. So in some cases you can and you ought to stand up for yourself.

MR. MEDINE: Adding the human factor for computers to allow them to respond electronically to your privacy requests. Eric Wenger for the attorneys general office.

MR. WENGER: I am here not as an assistant attorney general of the New York Department of Law, but as chair of the Privacy Subcommittee for the National Association of Attorneys General Internet Working Group. Paradoxically my views don't represent either one of those.

It has become clear from the hearing last year and also from the demonstrations that we have had today that there is a profit motive that is developing toward -- which equates incentives for companies to have stronger privacy policies.

We see that some of the things that were sort of implicit in the past, you know, a tradeoff of information for

services is becoming a little more explicit. Companies like Cyber Gold that pay people to look at advertisements and for their reactions to those advertisements.

In addition, I think the interesting point about the story that Shirley told this morning about Juno Online Services was that when we approached them and said to them we want you to accurately disclose what you are going to do with the information, they realized that the value of the data was less than the value of their reputation, as somebody who upheld privacy policies or upheld people's privacy interests, and so what they did was they explicitly changed their service agreement to make sure that consumers had the privacy rights that we were alleging they had advertised.

So that to me was a concrete demonstration of the fact that a strong privacy policy had a value to them. We saw from the surveys conducted by BCG and Harris and others that when consumers don't understand how the information is going to be used, that there is an incentive for them to either avoid giving the information or outright lie.

And we see from the -- I am glad that there was the demonstration or just the mention at least of the Lucent Technologies software that was just introduced that will allow consumers to create fake identities when they are asked to log into a site and register.

I think that that also makes it clear that if

industry does not take steps to make consumers feel comfortable about how the information is going to be used, then there will be low-tech solutions, like people avoiding giving information, and there will be high-tech solutions where, you know, some application of the cookie technology is used to create false identities and then give that information back to the companies, which would make it really useless to try to collect information in the first place.

I think that the McGraw-Hill policy that was laid out this morning is laudable. And it would be very close to my idea of what a basic policy of privacy should include. And I think that another concept that should be lauded is the P3 concept that was demonstrated here today.

At last year's hearing there was some discussion about how the PICS standard could be used and adapted to help set a standard for exchanging privacy preferences between end users and Websites, and that was just an idea for a new application of a concept then. Now it is a full-blown concept of its own.

But, I mean, it is a concept and that needs to be developed. And it needs to be adopted. And that's really the rub here; we have a lot of really great ideas but how do we get them to be implemented across the board so that they are accepted and useful and have meaning to both the businesses and, importantly, to the consumers so they feel

comfortable?

I think we all sort of agreed that it is important for consumers to have notice about the information collected from them, an opportunity to perhaps opt-out of the databases, access to the information that's collected about them, and a real opportunity to correct incorrect information and security, but unless we have some sort of base line standards that are out there and a real way to make sure that everybody is providing this sort of information to consumers, then it is not really meaningful.

And that's where I think there can be a role for government, for the FTC and for the states, to not only help to enforce the voluntary standards that are created but also to, in forums like this, help to provide incentives for industry to step up to the plate and create standards and where those standards don't work because there are parties that are not subject to self-regulation, help set base line standards perhaps for regulation or legislation, and I think that limited targeted regulations can in some instances provide the base line upon which the market incentives for strong privacy policies can take off. And that's what I would like to see happen.

MR. MEDINE: Jan Fox.

MS. FOX: Thank you. All of this is very impressive. I am not sure I understand how it works or what

all it does, but I would come back to the central idea that technology is a tool but it is not a fix. This is a public policy debate. This is a policy decision on how to protect consumers in a new marketplace.

And technology can be used to accomplish that, but we shouldn't say: Oh, well, there are ways to do this, we don't have to worry about it.

None of the self-regulatory proposals that have been described today obviate the need for enforceable privacy protections that are implemented by the Federal Trade Commission or by the states, but that apply to everyone in the market, not just the top of the market that chooses to step forward and voluntarily try to improve things.

I still want to repeat my central theme, which is that technology can be used to design systems where consumers give affirmative permission to have information that's identifiable to them collected and used. You don't have to design your technology to the lower level of simply allowing people to opt-out.

In looking at the description of setting up profiles where you put in your information, it is a little counterintuitive to me that you could protect your privacy by giving up more information. I don't quite understand how that works.

And I also would like to just mention a point that

you will discuss tomorrow, but since I wasn't invited tomorrow, I will go ahead and go on it for about a minute. I am not sure how all of this, all of this voluntary improvement of things is going to apply to the ad writers who flood people's E-mail boxes with scurrilous ads and inflammatory information and racey pictures that any child can see whenever you log on to the E-mail.

I am sure that the industry sees themselves in very separate compartments with the Internet service providers and the World Wide Web publishers, and the industry sees itself in distinct pieces. For a lot of consumers you turn on the computer, you log on through the telephone line, and it is all cyberspace.

So you are going to have to figure out how to solve the problem of the unsolicited commercial E-mail. I recommend just banning it.

MR. MEDINE: That would certainly be one of the things we will be discussing tomorrow. To follow up on your point, I take it what you are saying is that the technology we have seen today is very useful, but it seems as though all the technology we saw demonstrated requires a commitment on the part of the Websites and other users of information to abide by certain set of standards?

And what I think you are saying is that those standards have to be ingrained in law to make sure not only

the upper end of industry follows them but also make sure everybody follows them? Is that a fair summary?

MS. FOX: Yes.

MR. MEDINE: Other comments?

MR. ROTENBERG: Dave?

MR. MEDINE: Marc Rotenberg.

MR. ROTENBERG: Let me say first that I saw this discussion coming. And last year at this time when you did the hearings on consumer privacy and there was some discussion about technologies to protect privacy, I tried to sort of provide some guideposts for how that discussion might go.

And I said you really have to be very careful when you talk about how technology is used to protect privacy, not only technology necessarily protects privacy, just as not only technology necessarily destroys privacy, but you can distinguish, I think, between what are commonly called now privacy enhancing technologies or privacy enhancing techniques and privacy extracting techniques.

I put a great deal of emphasis in my presentation on anonymity because I think it is the core of privacy enhancing technologies.

It is widespread in our everyday world. Metro cards, copy cards, cash, 80 percent of consumer transactions in the United States are -- they are not user identified. You don't

provide a $20 bill with your serial number on it. And telephone cards, which are used in the U.S. but also in many other countries are all anonymous. Those are all privacy enhancing techniques.

And encryption, as a general matter, though not in all implementations, of course, can be a privacy enhancing technique. I share Jean Ann's concern that what we are looking at today are largely privacy extracting techniques.

These are techniques which take information from you as a condition of engaging in the marketplace -- and I think Jeff also made this point well. I don't see why we need to enter into that type of negotiation. I have good money. I will pay for products. I want the convenience of a credit card. I will use it, but a credit card transaction doesn't give the merchant the right to visit me.

And so today in our world we do not rely on these types of techniques that require individuals to give up personal information, so I think we really have to look at these proposals quite skeptically because the other thing that I did not see today is what will happen with the information once it is gathered.

I heard about auditing. I heard about contract. I heard some suggestion that maybe the FTC would have some authority to enforce if there was misrepresentation. I would like to see some of those mechanisms actually work. Because,

of course, we are talking about new consumer relations that have never previously existed. And we don't know if any of those mechanisms work. So we have to look very closely.

MR. MEDINE: Evan Hendricks, Privacy Times.

MR. HENDRICKS: I am echoing those comments. There is a real danger in these things that are done in the name of privacy that get you to disclose information about yourself, though I see how they could work as designed and intended, and if they were in a legal framework they do really have some potential, but without a legal framework you can envision a scenario where people are given a false sense of security and there is this danger you could be convinced or conned into disclosing information about yourself in a situation where ultimately there is no protection for it.

What if Firefly, which is now working with some major companies, they like them, they buy them out and they want to use that information to sell it? There is not much the individual can do about that. There is TransUnion, which used to be a credit bureau, and then they went into -- they were sitting on a gold mine, went into the business of selling lists in the direct marketing world, and that's something the FTC knows all about. So these sort of things are very real scenarios.

I think that Firefly offered a good standard, and I want to see the FTC establish a standard in the sense that

one of the things they said is that they don't sell or disclose, that is, information without consent. And that's -- there is an industry representative that lives with that standard, and I think that's a good fairness standard to start with on the Web.

Now, another thing that's going on is who is not here? We heard a little bit about the Adfinity program, which talks about taking Web activity and going to direct marketing databases, so you can overlay that against people's Web browsing.

They mention two companies, Websites that use it. One is called EDrive, one is called Motley Fool. I went to both of those and found no mention of a privacy policy, much less if you visit the site and register, they are going to be going in and looking at your demographics and things like that.

I think that many things the FTC can do here, one I think is to extend the rights of access to those groups that you talked about yesterday, the whole public records. I think that to the extent you can establish informed consent standards based on what Firefly said, that's something you can move aggressively to do. And I think also you have a duty to look at the legislation that is already pending in Congress, the Feinstein-Grassley-Klezcka bill on credit headers, the Vento bill for ISP's, the Franks bill, kids off

lists.

Those cover some of the areas covered in this hearing and you should be endorsing those bills, I think. And I also think we have to put our egos aside here and take a step back and look at what is needed from an infrastructure point of view.

I am not adequate to protect privacy, as highly as I might think of myself. I can't jet the job done. The Federal Trade Commission has done more than anybody to advance this issue, and I commend you for that, but you can see how big this issue is just from the two days of the four days of hearings you have had.

I think you need to recommend that we have what every other country has, that's an office dedicated to these issues, because that's how important they are and they work well in other countries.

The other -- I will close with saying this. We talked about -- we heard a lot of the things, Leslie Byrne mentioned this, a year from now, a year from now we might have this, a year from now we might have that. There is one DMA member that I think I wish he were here to testify for himself, but I would like to read a two-sentence quote here from him, Robert Posh.

And he is apparently very outspoken in direct marketing circles, but he says, "In two years technology will

have moved beyond the recall of the privacy types. All privacy attacks will be upon an information industry too big to be defeated and thwarted from the historical inevitability of a new society built on this new economy. Our opponents' arguments will be so irrelevant that they will be ignored. We are winning and shall continue to do so."

That's why I think you can't afford to wait a year on this stuff. I think the time to move is now.

MR. MEDINE: Janlori Goldman, Georgetown University Law School.

MS. GOLDMAN: I want to make a couple of quick points. When you first started this process you, the FTC, a number of years ago, we came in and talked about privacy enhancing technologies and said we don't know what they are yet, we don't know what they are going to look like and how we are going to work but we need to press to have this developed and work in concert.

I think today you have heard a number of people show they are doing that. And it is important and it is exciting and it is the first true opportunity that we have to give people some real front-end control over personal information when they use the Web.

I think what we need to do and what this process should continue to do is what you started out doing, which was to look at that as a piece of protecting privacy and a

new piece and an important piece for giving people a chance to have real control in a situation where they never have before.

But the other pieces are still important. Where the privacy enhancing technologies give people opportunities, they also create burdens. We have heard about some of those burdens.

I think that some of the discussions today have suggested that with some of these technologies, with some of these opportunities people are going to be asked to use their privacy as a chit to get access to certain sites and to get certain benefits. And that's the real danger here, particularly when you are talking about access to critical services, health services, for instance, which we are not finding in great numbers right now on the Web, but I think you will as people are moving more and more towards tele-medicine and that we should not see this as an answer.

We will just create a negotiation, we will just create a way to have the information exchanged. If we know what you want and we can work something out, then you can proceed.

I think we still do need to have some hard and fast rules that are a back-drop, and the privacy enhancing technologies then are a way to apply some of those rules.

Some other comments that were made today that give me

concern when I hear talk about cost and burden have to do with people who say: Well, it costs money for us to protect privacy. There are going to be costs for us associated with preserving privacy on the Net. And that may be true, but it is really important to try to quantify, as hard as that is, the cost of not protecting privacy.

And most of the companies and organizations that have worked to develop privacy enhancing technologies do acknowledge that there is a cost to not protecting privacy, but I think that will be the minority. There will be a number of folks who will need to be persuaded, and maybe with a strong arm, that the costs of not protecting privacy may be greater, even if it is not great to that particular company, that there are societal costs that need to be factored in.

The other comment is that in some of the survey results that were talked about today there was discussion about not trusting in government solutions. And I want to just suggest we put that in a little bit of context, that right now most people in this country don't trust government solutions for a wide variety of problems, but that doesn't mean that we should abandon them and say they are ineffective.

The privacy laws that we have on the books right now might not be very effective and in some places they don't even exist at all, but that is certainly not, I think, a good

justification to abandon the role of government in this process.

And the last point that I want to make is that, and we say this in the paper that is made available in the NTIA papers on self-regulation, there have been a number of instances, critical instances where people in this room actively sought legislative protection through a privacy law where industry said we need a law to bind us, to bind other private sector actors, and the government in terms of getting access to personal information.

The Electronic Communications privacy Act was an example of where industry and public interest groups got together and said to Congress: We want a law and here is a good outline of what we think it should look like. Or take the Video Privacy Protection Act. We need a law to make sure people will continue to rent videos or use electronic communications because there was a serious problem with trust and confidence on the part of the public.

So I want to suggest that we not always pose this as a conflict that has to be reconciled between industry saying we want self-regulation and only self-regulation that is going to work, this is a nascent industry, please don't regulate us. The electronic communications industry was nascent at the time, the video industry was nascent at the time, but in order for it to succeed, those industries and

those affected groups said: We will not succeed without a law giving the public confidence in these services, giving the public some assurance that even if the technology is not 100 percent secure -- and no technology is going to be -- there will be laws and enforcement mechanisms backing up the policy.

And I suggest that we may at some point, maybe a year from now, end up with many of the same groups saying please don't regulate us, that will be a disaster, we will be put out of business, coming back and saying without some kind of enforceable regulation and national policy, we won't be able to succeed.

MR. MEDINE: Thank you.

COMMISSIONER STAREK: May I follow up, David?

MR. MEDINE: Absolutely.

COMMISSIONER STAREK: I thought those comments were particularly insightful, but let me see if maybe -- the way I see this coming down is that if companies will offer consumers at some point, you know, Websites are going to offer consumers a choice, you can either provide us with some information to have access to our Website or you can pay for it, and I think, you know, consumers might, maybe that's not a fair choice, but that's the way I foresee it.

Is that the way you foresee what is happening? Unless people begin to realize what Eric so ably laid out

here, which is most people who are doing business legitimately are going to realize that their reputation is what is important to them, and if their reputation means protecting consumers' privacy, that they will do it? We are talking about legitimate marketers here now.

MS. GOLDMAN: I think your point is really right. It is something we talked about a little bit earlier, which is that those reputable businesses who do have a stake in their good name will be the ones who do the right thing. They are the ones sitting in this room. They are the ones saying we are trying to do the right thing for privacy. They are not the ones I am necessarily as concerned about.

I would be very worried and I have been strongly opposed to any kind of a policy that allows people to pay to protect their privacy or suggest that those who can pay get greater protection because then you create a situation where there are the privacy have's, the privacy have not's.

I think we should treat this as a basic right and create a certain minimum level of protection. Then there are probably situations where people can, with greater means, have more privacy protection. I think that's just inevitable. It is the way the First Amendment works right now. Everyone supposedly gets a certain amount of access to the microphone and then after that you certainly have to pay a little bit more to have a greater audience.

The Internet obviously obviates some of that concern, but I would be very resistant to any kind of a structure that said you pay a little extra, you have greater privacy. The person from the New York Times said anonymity is not always a good thing. We like to know who is registering, who is coming on to our site for people who are participating in forums. Well, when I go to The New York Times site, I don't participate in any forums. So there has to be a way to make a really rational distinction between when there is a necessity for personal information and when there is not.

And in terms of the costs, people are going to try to offset costs by charging users, but that shouldn't necessarily be tied to privacy.

MR. HENDRICKS: Can I briefly respond to that? I think that is such an important question. What I think is going to happen is that Websites -- and if you look in the trade journals, you will see everything is designed at tracking information and tying it to the individual on these Websites.

What I think is going to happen is that Websites are going to continue to try and collect as much personal information, maybe like the grocery stores, not knowing what they want to do with it but they are going to collect it until they can figure out what to do about it. There won't be an understanding from the person about this information

being collected, and that's why problems develop later.

Eventually they will decide what to do with it. People won't like it, or it will get misused in some ways. There is no question there is a big thrust -- we can provide information for the record -- a big thrust to collect personalized information. And that's why I am afraid disasters are coming unless we can set rules for the road.

MR. MEDINE: Let me turn the payment question around to Janlori. How do you feel about being paid for your personal information, paid extra to protect your -- basically paid to give up your privacy?

MS. GOLDMAN: I think it is the same issue. You pose it that way and, of course, it is very enticing. Pay me to give up my privacy and, in fact, that's what most people do. And that's the conundrum.

I go to the grocery store, I want to use my frequent shopper card if I am going to get a discount. I want to use my frequent flyer card if I am going to get miles. And people constantly are giving up privacy in order to receive a benefit.

Where I think it is very troublesome is where there is not real choice. I think that in the health area, which is an area I have spent many years focused on, there is no choice. There is no meaningful choice there.

People are not able to -- this is where people pay

extra to protect privacy. They pay out of pocket. They go outside of plan and don't submit a claim for treatment they are otherwise entitled to be reimbursed for. That's where people right now are doing it, but people who can afford that are doing it. And I don't think that that's the right answer.

What we need to do is to say you can't condition the delivery of benefits and services on getting that consent, fortunately. People should be able to voluntarily, knowingly, in a meaningful way consent to giving information, otherwise it is not privacy, it is not about privacy, it is about that negotiation, it is about trading your privacy for some kind of a benefit. And I don't think that's the right way to set it up.

MR. MEDINE: Mary Culnan?

MS. CULNAN: I am going to change the subject and also try to be very brief because I know the hour is getting late and there are other people who want to speak. I thought the technology demonstrations were fascinating, but they struck me also as being very complex for the average person to use.

I even consider myself, I am not -- I can surf the Web but I never know what to do about helper applications and doing all this stuff is going to be beyond a lot of people's level of tolerance. But I think for some people they are

going to be terrific, and I hope they will move forward because I think it is definitely an interesting, one interesting solution.

But I think we are really not very far along the road, and we ought to go back to the basics. And I think what ought to be a top priority is the EPIC survey showed basically if those results extended all -- my guess is that they might apply to the Fortune 500 or random sample of people in the Direct Marketing Association, is basically back, first of all, to disclosure.

If we can come back in a year and could do a survey of the top 100 sites and everybody had good notice on their home page or a link, I would consider that to be great progress, but we also need some work on what is good disclosure.

Evan raised the point about in your Website information, they don't ask you for very much, but then they overlay it from a lot of other commercial databases. Shouldn't you know about that if the disclosure is going to be full and fair? What if you get something that says we do share information but we only share it occasionally with carefully selected firms? What does occasionally really mean? And what does carefully selected firms mean?

If you put people's names in a co-op database or something like that, it is kind of up for grabs for anybody

who has the money. People ought to know that, what these terms mean.

And then I think also one of the things that was missing from this morning's discussion, there seems to be a lot of agreement on notice, but on the accountability side; that is, are people really doing what they say they are doing, and so I think to come back next year and have a report, in fact, is there notice? Are people playing by the rules? What is good notice? That would be an enormous step forward.

So I would say to the FTC keep the heat on. Clearly you have gotten people's attention and I know you will keep talking to the businesspeople throughout the year and see what they are up to, but I think it is too soon for regulation now. I think give people a chance.

Plus, unless especially if it is regulation that says the label has to go here or the notice has to go here and just the second, the discussion right after lunch about does it come with the ad, does it go here, I think this is way too complicated when people don't have notice at all. So I think let's get some notices out there and then see what is what and keep an eye out for the bad apples.

MR. MEDINE: Leslie Byrne, is it enough to keep the heat on? Have you seen enough today to feel that we are on the right track and government should stay its hand?

MS. BYRNE: I am a Web surfer and I enjoy it. And what today's demonstrations showed me is that we are in an information arms race. We have got those who want, as Marc pointed out, those who want to extract information and those who have techniques to protect the information.

And as this arms race continues, Janlori brought up the fact that it is going to create an unfairness. Only those people who can devote either time or money or have the knowledge to protect themselves are going to be able to do it.

Several of the companies that presented themselves today talked about the technology platform and using these different techniques as implementing tools for public policy. I think that's an important thing. And Jean Ann put her finger on it. This affords us a tool to implement public policy.

I mean, it is great stuff, hooray, but we still should say: Do citizens of this country deserve notice? Yes. Do they deserve disclosure? Yes. Do they deserve choice? Yes. Do they deserve access to their information? Yes.

In that context, we can have all the technology walk through the door, but somebody has to set the base line of what is expected in this country to protect the citizens' privacy.

And just to flip this on its other side, if these software companies that came in today were asked to give up their proprietary information, they would go nuts. If we asked the same information of these companies and Congress is passing laws and the government is all involved in protecting proprietary information for businesses. Well, that's good. But shouldn't the average citizen be afforded the same level of protection as the software companies that we saw today?

MR. MEDINE: Deirdre, wearing your CDT hat.

MS. MULLIGAN: Staying off the topic of what you should do and saying what the technology does or doesn't do. I just want to start with Marc's survey. I thought it was very revealing in the fact that there was a lack of policies, but also in the fact that I think you said that there were a lot of sites that actually aren't collecting data, it was like 51 percent aren't collecting identifiable data.

And I think that some of the surveys yesterday also showed there were a lot of sites that are information sites, they are not service sites, and that as we transition from an Internet and a World Wide Web that are basically information based, where people are going to find out what is going on, to an Internet and a Web where people are going to get services, such as their Social Security information, PEEBS information, or other things that anonymity and tools that protect anonymity are not going to be the whole picture

because they are going to be instances that people are going to want to be able to give information because this infrastructure is going to be our telephone, it is going to be a lot of other things.

And so I think that probably the most interesting thing that technology is doing right now is if you listen to Saul Klein talk about Firefly, I think that there are a lot of things that you can do with data that can meet the goals of people who want to figure out how to do better things on their Website, or if you are the census, figure out, you know, what the population is doing, or if you are the health care industry, figure out where the underserved populations are, if you are the Public Health Department, that don't interfere with personal privacy.

And in actuality some of the technological applications can help us parse through that. And there has been some actual interesting work done kind of theoretically talking about, you know, where do we get to the privacy issue? And where are we talking about data that might be useful for other purposes that doesn't have to raise these issues?

And I think some of the technological applications can actually get us to some of those places.

I think the technology, as Jean Ann said, is a tool. And I think probably the most encouraging thing that I can

say right now at this point is that I actually feel, unlike Evan, what he read from the publication, Robert Posh, was saying is that I actually feel like the war for technology, I actually feel like there is finally a battle, that technology used to be in the hands only of corporations or only of the government and I was merely a victim.

And I actually feel like there is the potential here right now to take some of that technology back and use it in kind of some fairly subversive ways. The idea that I can actually walk in to a Website and say these are my privacy policies right here, and, yeah, we certainly have to set up guidelines about what can be negotiated, Janlori and I have both very affirmatively said that I don't think people should be asked to pay for their information, and I don't think anybody should be trying to buy my information.

Poor people have too little privacy as it is. But I think that actually -- we had this woman from CEI talking about a market, there is no market, there is no information, there is no bargaining power. There are a whole bunch of marketplace problems, but I think that we are at least for the first time talking, using technology to say, okay, this is what we can do, as Evan said, we can shine some light, we can start a process, and let's see where the technology can take us.

But I don't think it is a full solution, but I think

that's what it does.

MR. MEDINE: Thanks. Maya Bernstein.

MS. BERNSTEIN: I want to echo some of what each of you said and answer from my perspective the question that you asked Leslie Byrne. I am sort of one of the civil servants who is going to be among many others in the position of advising policy officials about what they should do next.

And I am very encouraged, as Deirdre was just saying, about some of the technologies we have heard and I think that the methods that we have seen go a long way to promote the privacy principles that the Information Infrastructure Task Force came out with in June of 1995.

They promote notice and choice and consent, access, security, but I think that what I -- the feeling I got during the day is that we are a little light on accountability. That's something Mary said as well.

And that's troublesome to me because that's the place where we are getting the most complaints from consumers. We are hearing that as the main concern of the Europeans when we are in talks with them. And we really need to hear more about that particular issue because it seems to be the one that's highest on the minds of the folks, that we are going to have to be responding to in the next, say, year and a half as the European Union Directive comes into focus and for other reasons.

I think that in particular in the consent and anonymity and such, that there needs to be more in terms of accountability or we are just going to refuse to do business with you. That's not very much of a choice. And like Janlori said, in the medical context, that's it, either you do business with us or you don't. There is not really any negotiation there at all. And I think that's the case in a lot of places.

We are also being pressed not to regulate industry at this time and most are being pressed by the people in this room or who were in this room today, those of us hangers-on, and as others have said, they are really the high end of the industry, the responsible members of the industry, and the challenge for us is to, and for industry also, is to figure out how to get everybody else who is not in this room to step up to the plate as well or to join in or to, you know, become converts to the cause, whatever it is.

We need to know how to make that happen. We need advice from the people in this room about how to get those other folks who are not in this room to participate. And maybe one of the things we need to know is what the people in this room are willing to live with in order to get the rest of the industry on board.

How much minimal or what is the level of regulation, if you want to call it that, or government intrusion into the

process that you are willing to live with in order to get the rest of the industry on board so there is some minimum standard for privacy?

Maybe that's the way we sell, we need maybe a little bit of regulation but not so much more. I mean, we are not really that excited about going out and regulating a whole new industry.

On the other hand, we are getting a lot of pressure from various corners to do so. So, finally, I guess it is another plug to please tell us what you think, to respond to the options paper by June 27th.

And also I actually have a few extra copies on the off chance that some of you have not seen it yet. Thank you very much for allowing us to participate in this.

MR. MEDINE: Julie DeFalco, National Consumer Coalition.

MS. DeFALCO: Great timing, thanks. I think what is very apparent right now is that privacy is sort of like a Rorschach ink blot, and it is pretty much whatever the person talking about it is projecting onto it.

I think basically what we are talking about here is the philosophical difference on the role of government and people's relationships to government and to businesses. And I can probably say for sure I disagree with pretty much everyone on this panel about that.

We have been talking about -- so I will go on with my five points. We have been talking about choice and part of choice is the right to contract. Negotiating privacy is like anything else. So if like the auto dealer industry, if you don't like the fact that the person trying to sell you a car won't sell it to you for less than $25,000, then you can go somewhere else.

And it is like that with anything. And if Ms. Mulligan doesn't think the Internet is a market, I don't know what else it is. Just because the government is not really involved in it doesn't mean it is not a market.

MS. MULLIGAN: You don't know that you don't have the information that they are asking you for $25,000.

MS. DeFALCO: I was talking about cars.

MS. MULLIGAN: The point is you know that they are asking you for $25,000. On the Internet if somebody asks you for your name, you have no idea what they are doing with your name. You need information on which to make that decision, and you don't have the information.

MS. DeFALCO: I agree. I was just getting to that point. My next point was I think it is a good idea, I think that all these notice and choice and access and all the stuff, it is a really good idea. I am not clear on why there has to be a single base line standard.

Historically many systems can coexist

simultaneously. Currency exists simultaneously, different currencies. And we can see with the European Union that it has been kind of a hassle getting one single currency over the different national currencies. The metric system versus English. Electric outlets are different here than Europe. Even state and local governments' laws you can say compete with each other for customers that are citizens, so I think saying there has to be one single base line that everybody has to do is -- because maybe it is not the best idea and maybe you pick the winner but maybe you don't. Maybe you are forgoing a better option.

Finally, I think you should be wary of large companies asking to be regulated. Generally I think that signals something quite different to me. And I think that if the large companies would probably be best trying to weed out the bad actors by applying pressure on their own. Calling for government regulation does not -- I think that people here keep talking about how there is a market failure, although if there is no market, I don't know how there can be a failure, but government can fail too.

And I think that I agree with Ms. Culnan that there should be time before the government tries to get involved, lest there be a government failure.

Thank you very much for letting me participate.

MR. WENGER: Can I ask a question? I am just sort of

curious as to --

MR. ROTENBERG: What the National Consumer Coalition is?

MR. WENGER: No, you can ask that. If you are saying that -- how do you expect the large companies to apply any sort of pressure to smaller companies that are not members of any sort of industry associations? I am curious as to that.

MS. DeFALCO: I don't know. I was thinking about it at lunch today. I think that would be one thing, of course. I like the idea of TRUSTe, I like these ideas, and I think that these are a really good way to go.

And I think there is actually a very large opportunity for marketing for the people developing these different proposals, although I don't know how they would find their customers if they don't collect information on them, but that would be one way to establish the credible standard, credible third party in that sort of thing. I haven't really thought it through. I will think about it tonight.

MR. WENGER: There is clearly an incentive for large companies who have public images to protect the image. And the question is when you have the Internet and it is possible not only for consumers to be anonymous but for businesses to be anonymous and change their identities daily, how is it possible for an industry association to reach those

companies?

MS. DeFALCO: How is it possible for the U.S. Government to reach industries that are in China, for example, and Russia? I mean, there has to be another way to look at this besides passing laws. People will just move offshore.

MR. WENGER: When I have companies that are doing business out of New York or affecting New York consumers, then I can explore the reaches of my constitutional jurisdiction, and that's an area that I try, I can try to reach out and protect.

And the industry associations can try to reach out and exert pressure on people who have a public image that they are concerned about, but I just still don't understand how an industry association is going to exert any sort of power over a company, a small company that has no interest in what the public thinks of them. Especially where we have transparent companies that consumers don't deal with.

MS. DeFALCO: If you have the wayward actor company selling, say, widgets, and they do something that makes somebody angry and you want to sue them, either they would be disobeying a law that's probably already on the books in terms of fraud, in which case you can sue them, or they would not be in this country.

And if they were that illegal, they would probably be

somewhere -- my point is basically that it is nice to pass a law, but with the global nature of the Internet, as people have been saying, it is going to be pretty hard to enforce the law. So it is better to go for these nonlegal standards.

MR. WENGER: The medium may be global. However, the consumers and businesses may be located here in the United States. And to the extent they are, then they are going to be, if they are marketing goods and services, just because they are marketing over the medium, doesn't mean they are going to be exempt.

MS. DeFALCO: Right. If you are selling widgets in New York state and you are doing something that's illegal and I want to sue them, then I can do that already, can't I?

MR. MEDINE: I am not sure we are going to resolve this, but I think we have each had a chance to state our views. Let's close out with Mike Nelson.

MR. NELSON: Thank you, David. Thank you for the invitation to be here. I found this a very, very interesting, stimulating day.

I said earlier, just before lunch, that I was a technological optimist. And after this afternoon I think I am even more so. The demos we have seen have indicated that there are some very ingenious solutions to some of the problems that are out there.

We have identified some that have not been solved. I think Evan's point about the question of future uses of data is a very important one. What happens when a company is bought out, changes ownership, suddenly decides to change policy? There are some interesting questions there.

There are interesting questions about electronic money, about digital signatures, about anonymity and when it should and when it should not be applied. But I think for some of the fundamental questions that consumers have, we have technological solutions. We have seen some very exciting ways to address the problems.

And I think I would emphasize that these solutions do not need to be used by everyone. They don't even need to be used by more than 5 or 10 percent of the Internet users to have a huge impact. The V-chip, which has gotten a lot of attention lately, will never be used by most families, but the fact that five or ten or 20 percent of homes will have a V-chip in their television and that often those homes will be the most affluent and best educated homes means that there will be pressure on broadcasters to broadcast certain types of programming.

Likewise, if these technologies are used by a large number of people, but not a majority of Internet users, it will have a real pressure on Website providers to have effective transparent useful privacy policies. So I think we

can make a lot of progress here.

For me the most important thing about these demos is that it allows consumer to set their own policy. Government doesn't need to set it for them. They set their own policy. And the second most important thing is that they have the ability to know how their information is being used.

The magic of a small town, where there is no privacy, is the fact that you know what everybody else knows about you. So there is a balance of power, as was indicated earlier, and I think this technology does lead to that. It allows you to track where your information goes and to know how policies are being implemented.

I contrast this meeting to a meeting I went to in March in Monaco. And I spent three days at a UNESCO meeting on info ethics. One day was devoted to privacy.

MS. SARNA: It sounds like a tough life. Somebody has to do it.

MR. NELSON: It was a tough assignment. One day was devoted to privacy and problems of protecting privacy in cyberspace, and it was so different from this meeting.

At that meeting we had speaker after speaker giving what-if scenarios, talking about the problems. Many of them had never used the Internet but they feared what would happen if they did.

The only people providing any solutions to these

problems were the two or three U.S. speakers. And for the most part there didn't seem to be too much excitement about the solutions, much more interest in the problems.

Today we have heard a lot about solutions, and I think that's really exciting. I think the difference is really the difference between the U.S. approach where government asks the question do we really have to regulate this? And the European approach where the question is: Well, we are going to regulate it, give us a good reason why we shouldn't.

It is a very different approach and ours is obviously the better approach in this area because we are moving forward on lots of different tracks, providing lots of experiments.

Industry can move faster than government, but most importantly industry can develop lots of different approaches. And then government can step in where appropriate to back up the solutions. But it is a government that can back up an industry-led effort, and I think that's a very important point.

I think the other big difference between what I saw at the UNESCO meeting and here was the UNESCO government representatives didn't get it. I think the FTC, OMB, the FCC, NTIA are all to be commended for really doing the work to understand these technologies, to actually use the

technologies and to make some progress that way.

And I hope we can go on from this meeting to reach out to some of the other government agencies in the Federal Government, some of the state agencies and some foreign governments that don't yet get it and still think the answer is to step in with some top-down regulatory system before the technologies are really developed and the solutions have been explored.

Thanks, again, for organizing this. And I really commend you for an outstanding day.

MR. MEDINE: I think we are all beat. So I want to thank everyone for participating. Maybe we will meet next year in Monaco.

(Laughter.)

MR. MEDINE: Thanks. Rest all. We will see you tomorrow on E-mail.

(Whereupon, the meeting recessed at 6:45 p.m., to resume on Thursday, June 12, 1997 at 8:45 a.m.)

C E R T I F I C A T E O F R E P O R T E R

TITLE: PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY

HEARING DATE: June 11, 1997

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: 6/17/97

KAREN BRYNTESON

C E R T I F I C A T E O F P R O O F R E A D E R

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE

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